

# Dai droni alle armi autonome

Lasciare l'Apocalisse alle macchine?

a cura di Francesca Farruggia

Prefazione di Giorgio Parisi



**Sociologia**

**FrancoAngeli** 



Il presente volume è pubblicato in open access, ossia il file dell'intero lavoro è liberamente scaricabile dalla piattaforma **FrancoAngeli Open Access** (<http://bit.ly/francoangeli-oa>).

**FrancoAngeli Open Access** è la piattaforma per pubblicare articoli e monografie, rispettando gli standard etici e qualitativi e la messa a disposizione dei contenuti ad accesso aperto. Oltre a garantire il deposito nei maggiori archivi e repository internazionali OA, la sua integrazione con tutto il ricco catalogo di riviste e collane FrancoAngeli massimizza la visibilità, favorisce facilità di ricerca per l'utente e possibilità di impatto per l'autore.

Per saperne di più:

<https://www.francoangeli.it/autori/21>

I lettori che desiderano informarsi sui libri e le riviste da noi pubblicati possono consultare il nostro sito Internet: [www.francoangeli.it](http://www.francoangeli.it) e iscriversi nella home page al servizio "Informatemi" per ricevere via e-mail le segnalazioni delle novità.

# Dai droni alle armi autonome

Lasciare l'Apocalisse alle macchine?

a cura di Francesca Farruggia

Prefazione di Giorgio Parisi



**Sociologia**

**FrancoAngeli** ©

Questo volume è stato pubblicato con un contributo del Dipartimento di Scienze Sociali ed Economiche - DISSE, su fondi dei Progetti di Ateneo di Sapienza Università di Roma.

Copyright © 2023 by FrancoAngeli s.r.l., Milano, Italy.

L'opera, comprese tutte le sue parti, è tutelata dalla legge sul diritto d'autore ed è pubblicata in versione digitale con licenza *Creative Commons Attribuzione-Non Commerciale-Non opere derivate 4.0 Internazionale* (CC-BY-NC-ND 4.0)

*L'Utente nel momento in cui effettua il download dell'opera accetta tutte le condizioni della licenza d'uso dell'opera previste e comunica sul sito*  
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.it>

# Indice

<b>Acronimi</b>	pag.	9
<b>Prefazione</b> , di <i>Giorgio Parisi</i>	»	13
<b>Introduzione</b> , di <i>Fabrizio Battistelli</i>	»	17
<b>1. Armi non umane. Miti, sogni e incubi dell'autonomia delle armi</b> , di <i>Fabrizio Battistelli</i>	»	21
1.1. Introduzione. La preistoria	»	21
1.2. L'automazione del campo di battaglia come risposta tecnica a un'esigenza mediatica	»	22
1.3. La legittimazione della guerra e il mito delle "perdite zero"	»	26
1.4. L'inizio della storia: i droni tra diritto, politica, economia e filosofia	»	31
1.5. Osservazioni conclusive	»	38
Riferimenti bibliografici	»	40
<b>2. Caratteristiche, prospettive e problematicità dell'Intelligenza Artificiale</b> , di <i>Diego Latella, Gian Piero Siroli, Guglielmo Tamburrini</i>	»	43
2.1. Introduzione	»	43
2.2. <i>Machine Learning</i>	»	45
2.3. Limiti e problematicità del <i>Machine Learning</i>	»	51
2.4. Osservazioni conclusive	»	54
Riferimenti bibliografici	»	57
<b>3. Vulnerabilità delle tecnologie informatiche, Intelligenza Artificiale e LAWS</b> , di <i>Gian Piero Siroli</i>	»	61
3.1. Introduzione	»	61

3.2. Vulnerabilità intrinseche delle tecnologie informatiche	pag.	62
3.3. Vulnerabilità specifiche delle tecnologie IA/ML	»	66
3.4. Dibattito internazionale	»	70
3.5. Osservazioni conclusive	»	73
Riferimenti bibliografici	»	74
<b>4. Sviluppo e applicazioni delle armi semi-autonome e autonome letali</b> , di <i>Michael Malinconi, Juan Carlos Rossi</i>	»	76
4.1. Introduzione	»	76
4.2. Sviluppo e investimenti sui LAWS a livello internazionale	»	78
4.3. Caratteristiche e prospettive dei nuovi sistemi d'arma	»	83
4.3.1. Munizioni <i>loitering</i>	»	83
4.3.2. I sistemi d'arma ravvicinati o a corto raggio (CIWS)	»	84
4.3.3. Veicoli aerei da combattimento senza equipaggio – <i>Unmanned Combat Aerial Vehicles (UCAV)</i>	»	85
4.3.4. Munizioni guidate di precisione	»	86
4.3.5. Veicoli terrestri senza equipaggio – <i>Unmanned Ground Vehicles (UGV)</i>	»	87
4.3.6. Veicoli marini senza equipaggio – <i>Unmanned Marine Vehicles (UMV)</i>	»	87
4.4. Lo <i>swarm</i>	»	88
4.5. Droni armati in azione: la guerra in Ucraina	»	91
4.6. Osservazioni conclusive	»	94
Riferimenti bibliografici	»	95
<b>5. Il dibattito etico sulle armi autonome</b> , di <i>Guglielmo Tamburrini</i>	»	98
5.1. Le fonti normative del dibattito etico sulle armi autonome	»	98
5.2. La guerra giusta e i principi di distinzione e proporzionalità	»	99
5.3. Responsabilità degli operatori militari e dignità delle vittime	»	105
5.4. Armi autonome ed etica delle conseguenze	»	106
Riferimenti bibliografici	»	111

<b>6. L'opinione pubblica e i droni</b> , di <i>Francesca Farruggia</i>	pag.	113
6.1. Opinione pubblica e uso della forza	»	113
6.2. I droni e l'opinione pubblica italiana	»	114
6.3. Il fenomeno droni: livello di conoscenza e tenore delle opinioni	»	115
Riferimenti bibliografici	»	125
Sitografia dei sondaggi	»	126
<b>7. L'opinione pubblica di fronte alle armi autonome</b> , di <i>Francesca Farruggia</i>	»	127
7.1. L'opinione pubblica mondiale e le armi autonome	»	127
7.2. L'opinione pubblica italiana e le armi autonome	»	131
7.2.1. L'indagine IPSOS	»	131
7.2.2. L'indagine Demetra-Archivio Disarmo	»	133
7.3. Le giovani generazioni e le armi autonome	»	137
7.4. Osservazioni conclusive	»	140
Riferimenti bibliografici	»	141
Sitografia dei sondaggi	»	141
<b>8. Il diritto internazionale umanitario e la sfida delle armi autonome all'intus-legere</b> , di <i>Sofia Bertieri, Adriano Iaria</i>	»	142
8.1. Introduzione	»	142
8.2. Mezzi e metodi di combattimento	»	143
8.3. La protezione dei civili	»	146
8.4. Il ruolo dei consulenti giuridici e politici	»	148
8.5. L'umanità e la pubblica coscienza	»	150
8.6. La posizione UE e italiana	»	152
8.7. Osservazioni conclusive	»	156
Riferimenti bibliografici	»	157
<b>9. Il dibattito internazionale sulle armi autonome</b> , di <i>Guglielmo Tamburrini</i>	»	160
9.1. La comunità scientifica e l'etica delle armi autonome	»	160
9.2. Le armi autonome alla <i>Convention on Certain Conventional Weapons</i>	»	163
9.3. Il controllo umano significativo e i suoi contenuti	»	165
9.4. Verso un trattato internazionale sul controllo umano significativo delle armi autonome?	»	169
9.5. Osservazioni conclusive	»	171
Riferimenti bibliografici	»	173

<b>10. Le armi autonome tra sviluppo economico e controllo politico: istituzioni internazionali, comunità scientifiche, società civile</b> , di <i>Barbara Gallo, Maurizio Simoncelli</i>	pag.	176
10.1. Spese militari e investimenti nelle armi semiautonome e autonome	»	176
10.2. La IA in guerra e in combattimento: problemi strategici e tattici	»	178
10.3. Dibattiti e proposte nelle istituzioni internazionali	»	180
10.4. L'impegno della comunità scientifica e della società civile	»	182
Riferimenti bibliografici	»	188
<b>Appendice. I principali modelli di LAWS</b> , di <i>Michael Malinconi, Juan Carlos Rossi</i>	»	191
<b>Gli autori</b>	»	201



## *Acronimi*

ASW = Anti-Submarine Warfare (lotta antisommergibile)  
BLOS = Beyond Line of Sight (Oltre il limite della visuale)  
CCW = Convention on Certain Conventional Weapons (convenzione su certe armi convenzionali)  
CETC = China Electronics Technology Group Corporation  
CICR = Comitato Internazionale della Croce Rossa  
CIG = Corte Internazionale di Giustizia  
CIWS = Close in Weapon System (sistemi d'arma ravvicinati)  
CODE = Collaborative Operations in Denied Environment (operazioni di collaborazione in ambienti ostili)  
CPI = Corte Penale Internazionale  
C-RAM = Counter-Rocket, Artillery, Mortar (sistemi contro razzo, artiglieria e mortaio)  
CUS = Controllo Umano Significativo  
C3IR = Command, Control, Communication, Intelligence and Reconnaissance (comando, controllo, comunicazione, intelligence e ricognizione)  
DARPA = Defense Advanced Research Projects Agency (USA)  
DASA = Defence and Security Accelerator (acceleratore di difesa e sicurezza)  
DECANT = Defence Capability for Autonomous and Novel Technologies (capacità di difesa per tecnologie autonome e nuove)  
DIU = Diritto Internazionale Umanitario  
DMZ = Zona Demilitarizzata  
DL = Deep Learning (apprendimento in profondità)  
DoD = Department of Defense (USA)  
DSTL = Defence Science and Technology Laboratory (UK)  
EDM4S = Electronic Drone Mitigation System (sistema elettronico di mitigazione dei droni)  
EO = Elettro-Ottico  
FPI = Foundation for Advanced Studies (Russia)  
GAN = Governo di Accordo Nazionale  
GGE = Gruppo di Esperti Governativi

GIDE = Global Information Dominance Experiment (sperimentazione per il Predominio globale dell'informazione)  
GOFAI = Good Old-Fashioned Artificial Intelligence (Intelligenza Artificiale "all'antica")  
HRW = Human Rights Watch  
IA = Intelligenza Artificiale  
IAI = Israel Aerospace Industries  
ICRAC = International Committee for Robot Arms Control (Comitato internazionale per il controllo delle armi robot)  
ICT = Tecnologie Informatiche e di Comunicazione  
IDC = International Data Corporation  
IDF = Israel Defense Forces  
IFF = Identification Friend or Foe (identificazione amico/nemico)  
IHRC = International Human Rights Clinic  
IJCAI = International Joint Conference on Artificial Intelligence (conferenza internazionale congiunta sull'intelligenza artificiale)  
IoT = Internet of Things (Internet per gli oggetti quotidiani)  
iPRAV = International Panel on the Regulation of Autonomous Weapons (Conferenza internazionale sull'intelligenza artificiale)  
ISTAR = Intelligence Surveillance Target Acquisition and Reconnaissance (intelligence, sorveglianza, acquisizione del bersaglio e ricognizione)  
ISR = Intelligence, Surveillance, and Reconnaissance (intelligence, sorveglianza e ricognizione)  
ISR&T = Intelligence, Surveillance, Reconnaissance & Targeting (intelligence, sorveglianza, ricognizione e acquisizione del bersaglio)  
JAIC = Joint Artificial Intelligence Center (USA)  
KAIST = Korea Advanced Institute of Science and Technology  
LAWS = Lethal Autonomous Weapon System (sistemi di armi autonome letali)  
LOCUST = Low-Cost UAV Swarming Technology (tecnologia di sciami UAV a basso costo)  
LRASM = Long-Range Anti-Ship Missile (missili anti-nave a lungo raggio)  
MAD = Mutually Assured Destruction (distruzione reciproca assicurata)  
MCM = Mine Counter Measures (sistemi antimina)  
MCS = Mission Control System (sistemi di controllo di missione)  
MIT = Massachusetts Institute of Technology  
ML = Machine Learning  
NBS = Nächstbereichschutz system (Sistema di protezione del campo di applicazione)  
NC3 = Nuclear Command Control and Communications (Comando nucleare per il controllo e le comunicazioni)  
NSA = National Security Agency (USA)  
OEWG = Open Ended Working Group (gruppo di lavoro aperto)  
OODA = Osservare, Orientare, Decidere e Agire  
RA = Realtà Aumentata  
R&S = Ricerca e Sviluppo

RWS = Remote Weapon Station (postazione armata da remoto)  
SCO = Strategic Capabilities Office (USA)  
SEAD = Suppression of Enemy Air Defences (soppressione delle difese antiaeree  
nemiche)  
ST = Singapore Technology  
SKR = Stop Killer Robots (Fermare i robot killer)  
SRC = Skolkovo Robotics Center (Russia)  
STOM = Ship to Objective Maneuver (nave per le manovre ad)  
SVM = Support Vector Machines (macchine di supporto ai vettori)  
TPU = Tensor Processing Unit (unità di processamento del tensore)  
UAS = Unmanned Aircraft System (sistema aereo senza pilota)  
UAV = Unmanned Aerial Vehicle (velivolo senza pilota)  
UCAV = Unmanned Combat Aerial Vehicle (velivolo da combattimento senza pi-  
lota)  
UGV = Unmanned Ground Vehicle (veicolo terrestre senza pilota)  
UMV = Unmanned Maritime Vehicle (natante marittimo senza pilota)  
USV = Unmanned Surface Vehicles (natante da superficie senza pilota)  
USPID = Unione degli Scienziati per il Disarmo  
UUV= Unmanned Underwater Vehicle (sottomarino senza pilota)  
XAI = Explainable Artificial Intelligence (intelligenza artificiale interpretabile)



# *Prefazione*

di *Giorgio Parisi*

Sappiamo tutti che la scienza è un'arma a doppio taglio. La scienza aumenta il potere dell'uomo, che può scegliere la direzione in cui usare questo potere. Ogni volta che si compiono grandi progressi è necessaria una profonda riflessione su cosa sia lecito fare e su cosa non si debba fare.

L'intelligenza artificiale (IA) non sfugge a queste considerazioni. Nel 2019 le accademie dei paesi del G7, le cui delegazioni erano riunite a Parigi, hanno firmato all'unanimità una dichiarazione su intelligenza artificiale e società (dal titolo in inglese *Artificial Intelligence and Society*). Personalmente sono affezionato a questa dichiarazione in quanto come Presidente dell'Accademia Nazionale dei Lincei guidavo la delegazione italiana.

Nella premessa il documento dichiara che l'intelligenza artificiale è una delle tecnologie che sta trasformando la nostra società e molti aspetti della nostra vita quotidiana. La IA ha già apportato molti benefici positivi e può essere fonte di una considerevole prosperità economica. Ma l'intelligenza artificiale solleva anche questioni relative all'occupazione, alla riservatezza dei dati, alla privacy, alla violazione dei valori etici e alla fiducia nei risultati ottenuti.

Tra i vari punti sollevati c'è una dichiarazione estremamente importante che riguarda proprio le armi autonome. Cito testualmente:

L'intelligenza artificiale apre nuove possibilità per le applicazioni militari, in particolare per quanto riguarda i sistemi d'arma con significativa autonomia nelle funzioni critiche di selezione e attacco dei bersagli. Tali armi autonome potrebbero portare a una nuova corsa agli armamenti, abbassare la soglia della guerra o diventare uno strumento per oppressori o terroristi. Alcune organizzazioni chiedono un divieto sulle armi autonome, simile alle convenzioni in materia di armi chimiche o biologiche.

Tale proibizione richiederebbe una definizione precisa di armi e di autonomia. In assenza di un divieto di sistemi di armi autonome letali (*Lethal Autonomous*

Weapons Systems, LAWS), dovrebbe essere garantita la conformità di qualsiasi sistema d'arma al Diritto Internazionale Umanitario.

Queste armi dovrebbero essere integrate nelle strutture di comando e controllo esistenti in modo tale che la responsabilità e la responsabilità legale rimangano associate a specifici attori umani. C'è una chiara necessità di trasparenza e di discussione pubblica delle questioni sollevate in questo settore.

Si tratta di un problema estremamente delicato che deve essere affrontato con grande energia per essere risolto. Non è facile. La guerra si basa sul disegno, sulla fabbricazione e sullo schieramento, virtuale o attuale, di armamenti sempre più sofisticati. In questa prospettiva un autentico salto di qualità che potrebbe cambiare i connotati dei conflitti, sarebbe rappresentato dalle armi autonome, cioè da sistemi dotati di una IA in grado di “ragionare” e agire in assenza dell'uomo che li ha “istruiti”.

L'interesse dei militari ad espandere l'uso di armi autonome ha delle motivazioni chiarissime e giustificate dal loro punto di vista. Tuttavia, non possiamo permettere che un algoritmo debba risolvere problemi etici delicatissimi come per esempio:

- uccidere o non uccidere persone che sembrano combattenti nemici, ma forse non lo sono?
- Quanti civili morti sono un *danno collaterale* accettabile (espressione usata specialmente quando i morti non sono nostri o dei nostri alleati)?
- Come evitare in particolare danni gravissimi a bambini?

I trattati internazionali sono fondamentali per evitare catastrofi future. È una storia di insuccessi, di successi e di successi parziali. L'insuccesso più clamoroso è stato il trattato dell'Aia del 1899 in cui si vietavano i gas asfissianti (non ratificato dagli Stati Uniti), tra i tanti successi ricordiamo il Comprehensive Test Ban, ovvero il divieto assoluto di fare test di bombe nucleari, mentre tra i successi parziali metterei il trattato di non proliferazione (1968).

Può sembrare strano affermare che questo trattato abbia avuto un successo parziale: infatti è uno dei principali strumenti per evitare guerre nucleari ed è stato determinante per arrestare la proliferazione delle armi nucleari. L'importanza di questo trattato è stata immensa, ma non è stato pienamente applicato. In particolare, l'articolo VI afferma che ciascuna delle Parti del Trattato si impegna a perseguire in buona fede negoziati su misure efficaci relative alla cessazione della corsa agli armamenti nucleari in tempi brevi e al disarmo nucleare, nonché su un trattato sul disarmo nucleare generale e completo sotto un controllo internazionale rigoroso ed efficace.

Purtroppo, un trattato sul disarmo generale e completo è ancora molto lontano, e non si sono praticamente visti negoziati sull'eliminazione completa delle armi nucleari. È ancora più preoccupante l'attuale impossibilità

di arrivare a un trattato in cui gli stati nucleari si impegnino a non usare per primi le bombe nucleari, in quanto stati chiave, come gli Stati Uniti, la Russia, il Regno Unito, la Francia e il Pakistan, hanno ripetutamente dichiarato che si riservano l'uso di armi atomiche anche in caso di un attacco puramente convenzionale.

Queste difficoltà sui trattati concernenti le armi nucleari non ci devono far pensare che sia impossibile un trattato internazionale che vieti armi autonome letali. Un simile trattato è possibile ma è assolutamente necessario fare una riflessione chiara su tutti gli aspetti connessi. Un passo estremamente importante in questa direzione è fornito da questo volume che affronta nei suoi vari capitoli problematiche molto differenti.

Bisogna anche mobilitare l'opinione pubblica che sta assistendo rassegnata, come ad un fatto ineluttabile, alla progressiva introduzione di queste armi letali. Gli scienziati (sia delle scienze naturali e sociali, come coloro che hanno contribuito a questo libro) hanno una grande responsabilità nel comunicare questi aspetti delicati in maniera comprensibile ad una opinione ignara. Ma un compito estremamente importante spetta ai mezzi di informazione in maniera che venga esercitata una pressione sui decisori politici, che devono farei passi concreti per proteggere l'umanità dai danni più crudeli delle guerre.





# Introduzione

di *Fabrizio Battistelli*

Nelle scienze esatte il passo che separava lo studio dei sistemi fisici complessi da quello della IA si è dimostrato molto breve. Più lungo, ma prevedibilmente percorribile in un futuro prossimo, è il cammino verso applicazioni utili per l'umanità, dalla scoperta di nuove terapie fino alla guida automatica delle automobili. Il percorso è più accidentato (ma viene perseguito nei laboratori delle maggiori potenze senza badare a spese) quando i sistemi complessi e la IA vengono studiati per fini non scientifici bensì strategici: non per creare ma per neutralizzare, non per promuovere ciò che ci può servire ma per interdire ciò che (temiamo) ci possa minacciare. Un esempio tanto attuale quanto drammatico prende corpo quando dal dominio della vita, della salute e del benessere morale e materiale, così come della produzione intellettuale e creativa – in una parola dal dominio della pace – ci trasferiamo nel dominio della guerra, secondo processi incrementali che vengono efficacemente descritti in questo volume.

È dalla rivoluzione industriale che il combattimento si fonda in misura crescente sul disegno, sulla fabbricazione e sul dispiegamento di armamenti sempre più sofisticati. In questo quadro un autentico *breakthrough*, un salto di qualità che potrebbe cambiare i connotati dei conflitti, è rappresentato dalle armi letali autonome LAWS, cioè da sistemi dotati di una IA in grado di “ragionare” e agire in assenza dell'uomo che li ha “addestrati”. Come propongo nel capitolo 1, l'intervento di qualcuno o di qualcosa in grado di farci vincere la guerra senza farci morire in battaglia è un sogno antico quanto l'uomo storico (quello cioè di cui abbiamo tracce documentate). Ai nostri giorni, però, questo sogno può trasformarsi in una realtà da incubo.

I più recenti progressi nella IA convergono nel conferire alle macchine (tanto civili quanto militari), una crescente indipendenza in grado di affrancarle dal controllo diretto dell'uomo. In particolare in quella frontiera avanzata che è “l'arte” della guerra, si sta progredendo dal controllo umano diretto (il cosiddetto *man-in-the-loop*), al controllo umano indiretto (*man-on-*

*the-loop*) fino all'incombente – a meno che non venga bandito prima – *man-off-the-loop*: ovvero alla completa autonomia della macchina dal controllo umano. Come nel capitolo 2 ammoniscono Diego Latella, Gian Piero Siroli e Guglielmo Tamburrini, grazie al progresso degli algoritmi le macchine si stanno mostrando capaci di apprendere, autonomamente e senza intervento umano. Nel capitolo 3 Siroli ricorda che, nel caso dei sistemi d'arma autonomi, i loro tempi di risposta sarebbero ben più repentini di quelli umani, abbattendo i tempi del ciclo osservazione-decisione-azione, cruciale nelle operazioni militari. Ne conseguirebbero modalità di ingaggio caratterizzate da ritmi “disumani” come già accade per certi tipi di droni nel caso di sciame (*swarms*) di sistemi coordinati tra loro, come ricostruiscono Michael Malinconci e Juan Carlos Rossi nel capitolo 4.

Sistemi fisici complessi, in cui numerose unità indipendenti interagiscono tra di loro in modo non necessariamente “ordinato” e tuttavia altamente funzionale, sono stati osservati nei comportamenti di alcune specie animali, come gli sciame di insetti oppure gli stormi di storni studiati da Giorgio Parisi (*In un volo di storni. Le meraviglie dei sistemi complessi*, Rizzoli, Milano, 2021). Nel frattempo, invece di funzioni che sarebbero ben più auspicabili, questi sistemi hanno ispirato sofisticate applicazioni di IA nell'ambito delle armi semi-autonome. Si è pervenuti così alla progettazione e produzione di microelicotteri armati a pilotaggio remoto che, guidati da algoritmi e dotati di GPS, processori e radio, riescono a volare senza scontrarsi, stazionare in aria aspettando il proprio turno per inserirsi nei ristretti spazi disponibili e da lì attaccare un nemico, proprio come farebbe uno sciame di api o di vespe contro un intruso. È questo il caso del piccolo velivolo senza pilota *Kargu* prodotto in Turchia (4 pale rotanti in un chilo e mezzo di peso), capace di raggiungere e colpire una postazione militare o una nave, distruggendole.

Esiste tuttavia un parziale motivo di ottimismo nei confronti del passaggio da comportamenti *automatici* a comportamenti *autonomi* e, di conseguenza, nei confronti di scenari di guerra inimmaginabili appena una generazione fa. Paradossalmente, esso deriva dagli ostacoli tecnici che, ancora oggi, si frappongono alla completa autonomia di macchine da guerra “intelligenti”. Come si vedrà dalle pagine che seguono, alcuni di questi ostacoli sono tali da convincere gli stessi responsabili della ricerca e sviluppo della IA applicata al militare a dilazionare l'avvento di un campo di battaglia totalmente autonomizzato. Ciò almeno sinché non esisteranno prove concrete che le nuove tecnologie non generino nella loro gestione disastri capaci di ritorcersi sugli stessi attori che le hanno attivate.

In analogia a quanto avviene per le applicazioni civili, ma in misura incomparabilmente superiore, è da notare che nella IA è cruciale il problema della *distinzione*. Infatti, a differenza di una situazione di pace, l'ambiente

bellico è, oltre che massimamente turbolento, anche intenzionalmente ingannevole. Niente a che vedere non soltanto con il mondo bene ordinato, ripetitivo e privo di sorprese di una catena di montaggio robotizzata di un'industria civile ma neppure, domani, con il traffico di una metropoli dove i veicoli si muovano mediante la guida automatica.

Come si è dovuto constatare in questi tempi di drammatici conflitti quali l'invasione russa dell'Ucraina, quando si parla della *fog of war*, o “nebbia della guerra”, ci si riferisce a un ambiente caratterizzato da una massima intensità di imprevisti, di origine per lo più intenzionale, a cominciare dall'intrinseca tendenza all'inganno da parte del nemico. Come spiega Guglielmo Tamburrini nel capitolo 5, sulla base delle attuali tecnologie della IA i problemi di discriminazione percettiva indotti da contesti non routinari impediscono una soluzione tecnologica soddisfacente. Test eseguiti su sistemi percettivi della IA formati da reti neurali profonde mostrano il fallimento della IA nel distinguere tra loro – a fronte delle minime perturbazioni introdotte nel corso di un *adversarial testing* (percepite invece dall'occhio umano) – oggetti tanto diversi tra loro quali una tartaruga e un fucile.

Sarebbe drammaticamente riduttivo sperare che uno scenario infausto come l'abdicazione a pensare e decidere su aspetti costitutivi della condizione umana quali la vita e la morte possa essere evitato unicamente grazie a difficoltà di ordine tecnologico e operativo, in quanto è altamente probabile che, prima o poi, esse saranno destinate a essere superate. Piuttosto, una grande responsabilità spetta alla comunità dei ricercatori delle scienze “esatte”, tanto quanto ai ricercatori sociali, in vista delle sinergie che gli uni e gli altri possono sviluppare collaborando tra loro, come hanno inteso fare in questo libro. Da un lato il dibattito internazionale sulle LAWS ha nelle comunità scientifiche di riferimento un inesauribile e perennemente aggiornato patrimonio di conoscenze, metodi e risultati (ancora Tamburrini nel cap. 9).

Nell'esperienza di un'altra fatale tecnologia come quella nucleare, ai tempi della guerra fredda furono gli scienziati – soprattutto ma non unicamente fisici – a svolgere un ruolo cruciale nella prevenzione della catastrofe. Infatti le loro analisi furono decisive nel mettere in guardia i rispettivi governi circa le conseguenze irreversibili di un conflitto atomico. Inoltre, grazie ai rapporti di colleganza stabiliti negli anni tra scienziati americani e sovietici (emblematico il caso del gruppo Pugwash), i ricercatori consolidarono un network poi rivelatosi prezioso quando negli anni '80 del XX secolo furono negoziati e sottoscritti gli accordi sul taglio degli armamenti nucleari. Uno scenario simile non è impossibile in riferimento alle armi semiautonome oggi e autonome domani, se alla pressione esercitata sui governi dagli esperti si aggiungerà quella dei comuni cittadini come mostrano i dati analizzati da Francesca Farruggia nei capitoli 6 e 7, in Italia e pressoché ovunque nel

mondo, l'orientamento popolare è verso chiare e sostanziali limitazioni nei confronti di queste pericolose tecnologie. Spetterà infine al diritto internazionale – argomentano nel capitolo 8 Sofia Bertieri e Adriano Iaria – definire i termini del controllo degli armamenti semiautonomi e autonomi, e alla diplomazia implementare le iniziative per una prevenzione della proliferazione degli armamenti autonomi.

Se gli accordi internazionali e i provvedimenti legislativi sono una prerogativa delle istituzioni politiche, la spinta ad adottarli può provenire unicamente dalla società civile. La competenza e la capacità comunicativa delle comunità scientifiche – mostrano Barbara Gallo e Maurizio Simoncelli nel capitolo 10 – rappresentano la condizione necessaria affinché si crei una simile spinta; essa tuttavia si rivela sufficiente unicamente se raggiunge e mobilita le coscienze di strati sempre più ampi della popolazione. All'indomani della fine della guerra mondiale e dell'irruzione sulla scena internazionale dell'arma atomica nella tragica ecatombe di Hiroshima e Nagasaki, Albert Einstein lanciava un appello agli scienziati perché si assumessero la responsabilità di informare i concittadini su questioni che sono, diceva, di vita o di morte. Einstein paragonava alla scoperta del fuoco l'introduzione della tecnologia atomica. Di fronte all'applicazione a scopi bellici di innovazioni di questa portata, il grande scienziato osservava che «non esiste possibilità di controllo se non mediante il conseguimento della comprensione e la pressione [esercitata] da parte dei popoli del mondo» (A. Einstein, lettera-appello inviata da Princeton il 22 gennaio 1947).

L'avvento dell'intelligenza artificiale è oggi un passaggio epocale che ha molti punti di contatto con un evento altrettanto ambivalente quale la liberazione dell'energia nucleare indotta dall'uomo. Adesso come allora, è compito degli scienziati indicare le vie per prevenire i rischi delle scoperte, mentre lo è dell'opinione pubblica convincere i governi a intraprenderle.

# *1. Armi non umane. Miti, sogni e incubi dell'autonomia delle armi*

di *Fabrizio Battistelli*

## **1.1. Introduzione. La preistoria**

Quella delle armi è una strana storia di emancipazione delle macchine dall'uomo, che pure le ha create. Nell'evoluzione della specie, raramente la base di partenza è stata la formulazione di possibili modi per andare d'accordo tra gruppi differenti. Molto tardi nella vicenda umana alcune personalità illuminate hanno provato a proporre progetti di pace perpetua o anche soltanto accordi per il bando di strumenti di distruzione particolarmente micidiali per i tempi, quali la balestra o la polvere da sparo. E di solito, con scarsi risultati. Molto più spesso uomini di Stato e comandanti militari, e prima ancora poeti epici e narratori, hanno dato libero sfogo alla fantasia per ideare sempre nuove soluzioni allo scopo di sconfiggere l'avversario difendendo o attaccando. Ingenti risorse intellettuali e materiali sono state convogliate su questo obiettivo. Una costante è rappresentata dalla strategia di investire sulle armi per risparmiare sulle perdite. Fin dai primordi dell'uomo storico, il sogno degli eserciti (occasionale nei soldati, ricorrente nei comandanti) è stato quello di un *deus ex machina* (un "qualcuno" o un "qualcosa") dotati di poteri eccezionali che intervenisse nella battaglia gettandovi tutto il proprio peso e inclinando il piatto della bilancia a favore del *nostro* esercito e a danno del *loro*.

Quel trattato di polemologia in versi che è l'*Iliade* offre un esempio inequagliato di questa aspettativa. Senza risparmio di energie umane e divine, una panoplia di interventi prodigiosi fatti di apparizioni, azioni di forza, stratagemmi e incantesimi vede gli dèi dell'Olimpo schierarsi a favore dei greci (Era, Atena, Poseidone) e, sul fronte opposto, dei troiani (Apollo, Afrodite). Sul piano storico, all'incirca cinque secoli più tardi i romani vittoriosi introdurranno la pratica di trasportare nell'Urbe non soltanto i re e i capi dei popoli sconfitti destinati a mostrarsi in catene al seguito del generale trionfa-

tore, ma anche i loro dèi con i relativi poteri, da includere direttamente nel Pantheon romano. Agli albori dell'età moderna, il ruolo che nell'antichità classica era stato degli dèi verrà sempre più spesso rivestito dalle forze della natura. Nelle storie nazionali ricorrono i miti di eventi naturali apparsi a soccorrere l'esercito degli uni e a disperdere quello degli altri (il tifone che nel 1281 distrugge la flotta dei mongoli che sta per invadere il Giappone, i marosi che proteggono la Britannia e affondano i vascelli della Invincibile Armata spagnola).

L'interrogativo è, giunti all'età dell'Illuminismo, come dare spazio al mito, che (insieme al suo stretto parente l'inganno) è un ingrediente della propaganda di guerra, utile a esaltare la volontà di vittoria della popolazione e dell'esercito, contemporaneamente deprimendo la volontà del nemico. Coniuga mito e razionalità illuminista il maggiore stratega del XVIII secolo, Federico II di Prussia, che punta su fattori organizzativi moderni quali l'addestramento e la disciplina dei reparti, al fine di conseguire la superiorità sul campo di battaglia. È sintomatico che, con questo obiettivo operativo, il re prussiano evochi con il fedele generale von Saldern una metafora essa stessa molto moderna: quella di soldati da addestrare tanto e così bene al maneggio delle armi da trasformarsi in "automi tiratori"<sup>1</sup>.

## **1.2. L'automazione del campo di battaglia come risposta tecnica a un'esigenza mediatica**

Sin qui si tratta di semplici premonizioni. Per gli sviluppi veri e propri bisognerà aspettare l'ultimo terzo del XX secolo. Preparata dalle sempre più ingegnose applicazioni della scienza e della tecnologia a quella che, nella lettera a Engels del 7 luglio 1866, Marx chiamava «l'industria di macellare gli uomini» (Marx ed Engels, 1974, vol. *XLII*, p. 257), sulla scena bellica fa irruzione il concetto di automazione del campo di battaglia. Il 16 ottobre 1969, di fronte al senato degli Stati Uniti il capo di stato maggiore dell'esercito, generale William C. Westmoreland disegna il seguente scenario:

<sup>1</sup> Come osserva Michel Foucault, «I famosi automi [...] erano anche manichini politici [...] ossessione di Federico II, re minuzioso delle piccole macchine, dei reggimenti bene addestrati e delle lunghe esercitazioni» (Foucault, 1976, 148). Se l'uomo è, secondo il materialista La Mettrie, una macchina, la macchina può essere un uomo. Non a caso il Settecento è il secolo in cui (a prescindere da mode effimere e da raggiri, come l'imbattibile automa giocatore di scacchi detto "il Turco"), vengono anche effettuati i primi studi scientifici dedicati all'automazione.

Nel campo di battaglia del futuro le forze nemiche saranno identificate, tracciate e inquadrare come bersagli quasi istantaneamente mediante l'uso di connessione dati, valutazioni di intelligence assistite da computer e controllo di tiro automatizzato (Westmoreland, 1969).

Il successivo passo dottrinale in direzione del campo di battaglia automatizzato verrà compiuto al passaggio di Millennio con la dottrina della *Network-centric warfare* (Abrahamsson e Ydén, 2005), resa possibile dai progressi tecnologici realizzati nel complesso di capacità ISTAR (*Intelligence Surveillance Target Acquisition and Reconnaissance*). L'ultimo passo in ordine di tempo prenderà corpo con le armi autonome letali, LAWS.

Come mai il generale Westmoreland esternava sotto forma di una solenne previsione quello che al momento non era altro che un *wishful thinking*? La singolarità e nello stesso tempo la specificità dell'esternazione meritano una spiegazione. Essa, a sua volta, costituisce un classico esempio dello stretto rapporto che lega l'evoluzione del pensiero strategico non soltanto agli obiettivi politici, ma anche allo sviluppo economico, scientifico e tecnologico di una determinata società in un determinato periodo storico. Non è infatti un caso che l'urgenza di rendere automatizzato (e in prospettiva autonomo) il campo di battaglia sia stata formulata con tanta forza dal comandante del contingente militare di quella che, in proporzione alle forze impiegate, ha costituito la più sanguinosa guerra esterna nella storia degli Stati Uniti, e certamente la più contestata: la guerra del Vietnam. Con 58mila soldati americani caduti e oltre 300mila feriti, Westmoreland ha avuto modo di osservare da vicino e toccare drammaticamente con mano i costi politici di una carneficina.

La circostanza offre lo spunto per una riflessione sulla più cruciale delle tendenze rintracciabili nel pensiero politico-strategico contemporaneo, in particolare presso la superpotenza mondiale Stati Uniti: il mito della guerra "a perdite zero". L'idea di risparmiare il più possibile le vite dei propri soldati non è una novità per nessun esercito, naturalmente. È tuttavia nel XX secolo che l'ipotesi di realizzare una cospicua economia di vite umane nei propri ranghi, massimizzando le opportunità tecnico-scientifiche dell'azione militare (contemporaneamente massimizzando le perdite nei ranghi del nemico) si concretizza con l'avvento dell'arma aerea.

Superata la fase del primo conflitto mondiale, in cui l'ambiente terrestre è dominato dai massacri simmetrici della guerra di trincea (essa stessa imposta da un'arma proto-automatica come la mitragliatrice), entra in scena un nuovo e dirompente sistema d'arma: l'aeroplano. Confermando il dato che per manifestarsi inizialmente le innovazioni assumono forme tradizionali, le prime prove della nuova arma assumono le sembianze dei duelli cavallere-

schì tra i caccia a elica. Presto chiaritesi le potenzialità del dominio del cielo, il dopoguerra si caratterizza per la formulazione da parte dell'italiano Giulio Douhet (1921) della dottrina del bombardamento "strategico", per la prima volta messa in pratica nel 1937 dall'aviazione tedesca con l'annientamento della città spagnola di Guernica. Prendendo di mira non solo i bersagli militari, ma anche e soprattutto quelli civili, la teoria e la pratica del bombardamento strategico individuano nella moltiplicazione delle vittime tra la popolazione inerme non un semplice danno collaterale, ma l'obiettivo globale di demoralizzare il nemico e spezzare la sua resistenza. Nella Seconda guerra mondiale bombardamenti a tappeto contro i centri abitati e altri obiettivi civili vengono inizialmente effettuati dai tedeschi a scopo terroristico contro Varsavia, Rotterdam, Coventry, Londra ecc.; non diversamente da come nella seconda metà del conflitto faranno gli Alleati per motivi tattici a Cassino e, a scopo di ritorsione, contro le città tedesche di Colonia, Brema, Lubeca e Dresda, sino a toccare l'acme con l'irruzione sulla scena bellica dell'arma atomica. A fronte dell'accanita resistenza del territorio nazionale da parte delle forze armate giapponesi, le due bombe atomiche sganciate dagli Stati Uniti sulle città di Hiroshima e Nagasaki verranno per lo più giustificate con l'esigenza di risparmiare ulteriori perdite nelle file dei soldati americani (Maddox, 2004; Walker, 2005).

Ancora tollerati in un contesto di emergenza estrema e globale come il secondo conflitto mondiale, oggi gli enormi costi in vite umane presentati dalla guerra appaiono sempre meno legittimati agli occhi dell'opinione pubblica, a partire dai conflitti limitati della Guerra fredda, quali la Corea (1954) e soprattutto il Vietnam (1964-1974). Per quanti sforzi faccia l'élite politica e militare per "vendere" ai cittadini elettori il sacrificio di vite umane, quest'ultimo appare ogni volta più spropositato in una società come quella contemporanea, progressivamente più secolarizzata e focalizzata sui diritti individuali. Le fasi storiche precedenti erano state dominate dalla trascendenza religiosa, che minimizzava la rilevanza della vita terrena in favore dell'unica vita veramente importante, quella ultraterrena. Invece, nella società contemporanea l'immanenza indotta dai valori individualistici della modernità e del mercato rende l'idea della morte intollerabile.

Un ruolo decisivo in questo senso è esercitato in occidente dai mass media che adottano nei confronti dei decisori politici uno stringente «scrutinio» (Burk, 1998), che raggiunge il suo apice proprio con la guerra del Vietnam. Documentando vividamente e in tempo pressoché reale ciò che accade nella giungla vietnamita (innanzitutto il sacrificio di migliaia di giovani coscritti che muoiono), a partire dall'offensiva del Tet scatenata dai Vietcong nel 1968, la tv americana porta «nei tinelli di casa» l'evidenza di una guerra che non avrebbe potuto essere vinta se non a un prezzo difficilmente sostenibile per



qualsiasi leader di una democrazia rappresentativa. Negli USA il crollo del consenso sarà devastante e determinerà il cedimento del fronte interno (polemiche politiche e mediatiche, opposizione di massa alla leva militare, oceaniche manifestazioni contro la guerra con in prima fila veterani e invalidi che restituiscono le decorazioni ecc.). Per un intero paese il trauma sarà profondo e la crisi per i vertici politici e militari degli Stati Uniti sarà inevitabile. Lo scandalo per un episodio grave ma non estremo come lo spionaggio ai danni del partito di opposizione costerà allo stesso presidente Nixon l'*impeachment*. Dato specificamente rilevante, nelle politiche della difesa inizierà un lungo e tormentato processo autocritico che condurrà all'abbandono della coscrizione obbligatoria, all'introduzione di forze armate di soli volontari e a una drastica revisione delle strategie comunicative delle forze armate.

Consapevoli che un'interpretazione favorevole degli eventi militari non risiedeva tanto nei contenuti o nelle forme dei comunicati ufficiali e delle conferenze stampa bensì nel processo di creazione della notizia, tutta l'attenzione venne focalizzata sulla "gestione" della medesima (*news management*). Vista l'impossibilità in un ordinamento democratico di distogliere dal teatro delle operazioni i corrispondenti di guerra, i comandi militari iniziarono a canalizzarli in appositi gruppi (tecnica del *pool* di giornalisti, guerra del Golfo 1990-91). Successivamente, in Iraq nel 2003, i giornalisti furono addirittura incorporati (*embedded*) nei reparti, presso i quali essi si trovarono a condividere gli stress ma anche il cameratismo propri del gruppo primario del combattimento. In questo modo l'evento diventava notizia nel modo più socialmente naturale possibile.

A complicare le cose, tuttavia, nel frattempo si andava verificando un'accelerazione nell'"intrusione" dei "profani" (mass media e cittadini) nella guerra, cioè nel *sancta sanctorum* del potere politico. A mezzi di comunicazione di massa sempre più esigenti, infatti, sono andati aggiungendosi i *social media* con la loro straordinaria capacità di veicolare testi e immagini sulle ali di tecnologie sempre più sofisticate e, contemporaneamente, maneggevoli, economiche e alla portata di tutti. Si pensi, solo per fare un esempio, ai telefoni cellulari in grado di scattare foto, uno strumento dirompente per la capacità generalizzata e distribuita a tutti di documentare gli eventi mediante l'inattaccabile prova fotografica caso delle torture nel carcere americano di Abu Ghraib (Iraq, 2004).

L'agguerrito scrutinio dell'opinione pubblica, così, coinvolge al completo gli attori incaricati della sicurezza interna ed esterna, rendendo protagonisti tutti coloro che hanno a disposizione un pc, cioè un numero crescente di persone, negli stessi paesi in via di sviluppo. La loro intrusione si configura come un dato politico che può essere anche manipolato dal potere ma che non può essere impedito in sé e quindi è in grado di condizionare le scelte dei governi.

Di lì a poco, l'inarrestabile diffusione dei social sfiderà la capacità di controllo anche da parte dei regimi più autoritari (il sito cinese WeChat veicola i messaggi di oltre un miliardo di utenti). Nell'esorbitante numero degli interlocutori da sorvegliare i governi autoritari trovano la loro nemesi. Invece nelle democrazie tecnologizzate la nemesi si manifesta nell'esorbitante quantità dei dati appositamente raccolti dagli organi governativi stessi. Nel caso dei droni, ad esempio, uno "tsunami di dati", rilevati da appositi apparati che operano autonomamente, si abbatte sugli analisti addetti. Nell'intelligence dell'aviazione americana, la proporzione stimata è di diciannove analisti per ogni drone; destinati a diventare duemila quando l'attuale visione ristretta del drone sarà sostituita dallo «sguardo di Gorgone» capace di abbracciare in un solo colpo l'intera città (Bauman e Lyon, 2014, p. 6).

### 1.3. La legittimazione della guerra e il mito delle “perdite zero”

Per quanto spregiudicata sia la loro azione di governo, in un ordinamento democratico-rappresentativo è difficile per i leader ignorare del tutto i cittadini, sebbene ne possano sempre condizionare gli atteggiamenti. Un caso di scuola resta la martellante campagna orchestrata nel 2002-03 dal presidente Bush per legittimare l'intervento militare in Iraq con il pretesto di neutralizzare le «armi di distruzione di massa» attribuite a Saddam e di punire il suo presunto «coinvolgimento negli attacchi terroristici dell'11 settembre». In ogni caso la politica non può prescindere dalla variabile del consenso, e deve comunque cercare di ottenerlo.

Per uno scopo scarsamente popolare come l'uso della forza i governi devono garantire alle proprie decisioni la legittimazione, cioè una risorsa che presuppone il consenso dell'opinione pubblica. Il concetto sociologico di *legittimazione* ne contiene a sua volta altri: da un lato la coppia legittimità/legalità (concetti giuridici), dall'altro l'*efficacia* (concetto economico) (Battistelli, Galantino, Lucianetti, Striuli, 2012). Per potersi dire legittimo il ricorso alla forza armata deve soddisfare tre condizioni: basarsi su una *iusta causa*, la quale in età moderna è iscritta nel diritto di autotutela individuale e collettiva ex art. 51 della Carta delle Nazioni Unite e/o nell'autorizzazione del Consiglio di Sicurezza ex art. 42. Una volta assicurata la *legittimità* all'impiego della forza (*jus ad bellum*), quest'ultimo deve altresì garantire la *legalità* dei mezzi impiegati (*jus in bello*). L'intervento militare, dunque, è chiamato a rispettare i vincoli cui lo Stato deve attenersi secondo il diritto internazionale umanitario (Convenzioni di Ginevra del 1949, protocolli ag-

giuntivi, clausola Martens)<sup>2</sup>. Infine, per quanto riguarda l'efficacia, essa si misura sulla base di tre condizioni politiche: la prima è la massima salvaguardia della vita dei combattenti; il secondo è la durata il più possibile breve delle operazioni; il terzo consiste nel successo delle operazioni medesime.

Frutto dello sforzo plurisecolare del diritto di estendere la propria competenza, progressivamente conseguita all'interno dello Stato, anche ai rapporti fra Stati, questa parte del ragionamento configura un auspicio piuttosto che un effettivo risultato. Additato da molti come un nobile tentativo (Bobbio, 1994), giudicato da altri come un'aspirazione utopica (Morgenthau, 1997), la normativizzazione della guerra e della pace sperimenta nell'era contemporanea una situazione largamente contraddittoria, caratterizzata com'è da grandi minacce (prima fra tutte quella rappresentata dall'arma nucleare) ma anche da spinte in controtendenza provenienti dal basso.

Da un lato la persistenza del fenomeno guerra "autorizza" – in un processo tautologico di rispecchiamento fra gli attori statali – i governi a non rinunciarvi. Dall'altro, almeno nelle società occidentali, questa forma di relazione estrema con un particolare tipo di "altri" (i nemici) ha visto significativamente indebolirsi la propria legittimazione di massa. I costi umani che comporta il ricorso alle armi, infatti, sempre meno vengono considerati danni collaterali, involontari ed inevitabili, e sempre più spesso vengono considerati il frutto di specifiche scelte di natura politica di cui i decisori sono chiamati a rispondere.

A far riflettere i politici contribuiscono, sia pure parzialmente, gli stessi studiosi che, di parte non solo progressista ma anche conservatrice, appaiono unanimi nel diagnosticare una società occidentale che, nella sua fase post-moderna, è sempre meno incline all'uso della forza, tanto più quando provoca vittime. Fra i consulenti di George W. Bush, uno studioso neo-con come Robert Kagan ammette l'esistenza di una «crescente avversione post-moderna alla forza militare, alla politica di potenza e all'idea stessa di equilibrio tra potenze» (Kagan, 2004, p. 17). Ovvero, come precisa un altro studioso, il clintoniano Joseph S. Nye fautore del *soft power* USA basato su mass media, consumi e diritti umani, «le democrazie post-industriali sono focalizzate sul benessere piuttosto che sulla gloria delle gesta militari e aborriscono la perdita di vite umane» (Nye, 2005, p. 24).

La crescente impopolarità del ricorso alla forza soprattutto (ma non unicamente) nelle società occidentali è un dato di fatto (Battistelli, 2004; Giacomello e Coticchia, 2007). Questo atteggiamento è indissolubilmente connesso al tema della morte: uccidere ed essere uccisi sono modalità costitutive della guerra, un aspetto che genera avversione e raccapriccio nella «civiltà

<sup>2</sup> V. oltre cap. 8.

delle buone maniere» (Elias, 1982). Rispetto alle società pre-moderne, nelle quali la morte era considerata un evento familiare, reso accettabile dalla religione, la moderna società occidentale, depauperata della funzione consolatoria offerta dal cristianesimo, lascia l'individuo solo nell'affrontare questo "scandalo" della condizione umana. Fino al punto che, nella società post-moderna, la morte è divenuta un vero e proprio tabù, un evento inaccettabile, «intrinsecamente vergognoso e orripilante» (Gorer, 1965: 171, cit. in Bauman, 1995). I governi, dunque, si trovano in imbarazzo a decidere di interventi militari che comportano la perdita di quel bene supremo che, con la crisi della trascendenza, è divenuta la vita umana, come mostrano due differenti spiegazioni.

Sociologi, politologi ed esperti di strategia hanno discusso a lungo tanto sulla genesi di questo che è ormai un consolidato atteggiamento occidentale di fronte alla morte e si sono interrogati sulle possibili "soluzioni", siano esse rappresentate dagli adattamenti spontanei degli attori interessati (i soldati e le loro comunità di riferimento) ovvero quelli intenzionali (cioè le strategie comunicative e organizzative dei vertici politici e militari).

Quanto alle spiegazioni, è da ricordare quella "demografica" avanzata da Edward Luttwak (1994, p. 27), secondo cui i paesi membri del Consiglio di sicurezza dell'ONU – Stati Uniti, Regno Unito, Francia più la Russia (mentre non è citata la Cina) – possono ancora possedere una base economica e una forza militare adeguate a condurre guerre, ma «le loro società sono così allergiche alle perdite, che di fatto essi sono debellicizzati o quasi». Operata questa diagnosi, Luttwak descrive l'imperante atteggiamento di ipertutela delle vite umane, per il quale conia il termine di *motherism* sul modello dell'italiano "mammismo". Mentre infatti nelle società precedenti l'elevata numerosità dei figli e le precarie condizioni di vita rendevano la morte di uno o più di essi un evento frequente, in quella contemporanea il drastico calo delle nascite rende per una madre e un padre inconcepibile l'idea di poter perdere un figlio. Ciò perfino in forze armate formate da soli volontari, dove i genitori possono essere favorevoli all'arruolamento del figlio o della figlia, ma poi ne vivono l'eventuale decesso «come uno scandalo oltraggioso, piuttosto che come un rischio professionale» (Luttwak, 1994, p. 25). È così che, secondo l'esperto di questioni strategiche, in un prossimo futuro i paesi che presentano una ridotta natalità non saranno più in grado di giocare un ruolo di grande potenza, capace di proiettare la forza sulla scena mondiale laddove è necessario.

Diversa ma non incompatibile con quella appena esposta, è l'interpretazione micro-sociale di Anthony King (2010), ricavata dall'esperienza dei militari britannici caduti in Afghanistan. Tramontata l'etica patriottica e collettiva che aveva sostenuto socialmente e psicologicamente il guerriero e sa-

cralizzato il suo sacrificio – da Sparta fino alla Prima guerra mondiale (culto del Milite ignoto) – nell’iperindividualistica società postmoderna l’elaborazione del lutto è ben più ardua che in passato e segue una procedura complessa. Lo studio effettuato dal sociologo inglese sui necrologi e sulle commemorazioni funebri dedicate a soldati nel Regno Unito mostra come questa procedura si sviluppi in due fasi. Nella prima il caduto viene recuperato nella sua identità di militare, vista tuttavia non più come l’adempimento di un dovere collettivo bensì come l’adempimento di una vocazione individuale, perseguita con consapevolezza e coerenza. Nella seconda fase, il caduto viene presentato come persona, come figlio, coniuge, padre, «uno di noi» nella vita della comunità. Questo «addomesticamento» del soldato va di pari passo con una momentanea «svilirizzazione» dello Stato che, a differenza di quanto era accaduto per circa 2/3 del XX secolo, adesso:

Non è più libero di impiegare e perdere le proprie forze armate come crede [...] [avendo invece] il dovere di prendersi cura dei propri soldati, la cui protezione è ora (anche più che il compimento della missione) la sua responsabilità principale (King 2010, p. 21).

Passando dall’analisi del nodo opinione pubblica/evento bellico che provoca vittime alle “soluzioni” approntate dai governi per gestirlo, queste appaiono per lo più banalmente situazionali e, come tali, di corto respiro. La più grossolana è quella praticata dai regimi autoritari, che consiste nell’impedire la circolazione dell’informazione sui costi umani del conflitto nel quale è stato coinvolto il paese, proibendo la pubblicazione delle notizie in materia e perseguitando i giornalisti colpevoli di occuparsene. Il silenzio è il metodo più utilizzato da una “democrazia” come la Russia post-comunista. Qui i governi direttamente o indirettamente controllati da Putin hanno steso la coltre del segreto su campagne repressive come quella condotta in Cecenia, la cui denuncia è costata la vita nel 2006 alla giornalista Anna Politovskaja. Efficace nel breve periodo, peraltro, la censura parziale o integrale non impedisce mai del tutto la circolazione dell’informazione, come la stessa Unione sovietica dovette constatare in occasione dell’occupazione dell’Afghanistan. Gli altissimi costi in vite umane (quasi un altro Vietnam) che comportò l’ultima delle guerre dell’URSS (1979-1989) ebbero un ruolo decisivo nella delegittimazione e nella crisi dell’intero regime sovietico. L’«operazione speciale» (cioè l’invasione dell’Ucraina) in cui sono attualmente impegnate le forze armate russe costituirà un decisivo banco di prova per la verifica o meno dell’ipotesi «perdite umane».

Più morbida ma non meno insidiosa la strategia dei governi degli Stati

Uniti nell'affrontare i lutti delle campagne militari all'estero. L'esperienza del Vietnam era stata così traumatica per i cittadini americani, da ricevere una specifica denominazione giornalistica, la *body-bag syndrome* (cioè la sindrome dell'"involucro di plastica" con il quale venivano reimbarcate per gli Stati Uniti le salme dei caduti). Di conseguenza, mai per tutta la durata della guerra in Iraq, né il presidente G.W. Bush, né alcun altro membro del governo degli Stati Uniti si è mai recato a ricevere il corpo di uno di questi soldati. Relativamente facile da praticare in società tradizionali e rette da governi autoritari, la strategia del silenzio resta un semplice attenuatore dei fattori di crisi. Non è agevole mettere a tacere i costi umani delle guerre in un paese come gli USA, che della libertà di parola ha fatto un caposaldo costituzionale a norma del primo emendamento della Costituzione e, soprattutto, un valore condiviso e un comportamento diffuso. Su tale libertà i mass media "classici" hanno fondato il loro impero che, pur ridimensionato oggi dall'incalzare dei social, ha trovato in questi ultimi un erede non meno agguerrito.

Alla ricerca di soluzioni strutturali, cioè non di semplici palliativi bensì di rimedi validi una volta per tutte, gli spin doctor della Difesa hanno messo a punto una soluzione creativa: la *guerra a perdite zero* (Rogers, 2000). Nella narrazione che è andata sviluppandosi nell'establishment politico-militare negli ultimi decenni, la risposta all'eccessiva sensibilità del pubblico in tema di morti in guerra è promettere che questa sarà per così dire gratis o almeno che costerà molto poco in termini di caduti. Si tratta di una promessa largamente aleatoria, come mostrano le ultime campagne combattute dagli Stati Uniti. Esse infatti hanno oscillato tra il record positivo in termini di costi/benefici conseguito nella guerra del Kosovo nel 1999 (appena due americani deceduti, causa incidente), la soddisfacente performance della guerra del Golfo 1 per la liberazione del Kuwait nel 1991 ("solo" 380 morti nei ranghi degli americani) sino ai ben più realistici (e drammatici) standard di conflitti a bassa intensità ma di lunga durata, quale l'Afghanistan (3.573 caduti dal 2001 al 2021 fra i militari regolari e altrettanti fra i contractors) e l'Iraq (4.431 caduti dal 2003).

Il differenziale tra il valore che la vita umana riveste in Occidente e quello che riveste in Oriente rappresenta, di fronte a un particolare tipo di minaccia come quella terroristica, un serio fattore di inferiorità, o almeno come tale viene percepita dal nemico. Emblematica in questo senso la «Dichiarazione di guerra contro gli Americani che occupano la terra dei due Luoghi Santi» formulata da Osama bin Laden e pubblicata da un giornale londinese nel 1996: «Questi [nostri] giovani amano la morte come voi amate la vita» e «sono differenti dai vostri soldati» che i capi politici [americani] devono «convincere a combattere», laddove il problema dichiarato dai capi jihadisti

è di “trattenere i nostri giovani che attendono il loro turno [per diventare martiri]»<sup>3</sup>.

Senza entrare nel complesso discorso circa le alternative nella prevenzione del fenomeno terroristico, qui ci limitiamo a ricordare che la soluzione non è da cercare nel parossismo tecnologico cui indulge spesso la cultura (strategica e non solo) americana. Non esiste la *silver bullet*, la “pallottola d’argento” in grado di modificare radicalmente lo scenario tattico e strategico. La stessa realizzazione dell’antico sogno di colpire il nemico da una postazione inattaccabile possiede un indiscutibile efficacia “tecnica” ma non è, neppure essa, risolutiva.

#### **1.4. L’inizio della storia: i droni tra diritto, politica, economia e filosofia**

Venti anni fa, il 4 febbraio 2002, nei pressi della città di Khost in Afghanistan, un drone americano lanciava un missile Hellfire contro tre uomini, uccidendoli. Quello era il primo attacco effettuato da un velivolo a pilotaggio remoto con armi a bordo. Il drone era sulle tracce di Osama bin Laden ma con ogni probabilità le vittime non erano terroristi bensì uomini intenti a recuperare rottami di metallo. «Un’azione della CIA puramente per uccidere – commentò dieci anni dopo John Sifton su *The Nation* (2012) – effettuata indipendentemente da ogni azione militare». Con questa che ha tutta l’aria di un test, era iniziata l’era delle ‘esecuzioni mirate’ mediante droni. La nuova arma era stata adottata per la prima volta durante l’amministrazione di George W. Bush nella «guerra contro il terrorismo» proclamata dagli Stati Uniti all’indomani degli attentati di New York e di Washington nel 2001, ma solo nel corso della presidenza di Barack Obama era assunta ad arma tattica con un’indubbia valenza anche strategica.

I teatri destinatari delle azioni dei droni armati sono quelli dove si addestrano e operano le unità del terrorismo islamista, all’interno di “Stati falliti” e attanagliati dalla guerra civile (Afghanistan, Yemen, Somalia) o alleati incerti e turbolenti (Pakistan). Un bilancio sull’effettivo ruolo dei droni nel contrasto del terrorismo è oggetto di un acceso dibattito ad opera di fautori e critici di questi sistemi d’arma, con i primi che sottolineano la capacità di neutralizzare insorgenti e terroristi in impareggiabili condizioni di sicurezza e di economicità, mentre i secondi mettono sotto accusa la dubbia legalità, l’imprecisione nell’individuazione degli obiettivi e i conseguenti costi in termini di vite di innocenti che caratterizzano queste azioni. Come si vedrà, le

<sup>3</sup> [www.librarysocialscience.com/newsletter/posts/2015/2015-05-20--RAK.html](http://www.librarysocialscience.com/newsletter/posts/2015/2015-05-20--RAK.html).

stime sul numero di vittime degli attacchi dei droni sono altamente aleatorie, variando fra il 3-4% dei decessi secondo il governo degli Stati Uniti e l'11-15% delle altre fonti.

Rimane il fatto che, accanto ai bersagli “ufficiali” rappresentati da individui armati (terroristi e/o criminali), i droni armati hanno provocato centinaia di vittime nella popolazione civile. Emergendo dal silenzio che solitamente accompagna tali situazioni, alcuni casi hanno trovato spazio sulla scena mediatica internazionale. Si tratta ad esempio dei tre sospetti terroristi uccisi da un attacco effettuato in Yemen il 30 settembre 2011, la cui particolarità consiste nel possesso della cittadinanza americana da parte delle vittime. Oppure dell'ingegnere yemenita Feisal Ben Jaber che, avendo perso sotto i colpi dei droni due familiari innocenti nello stesso anno, ha intrapreso una campagna giudiziaria e di informazione presso l'opinione pubblica internazionale per attirare l'attenzione sull'illegalità e pericolosità di questi sistemi d'arma.

Pur raccogliendo nell'establishment politico e militare vasti consensi grazie alla loro economicità finanziaria e politica, i droni hanno due nemici o, se si preferisce, due «sistemi d'arma» molto particolari, che li controbilanciano. Differentemente dai primi, i secondi non sono letali ma non per questo sono del tutto inermi. Si tratta del diritto e dell'opinione pubblica.

Quanto al primo, la Dichiarazione Universale dei Diritti Umani, proclamata dall'Assemblea generale delle Nazioni Unite il 10 dicembre 1948, prevede all'art. 3 il «diritto alla vita, alla libertà e alla sicurezza degli individui», un impegno che, nei rapporti internazionali, impone agli Stati di salvaguardare i diritti umani anche quando ricorrono all'uso della forza. Come abbiamo visto nel paragrafo precedente, pure in questo caso la loro azione deve rispettare i criteri della legittimità e della legalità.

Il problema è che il diritto internazionale umanitario prevede solo i seguenti tipi di conflitto: o tra forze armate di due/più Stati, o tra forze armate regolari e gruppi armati, o di gruppi armati tra di loro, sempre comunque sul territorio di uno Stato. A spiazzare tutti, nel XXI secolo ha fatto la sua comparsa il conflitto tra un soggetto di diritto internazionale (Stato, organizzazione internazionale) e un attore non statale presente sul territorio di un altro Stato, ovvero in spazi non sottoposti alla giurisdizione di alcuno Stato, e attivo transnazionalmente (gruppi armati ma anche pirati marittimi, hacker e, infine, gli stessi piloti di droni). In un conflitto asimmetrico transnazionale, dunque, bisogna stabilire quale normativa applicare tra il diritto umanitario dei conflitti armati internazionali, il diritto umanitario dei conflitti armati non internazionali e il diritto internazionale dei diritti umani. Una questione resa ardua dal coinvolgimento di ben tre soggetti: lo Stato vittima, l'attore non-statale transnazionale, lo Stato sul cui territorio è condotta l'azione.



A complicare le cose, un ruolo da protagonista viene rivendicato dalla tecnologia, che promette di compensare le asimmetrie dei conflitti non convenzionali grazie all'impiego di sistemi dotati di ineguagliate capacità di lettura e intervento sul campo di battaglia in condizioni di semi-autonomia come i droni. Nonostante le polemiche politiche e le controversie legali, i responsabili della difesa e della sicurezza degli Stati Uniti sono tenacemente schierati a favore dell'uso dei velivoli senza pilota e ciò per una pluralità di fattori di natura operativa, economica e filosofica.

Sul piano operativo i droni gestiscono tutti quei compiti che sono stati definiti *dull, dirty and dangerous*, cioè «stupidi», «sporchi» e – soprattutto – «pericolosi». Manovrati a migliaia di chilometri di distanza, i droni garantiscono ai «piloti» (tecnici che operano seduti davanti a una console armati di un joystick) condizioni di sicurezza assoluta; un dato, come abbiamo visto, decisivo nel contesto sociale e politico dell'Occidente contemporaneo. Rinviando al cap. 4 per la trattazione degli aspetti operativi dei droni, qui ci focalizziamo sugli aspetti economici e filosofici.

In favorevole confronto rispetto agli aerei con pilota, i velivoli che a bordo non ne hanno nessuno esibiscono eccellenti performance dal punto di vista economico e finanziario. Ad esempio, paragonato ad un caccia di ultima generazione come l'F-35, il cui valore supera i 130 milioni di dollari, un drone armato del tipo *Predator* ne costa circa 10, cioè tredici volte di meno. Indiscutibilmente vittoriosi nel confronto con gli aerei nell'analisi costi/benefici, i droni rivestono anche un ruolo propulsivo nel sospingere in avanti l'innovazione tecnologica, in quanto la ricerca e sviluppo loro dedicati, costituiscono, situati come sono all'interno della strategica filiera della robotica, il crocevia con le più avanzate applicazioni delle scienze dell'informazione. Per finanziare le piattaforme robotiche in generale il dipartimento della Difesa degli Stati Uniti ha stanziato nel 2021 ben 7 miliardi e mezzo di dollari<sup>4</sup>.

È inoltre da sottolineare che, soprattutto ma non unicamente nelle fasi di ristagno economico, negli Stati Uniti e nelle altre economie di mercato la spesa militare riveste una funzione di volano keynesiano. Anche nei principali Paesi dell'Unione Europea i finanziamenti per una tecnologia d'avanguardia e *cost-effective* come quella dei droni si fanno largo nella crisi fiscale degli Stati, che devono gestire crescenti tagli alla spesa pubblica. La questione cruciale è a quali funzioni-obiettivo applicare i tagli. L'emergenza pandemica insorta nel 2020 ha portato alla luce la debolezza del sistema sanitario nelle varie versioni nazionali. Dagli Stati Uniti, che neppure il pre-

<sup>4</sup> [nationaldefensemagazine.org/articles/2021/5/27/pentagon-gets-\\$7-5-billion-for-unmanned-systems](https://nationaldefensemagazine.org/articles/2021/5/27/pentagon-gets-$7-5-billion-for-unmanned-systems).

sidente Obama è riuscito a dotare di un'assistenza sanitaria pubblica degna di questo nome, al Regno Unito, che era stato il primo paese a introdurla e poi l'ha smantellata nella fase liberista della Thatcher, all'Italia il cui welfare sanitario statale-regionale è stato oggetto negli ultimi venticinque anni di una inarrestabile campagna di riduzione e di riallocazione delle risorse dal settore pubblico a quello privato.

A fronte di una strutturale sottovalutazione dei danni causati dai *pericoli* (inintenzionali in quanto provenienti dalla natura come i cataclismi) e dai *rischi* (intenzionali in quanto provenienti da “nostre” decisioni di segno positivo ma ambivalenti quanto agli esiti), tutta l'attenzione politica e lo sforzo finanziario dei governi è concentrato su strategie e mezzi per prevenire le vere o presunte *minacce* (danni intenzionalmente inflitti a un nemico) (Battistelli e Galantino, 2019). Alla fortuna dei droni ha anche contribuito un'altra caratteristica, quella di essere una tecnologia *dual use*, ovvero applicabile in ambito sia militare sia civile. Avendo individuato nei droni i futuri catalizzatori della ricerca e sviluppo per l'industria aeronautica, elettronica e dell'informazione, a partire dal 2001 la Commissione Europea, vincolata dai trattati costitutivi dell'Unione che proibivano il finanziamento di programmi militari, ha cominciato a destinare fondi ai droni civili. Nel 2002 i droni sono entrati nell'agenda politica mediante il documento *STAR 21* predisposto dal Gruppo consultivo europeo sull'aerospazio, un'istanza a composizione ibrida in cui coabitano soggetti pubblici e privati, nazionali ed europei, di designazione politica così come aziendale<sup>5</sup>. Superando le cautele iniziali, nel 2005 è stata istituita la *European Defense Agency* per promuovere la collaborazione tra le industrie degli armamenti, nel cui programma-quadro 2007-2013 è entrata la categoria, “sicurezza” con 18 programmi relativi ai droni. Germania, Francia e Italia, cui si sono poi unite Spagna e Repubblica Ceca, collaborano alla progettazione di un Eurodrone, la cui operatività è prevista nel 2025 (PAX, 2019).

Grazie al nuovo strumento procedurale ribattezzato *roadmap*, a Bruxelles il processo decisionale democratico viene capovolto, antepoendo obiettivi specifici e risultati pratici alle deliberazioni sulle finalità generali (Hayes *et al.*, 2014). Nel 2013 la Commissione Europea ha lanciato la *Roadmap for the integration of Remotely-Piloted Aircraft Systems into the European Aviation System*, con il mandato di integrare i droni civili nello spazio aereo entro il

<sup>5</sup> Il Gruppo era così formato: cinque commissari europei, i dirigenti delle sei maggiori aziende aerospaziali, l'Alto rappresentante per la sicurezza comune e la politica di difesa nonché due membri del Parlamento europeo. Nel 2005 è sopraggiunta l'Agenzia Europea per la Difesa (EDA), dove gli Stati membri sono rappresentati da esponenti militari e industriali, la quale ha canalizzato importanti finanziamenti sui veicoli senza pilota, sia terrestri (26 milioni di euro), sia acquatici (47 milioni) sia aerei (105 milioni).

2028. È apparsa chiara la strategia europea di puntare sui droni come sintesi delle capacità civili e delle capacità militari in modo da sostenere le seconde mediante gli altrimenti inaccessibili programmi di finanziamento FP7, Horizon 2020, COSME (Csernatoni, 2016). In favore del processo continua a operare la crescente contiguità tra i due ambiti della sicurezza, quella internazionale e quella interna, in cui i droni possono giocare un ruolo da protagonisti. In particolare essi sono ritenuti importanti nelle missioni di sorveglianza marittima e dei confini nell'ambito migratorio. In conclusione, si stanno verificando due fenomeni: da un lato la sostanziale forzatura della logica *dual use*, introdotta circa tre decenni fa nell'assunto di riconvertire in senso civile le ridondanti industrie militari dei maggiori Paesi europei; dall'altro un'ulteriore spinta alla tendenza verso il *blurring*, cioè verso lo sfumare del confine fra le competenze militari e le competenze civili in tema di sicurezza, a tutto scapito delle seconde.

Non meno importanti, agiscono a favore dei droni i fattori, "filosofici", via via che «l'accento dovrà essere posto sempre di più sulle modalità automatizzate della guerra, le quali riducono l'esposizione umana al combattimento» (Quester, 2005, p. 34). Tra questi fattori includiamo le implicazioni di dottrina militare e di etica, aspetti tutti che confluiscono in una complessiva "ragione politica", sensibile all'incommensurabile vantaggio rappresentato dalla sostanziale invulnerabilità di questi armamenti. Qui, nella funzione armata che presuppone l'attacco a un determinato *target* mediante missili, emergono la principale specificità e il principale valore del drone come sistema offensivo. Tutti i restanti pregi, compreso quello economico, diventano secondari di fronte al dato secondo cui il drone è un formidabile sterminatore delle vite degli altri (i nemici), così come è un ancora più formidabile protettore delle (proprie) vite. In estrema sintesi si potrebbe affermare: dall'utopia delle *perdite zero* nei propri ranghi, al dato di fatto delle innumerevoli perdite nei ranghi nemici a *rischio zero*.

Agendo in un ambiente aereo sostanzialmente incontendibile e, soprattutto, sottraendo totalmente ad esso la presenza di un equipaggio, il drone rivoluziona il concetto stesso di guerra (in latino *bellum*, da *duellum*, da *duo*) che tradizionalmente è sempre stato definito, a partire dal mito degli Orazi e Curiazi fino alle analisi di Clausewitz, come sfida fra due forze fisiche e due volontà. Con il drone viene meno, accanto all'archetipo della relazione ostile tra due soggetti (i combattenti, dal latino *cum-battere*, battersi con), anche l'archetipo omerico dei due strumenti speculari e contrapposti: la lancia e lo scudo. Nella guerra di droni, uno dei due combattenti non è alla portata del nemico, e quindi è attivo ma non presente. La decurtazione della relazione tra due soggetti si estende ai due mezzi dell'offesa e della difesa, facendone venire meno uno: resta la lancia e scompare lo scudo che, privo di uno dei

due combattenti da proteggere, diventa superfluo. A causa dell'assenza di umani che lo gestiscano sul campo, e grazie anche al suo ridotto valore economico, il velivolo guidato da remoto non è più (a differenza di un aereo da combattimento) un mezzo per cui siano indispensabili appositi scudi (contromisure elettroniche), né caratteristiche che lo rendono scudo a se stesso (tecnologia *stealth*): esso è un oggetto usa-e-getta sacrificabile senza rimpianto alcuno, neppure quello modesto che può essere provocato dalla perdita economica. In questo modo il drone è il più altruistico ed efficace degli scudi perché – tanto che esca indenne dalla missione, quanto che sia costretto dalle (attualmente improbabili) circostanze a sacrificarsi – tutela ben due attori di cruciale importanza. Da un lato il suo pilota, il quale lo guida da una base remota; dall'altro il leader politico dello Stato che risponde all'opinione pubblica nazionale della vita di quel pilota, così come di tutti i piloti e di tutti i soldati che prestano servizio per quello Stato.

Nel nuovo *bellum-duellum* della *war on terrorism* il conto che non torna è quello che riguarda il nemico, nella fattispecie colui che ricorrendo all'azione terroristica ha impugnato l'asimmetria e ora ne viene colpito per mezzo di uno strumento che, anch'esso, poco distingue tra combattenti e non combattenti. Ma è problematica anche la macroscopica asimmetria dei mezzi, che garantisce a una delle due parti l'invulnerabilità di fatto dal momento che l'obiettivo che ha valore (l'uomo) non può essere raggiunto in quanto assente dal campo, mentre l'oggetto che può essere raggiunto è quasi privo di valore. A livello macro la situazione è inquietante in quanto sintetizza plasticamente come poche l'ineguaglianza tra gli emisferi mondiali. A livello micro lo è in quanto annulla totalmente quella comunità di campo (peraltro già svuotata dalla superiorità aerea e dai bombardamenti strategici, per non parlare dell'arma atomica) che pure era stata, per millenni, una caratteristica, un mito e un'ideologia del *bellum-duellum*.

Non è passata inosservata, né tra gli osservatori né all'interno delle forze armate, la crisi che una situazione del genere può indurre nell'auto-rappresentazione del militare, almeno nel modello "istituzione"<sup>6</sup>. Il velivolo che attacca con i suoi missili non ha in cabina un irriducibile patriota giapponese come nel caso degli storici kamikaze: non ha nessuno<sup>7</sup>. O per meglio dire ha

<sup>6</sup> Secondo il sociologo americano Charles C. Moskos, la professione militare si caratterizza per la dicotomia tra il modello "Istituzione", fondato sui valori della tradizione (patriotismo, disciplina, onore, sacrificio) e il modello "Occupazione", basato sui valori del mercato (professionalità, competenza, tutela dei diritti) (Moskos, 1977; 1994). A partire dall'ultimo terzo del XX secolo, peraltro, si è andato affermando un terzo modello, quello "Post-moderno", basato sull'auto-realizzazione individuale (Battistelli, 1997).

<sup>7</sup> Secondo una delle più pessimistiche metafore del rapporto governo/società nel postmoderno, anche nella cabina da cui la politica dovrebbe condurre l'aereo che ci trasporta non c'è un pilota, bensì unicamente una voce registrata (Bauman, 2014).

un operatore che agisce a migliaia di chilometri di distanza, così che chi dovrebbe esserci non c'è (il pilota "vero"), mentre c'è chi *non* dovrebbe esserci (l'operatore del drone). A livello micro-sociale ciò ispira nel primo soggetto un sentimento di colpa a causa della propria assenza (sottrarsi al campo di battaglia è stato a lungo giudicato un comportamento disdicevole per il militare), mentre nel secondo soggetto ispira un sentimento analogo a causa della propria funzione, distante dalla scena ma drammaticamente risolutiva in essa. Dichiarò il professor Deane-Peter Baker, docente di etica presso l'accademia navale degli Stati Uniti: «C'è una sorta di nostalgia per come la guerra era una volta, cioè un nobile conflitto tra cavalieri. I droni sono il segno dell'avvento di una irrevocabile età post-eroica» (cit. in Winright, 2011)<sup>8</sup>.

La decisione se l'immagine umana che appare in video costituisca o meno un target nemico, quindi meritevole del missile da lanciargli addosso, costituisce per l'operatore di droni un'indubbia fonte stressogena. Ne vengono rilevati vari sintomi: l'atteggiamento di estraneazione che può colpire gli operatori di droni armati, detta «mentalità della playstation» (Cole *et al.*, 2010); le sindromi (all'opposto) di stress post-traumatico in seguito a esperienze cruente; l'elevato turn-over degli addetti (Chappelle, *et al.*, 2014). Tutti questi, comunque, rappresentano soltanto costi di natura micro (psicologici e socioculturali) o anche macro (etici), di peso relativo se rapportati ai ben più rilevanti benefici conseguibili a livello macro.

Nella sua sottile analisi circa la funzionalità sociale dei velivoli senza pilota, Bauman parte dalla notazione weberiana secondo cui nella modernità classica (da lui definita "solida") la razionalità scientifica è in grado di indicarci i mezzi ma non i fini della nostra azione, con l'aggravante che oggi, nella modernità "liquida", i mezzi si ergono a indicarci i fini. «All'inizio del XXI secolo – osserva Bauman – la tecnologia militare è riuscita a rendere fluttuante la responsabilità, e dunque a "spersonalizzarla"» (Bauman e Lyon, 2014, 78). Il fatto che missili intelligenti e droni abbiano «preso il posto sia della truppa che delle alte gerarchie dell'apparato militare nell'attività decisionale e nella scelta dei bersagli» ha come conseguenza la neutralizzazione della valutazione morale (tecnicamente detta "adiaforizzazione"). Quando, come accadde nel febbraio 2011, il missile sparato da un velivolo senza pilota uccise ventitré afgani che partecipavano a un matrimonio, gli operatori del drone imputarono l'errore all'ondata di dati, che «traboccarono dallo schermo come da un secchio stracolmo» (Bauman e Lyon, 2014, 78).

<sup>8</sup> Il fatto che i droni abbassino pericolosamente la soglia del conflitto non è un problema – aggiunge Baker confondendo tuttavia lo *ius in bello* con lo *ius ad bellum* – «lo sarebbe se noi non avessimo una giusta causa, ma se l'abbiamo, dovremmo celebrare qualunque cosa ci permetta di conseguire quella giusta causa» (ibidem).

Non è quindi infondato il sospetto che il drone che invia all'operatore un diluvio di informazioni che questi non riesce a processare, svolga una funzione che, per distinguerla da quella "manifesta" (cioè ufficialmente prevista), la sociologia definisce "latente": «esonerare l'operatore dalla colpa morale che lo assillerebbe se avesse pienamente e realmente il potere di scegliere i condannati da giustiziare e, ancor più importante, di rassicurarlo in anticipo sul fatto che se commetterà un errore non sarà accusato di immoralità» (Bauman e Lyon, 2014, p. 77).

La conclusione è che l'avvento dei droni ha determinato cambiamenti epocali. Nell'ambito micro (singoli militari) e meso (le forze armate) sono evidenti le conseguenze che la *post-heroic warfare* determina sulla cultura organizzativa e sull'interpretazione che ne danno i suoi membri. Nell'ambito macro, Bauman constata che lo «'sganciamento' già in atto tra l'opinione pubblica americana e la sua guerra», iniziato con il passaggio dalle forze armate di leva a quelle di mestiere, procederà spedito «verso l'obiettivo di rendere la guerra invisibile alla nazione [...] rendendola [...] più facile e allettante, grazie anche alla quasi totale assenza di danni collaterali e di costi politici» (Bauman e Lyon, 2014, p. 5).

Laddove il sogno prussiano dei soldati-automi tiratori era più che altro una metafora, i droni costituiscono il primo concreto passo per realizzare l'automazione del campo di battaglia. Conseguito lo stadio dell'interconnessione elettronica e del controllo di tiro automatizzato, è già in allestimento, come sempre accade in ambito strategico, lo scenario successivo: la guerra delle armi letali autonome giornalmente note come "robot-killer".

## 1.5. Osservazioni conclusive

Per le implicazioni strategiche, politiche ed etiche che rivestirebbe un campo di battaglia non più soltanto *automizzato* ma addirittura *autonomizzato*, piuttosto che di un sogno si deve parlare di un incubo. Esiste un'arma di difesa in grado di fronteggiare questo incubo? Un'"arma" potenzialmente esiste ed è al di fuori del campo di battaglia. Per paradosso, essa è impugnata dall'attore che, senza averne alcuna intenzione, ha contribuito a generare l'incubo stesso. Questo attore è l'opinione pubblica. È per aggirare la contrarietà dell'opinione pubblica a ledere comunque il diritto alla vita che il governo degli Stati Uniti ha spostato la sua guerra contro il terrorismo dagli «scarponi sul terreno» all'occhio elettronico che scruta e fulmina dal cielo. E che – di pari passo con le altre grandi potenze, a cominciare da Russia e Cina – si appresta a fare irrompere sulla scena macchine dotate di «intelligenza» e «capacità di giudizio» a livello situazionale.

Nello stesso tempo, proprio dall'opinione pubblica – in particolare dalla più ascoltata, quella occidentale e americana – può provenire un freno a questo abuso della tecnologia. Impersensibili al sacrificio di vite umane 'proprie', i cittadini non sono neppure completamente indifferenti agli spargimenti di sangue quando colpiscono esseri umani "altri", specialmente se ciò accade ad opera di armi provenienti dalla propria madrepatria<sup>9</sup>.

In questa nuova sensibilità risiede la forza di quella che, al culmine delle mobilitazioni contro la guerra a Saddam, alla vigilia dell'invasione dell'Iraq, il *New York Times* ha definito la nuova «superpotenza» internazionale, ossia l'opinione pubblica. Ancora negli anni '50 e '60 del XX secolo, questa entità veniva descritta come volatile, disinformata e sostanzialmente indifferente di fronte ai grandi temi politici, specialmente a quelli di carattere internazionale, in quanto remoti rispetto alle conoscenze e agli interessi dell'«uomo della strada» (Isernia, 1996). Ancora oggi nelle società tradizionali l'opinione pubblica riveste un ruolo marginale e subordinato alle strategie del potere politico e all'influenza del credo religioso. Tuttavia parallelamente ai processi di modernizzazione e di sviluppo economico, al rafforzamento dei mezzi di comunicazione e alla crescita dell'autonomia individuale, anche i cittadini delle società tradizionali mostrano una maggiore propensione a "intromettersi" in questioni non esclusivamente pertinenti all'utilità e alla sopravvivenza immediata del singolo individuo e della sua famiglia.

Le analisi delle scienze sociali rilevano la graduale emersione di un pubblico coerente e capace di confrontarsi anche con gli eventi che provengono da un ambito "esotico" come quello della politica internazionale (Everts e Isernia, 2001). Che gli individui formino le proprie opinioni a partire dai fattori biologici, comunicazionali, ideologici e soprattutto culturali che li caratterizzano non esclude che essi possano modificare tali opinioni nel tempo. Con il declinare delle ideologie, nella post-modernità occidentale la propensione a cambiare idea viene valutata positivamente. Quella che ancora cinquant'anni fa era connotata negativamente come "volatilità", oggi tende a essere letta come flessibilità e libertà di giudizio, cioè come capacità del pubblico di adattare il proprio pensiero alle diverse situazioni, subordinandolo molto meno che in passato ai vincoli culturali, politici e religiosi di partenza.

Nell'attuale scenario strategico, il già instabile equilibrio offesa/difesa, pesantemente condizionato dall'avvento di armi semi-autonome come i droni, con l'ulteriore ingresso di quelle autonome segnerebbe un mutamento di paradigma nella conduzione dei conflitti, con irreparabili conseguenze sul piano etico, giuridico e comportamentale, oltre che operativo. In questo, come in altri casi, l'unica misura in grado di fermare questo piano inclinato è la messa al

<sup>9</sup> V. oltre, cap. 6.

bando delle LAWS. Viceversa l'introduzione delle medesime, in una qualsiasi loro versione, innescherebbe un processo imitativo inarrestabile.

C'è da sperare che da parte della specie umana prevalga l'istinto di conservazione; piuttosto che quello della massimizzazione della funzione di utilità (o meglio di quella che si crede la funzione di utilità del proprio paese), ancora più esiziale quando ci si sposta dal mercato alla forza delle armi. Del resto l'intera questione della intelligenza artificiale richiede un surplus di prudenza e di saggezza in tutti gli ambiti in cui verrà applicata. Da anni gli scienziati sociali – economisti, sociologi, psicologi – si interrogano sulla fine del lavoro umano (Rifkin, 2005; Falcone, *et al.*, 2018; Lane e Saint-Martin, 2021), spiazzato dal lavoro delle macchine, in particolare dal possibile ruolo delle macchine «intelligenti» (Ford, 2015).

Come osservava Herbert Simon (1985, cit. in Veltri, 2018, p. 534), «che siano gli uomini o le macchine ad essere impiegati in un particolare processo, non dipende semplicemente dalla produttività relativa in termini fisici, ma altresì dal loro costo. E il costo dipende dal prezzo». Poiché quello della vita umana è il prezzo più elevato da pagare, è un paradosso che per risparmiare le vite umane *proprie* si consenta a una macchina di annientare le vite degli *altri*. Innegabilmente in guerra i dispositivi automatici “costerebbero” di meno e quindi la tendenza “economica” sarebbe quella di farvi ricorso. Tuttavia, se in determinate circostanze un contingente di robot non si contrapponesse a un contingente di altri robot (come nella situazione simmetrica dal forte al forte), bensì ad esseri umani (nella situazione asimmetrica dal forte al debole), lo scenario diventerebbe apocalittico e le sue conseguenze inimmaginabili per la nostra specie.

## Riferimenti bibliografici

- Abrahamsson B. and Ydén K. (2005), *Organizations, Co-ordinated Actions and Network Based Defence*, in Ydén, ed. *Directions in Military Organizing*, Försvarshögskolan, Stockholm: 169-184.
- Battistelli F. (1997), “Peacekeeping and the Postmodern Soldier”, *Armed Forces and Society*, vol. 23, n. 3: 467-483.
- Battistelli F. (2004), *Gli italiani e la guerra: tra senso di insicurezza e terrorismo internazionale*, Carocci, Roma.
- Battistelli F., Galantino M.G., Lucianetti L.F., Striuli L. (2012), *Opinioni sulla guerra. L'opinione pubblica italiana e internazionale di fronte all'uso della forza*, FrancoAngeli, Milano.
- Battistelli F. e Galantino M.G. (2019), “Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk”, *Current Sociology*, vol. 67(1), 2019: 64-78.



- Bauman Z. (2005), *Il teatro dell'immortalità. Mortalità, immortalità e altre strategie di vita*, tr. it. il Mulino, Bologna.
- Bauman Z. (2014), *La solitudine del cittadino globale*, tr. it. Milano, Feltrinelli.
- Bauman Z. e Lyon D. (2014), *Sesto potere. La sorveglianza sulla modernità liquida*, tr. it. Laterza, Roma-Bari.
- Bobbio B. (1984), *Il problema della guerra e le vie della pace*, Bologna, il Mulino.
- Burk J., a cura di (1998), *La guerra e il militare nel nuovo sistema internazionale*, tr. it. FrancoAngeli, Milano.
- Chappelle W., Goodman T., Reardon L., Thompson W. (2014), "An analysis of post-traumatic stress symptoms in United States Air Force drones operators", *Journal of Anxiety Disorders*, 28: 480-487.
- Carruthers S. (2014) *Casualty Aversion: Media, Society and Public Opinion*, in Scheipers, 2014: 162-187.
- Cole C., Dobbing M., Hailwood A. (2010), *Convenient Killing: Armed Drones and the 'playstation' Mentality*, Fellowship of Reconciliation (GB), testo disponibile al sito: <https://www.for.org.utk/act/campaign>.
- Csernatoni R. (2016), "Defending Europe: dual-use technologies and drone development in the European Union", *Royal Higher Institute for Defence*, Bruxelles, Focus Paper, n. 35.
- Douhet G. (1921), *Il dominio dell'aria e altri scritti*, in L. Bozzo, a cura di, *Aeronautica militare*, Ufficio storico, Roma, 2002.
- Elias N. (1982), *La civiltà delle buone maniere*, tr. it. il Mulino, Bologna.
- Everts Ph. e Isernia P., a cura di (2001), *Public Opinion and the International Use of Force*, Routledge, London.
- Falcone R., Capirci O., Lucidi F., Zoccolotti P. (2018), "Prospettive di intelligenza artificiale: mente, lavoro e società nel mondo del machine learning", *Giornale Italiano di psicologia*, XLV, n. 1: 43-68.
- Ford M. (2017), *Il futuro senza lavoro. Accelerazione tecnologica e macchine intelligenti*, tr. it. il Saggiatore, Milano.
- Foucault M. (1976), *Sorvegliare e punire. Nascita della prigione*, tr. it. Einaudi, Torino.
- Giacomello G. e Coticchia F. (2007), "In Harm's Way: Why and When a Modern Democracy Risks the Lives of Its Uniformed Citizens", *European Security*, vol. 16, n. 2, pp. 163-182.
- Gorer G. (1965), *Death, grief and mourning in contemporary Britain*, Crescent Press, London.
- Hayes B. et al. (2014), *Eurodrones Inc*, Statewatch and Transnational Institute, Amsterdam-London.
- Isernia P. (1996), *Dove gli angeli non mettono piede. Opinione pubblica e politiche di sicurezza in Italia*, FrancoAngeli, Milano.
- Kagan R. (2004), *Il diritto di fare la guerra. Il potere americano e la crisi di legittimità*, tr. it. Mondadori, Milano.
- King A. (2010), "The Afghan War and 'postmodern' memory: commemoration and the dead of Helmand", *The British Journal of Sociology*, vol. 61, 1: 1-25.
- Krishnan A. (2009), *Killer Robots. Legality and Ethicality of Autonomous Weapons*, Ashgate.

- Lane M. and Saint-Martin A. (2021), *The Impact of Artificial Intelligence on the Labour Market: What do we know so far?*, OECD Social, Employment and Migration Working Papers 256, OECD Publishing.
- Luttwak E.N. (1994), "Where are the great powers? At home with the kids", *Foreign Affairs*, 73, n. 4, July-August: 23-28.
- Maddox R.J. (2004), *Weapons for Victory; the Hiroshima Decision Fifty Years Later*, University of Missouri Press, Columbia.
- Marx K. and Engels E. (1974), *Opere di Marx ed Engels*, tr. it. Editori Riuniti, Roma, 1974, vol. XLII.
- Morgenthau H.J. (1997), *Politica tra le nazioni. La lotta per il potere e la pace*, il Mulino, Bologna [1948].
- Moskos C.C. (1977), *Sociologia e soldati*, tr. it. FrancoAngeli, Milano.
- Moskos C.C. (1994), "From Institution to Occupation: Trends in Military Organization", *Armed Forces and Society*, vol. 4, n. 1: 41-50.
- Nye J.S. (2005), *Soft power. Un nuovo futuro per l'America*, tr. it. Einaudi, Torino.
- PAX (2019), *Military Drones and the EU*, testo disponibile al sito: <http://info@pax-forpeace.nl>.
- Quester G.H. (2005), "Demographic Trends and Military Recruitment: Surprising Possibilities", *The U.S. Army War College Quarterly: Parameters*, vol. 35, n. 1: 27-40.
- Rifkin J. (2005), *La fine del lavoro*, tr. it. Mondadori, Milano.
- Rogers A.P.V. (2000), "Zero-casualty Warfare", *International Review of The Red Cross*, n. 837.
- Scheipers S. (2014), *Heroism and the Changing Character of War. Toward Post-heroic Warfare?*, Palgrave Macmillan, Basingstoke.
- Sifton J. (2012), "A brief history of Drones", *The Nation*, 9 february.
- Simon H. (1985), "The Corporation: will it be managed by machines?", in M. Anshen e G.L. Bach, eds., *Management and Corporations*, McGraw Hill, New York: 17-55.
- Veltri F. (2018), "Dalla piramide alla clessidra. Verso una nuova divisione del lavoro sociale?", in A. Cipriani, A. Gramolati, G. Mari, a cura di, *Il lavoro 4.0. La Quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, Firenze.
- Walker J.S. (2005), "Recent Literature on Truman's Atomic Bomb Decision: a Search for a Middle Ground", *Diplomatic History*, 29, n. 2: 311-334.
- Westmoreland W.C. (1969), *Address by general W.C. Westmoreland, chief of staff*, U.S. Army, Washington D.C., 14 October 1969, Congressional Record, U.S. Senate, 16 October 1969.
- Winright T. (2011), *Deliberating on Drones and just War*, testo disponibile al sito: [www.catholicmoral-theology.com/deliberating-on-drones-and-just-war](http://www.catholicmoral-theology.com/deliberating-on-drones-and-just-war).

## *2. Caratteristiche, prospettive e problematicità dell'Intelligenza Artificiale*

di *Diego Latella, Gian Piero Siroli, Guglielmo Tamburrini*

### **2.1. Introduzione**

La IA nasce ufficialmente nell'estate del 1956 quando John McCarthy, uno dei padri di quella che lui stesso avrebbe chiamato "Artificial Intelligence", all'epoca giovane assistente alla cattedra di matematica al Dartmouth College ad Hanover (Stati Uniti), organizzò il Dartmouth Summer Research Project on Artificial Intelligence, un workshop al quale parteciparono molti pionieri della IA, come Marvin Minsky, Herbert Simon e Allen Newell, e altri eminenti scienziati come Claude Shannon e Nathaniel Rochester<sup>1</sup>. L'obiettivo del workshop era quello di chiarire e sviluppare concetti e idee sulle cosiddette "thinking machines".

A tutt'oggi, però, non si è pervenuti a una definizione soddisfacente di IA; in questa sede utilizziamo quella – in un certo senso riduttiva – proposta dall'UNIDIR, secondo cui: «[l']intelligenza artificiale è il campo di studi dedicato a rendere intelligenti le macchine. L'intelligenza misura la capacità di un sistema di determinare la migliore linea d'azione per raggiungere i propri obiettivi in una vasta gamma di ambienti» (UNIDIR, 2018, p. 2, trad. it. a cura degli autori).

In pratica, molti ricercatori nel campo della IA, piuttosto che affrontare il problema di una definizione teorica completa della disciplina, preferiscono darle una caratterizzazione ottenuta indirettamente, attraverso gli sviluppi tecnologici della stessa. È così che l'avanzamento delle conoscenze di IA avviene realizzando delle macchine capaci di risolvere autonomamente specifici problemi la cui soluzione necessita di una certa dose di "intelligenza". Così, nel 1952, un computer è riuscito a vincere a tris, nel 1994 fu il turno della dama, quindi degli scacchi nel 1997, fino allo sviluppo, nel 2014, di

<sup>1</sup> Si veda, ad esempio (Franklin, 2014).

programmi capaci di giocare e vincere sugli umani a vari giochi quali Atari, Go (2016) e poker (2017).

Un effetto secondario di questa tendenza è che solo le macchine più all'avanguardia vengono considerate “intelligenti”: ad esempio, negli anni '60 venivano considerate intelligenti le macchine capaci di giocare a scacchi, mentre oggi queste macchine vengono considerate dei semplici programmi informatici più o meno efficienti. Con il passare degli anni, la “intelligenza” delle macchine si è spostata venendo associata a compiti che noi riteniamo più complessi o creativi, come, per esempio, il gioco del Go. In altri termini, ciò che accade è che la capacità di risolvere un certo problema viene considerata espressione di intelligenza solo fino a quando non viene realizzata una macchina capace di trovare una risposta.

In ogni caso, le tecnologie della IA, e in particolare di quella branca della IA che va sotto il nome di *machine learning*, sono state applicate con notevole successo in vari domini, che vanno dal riconoscimento di immagini, della voce e del linguaggio naturale, alla traduzione automatica fra lingue (umane), all'aggregazione e analisi di immense quantità di dati (*data analytics* e *data science*) con fini predittivi o di diagnosi e al controllo di sistemi autonomi, come i veicoli a guida autonoma. Infine, sistemi di IA hanno sempre suscitato particolare interesse in ambienti militari (Din, 1986; Andride, 1987) e le applicazioni della IA in questo contesto vanno dai sistemi C3IR (Command, Control, Communication, Intelligence and Reconnaissance), a quelli di supporto alle decisioni, fino ad arrivare alle armi autonome<sup>2</sup>.

Accanto agli aspetti puramente tecnologici citati fino adesso e che costituiscono argomento di primario interesse nel contesto di questo libro, la IA come disciplina squisitamente scientifica ha visto e vede tuttora sviluppi concettuali e teorici di altissimo livello. Tra questi si annoverano la creazione e lo studio di modelli teorici per la rappresentazione della conoscenza, sia per la pianificazione (*planning*) e l'apprendimento (sul quale ci soffermeremo più in dettaglio più avanti) sia per la *explainability* – intesa come la “capacità di fornire spiegazione” – dei procedimenti computazionali e logici che portano ai risultati generati da sistemi di IA, così come sistemi logico-deduttivi per il ragionamento automatico, che fondano le proprie radici, anche storiche, nella logica matematica e nella teoria della calcolabilità. Lo studio di questi ultimi ha permesso di sviluppare, ad esempio, dimostratori automatici di teoremi. Molte classi di logiche sviluppate o utilizzate nell'ambito della ricerca di base sulla IA, come le logiche epistemiche (van

<sup>2</sup> Si veda, fra gli altri: (USDOD, 2016), (Allen e Chan, 2017), (Boulanin e Verbruggen, 2017), (Cummings, 2017), (Dyndal *et al.*, 2017), (Amoroso *et al.*, 2018), (CRS, 2018), (UNIDIR, 2018), (Rossi, 2019).

Ditmarsch *et al.*, 2015), temporali (Emerson, 1990), o spaziali (Aiello *et al.*, 2007) sono specializzazioni della logica modale (van Benthem e Blackburn, 2006), un campo di proficua ricerca nell'ambito della logica matematica.

Infine, è necessario citare lo studio e lo sviluppo della cosiddetta *swarm intelligence*, un paradigma utilizzato anche in ambito IA, nel quale vengono sviluppati algoritmi ispirati dal comportamento di popolazioni di agenti biologici, come colonie di insetti, stormi di uccelli o banchi di pesci. In questo caso, ogni singolo agente segue regole comportamentali e di interazione estremamente semplici che, però, danno origine a interessanti proprietà emergenti della popolazione al punto tale che quest'ultima, nell'insieme, può risolvere in maniera estremamente efficace ed efficiente problemi di notevole complessità.<sup>3</sup> Un'interessante area di ricerca e sviluppo collegata anche alla *swarm intelligence* è quella della *swarm robotics*, nell'ambito della quale si studiano e sviluppano “sciame” di sistemi robotici, i quali hanno la capacità di coordinare le loro azioni per operare collettivamente per il raggiungimento di un obiettivo condiviso. Ogni individuo dello sciame è pensato e realizzato come entità autonoma, che reagisce ai vari stimoli in base a sue regole interne. Lavorando come un gruppo, lo sciame può eseguire compiti sia semplici che complessi, che un singolo robot non sarebbe in grado di svolgere (Ekelof e Persi Paoli, 2020).

## 2.2. Machine Learning

Fra le tecniche sviluppate nell'ambito della IA per scopi civili, quelle di *Machine Learning* (ML), su cui ci concentreremo nel resto del capitolo, hanno riscosso particolare successo negli ultimi anni. Questo successo è in parte dovuto alla incredibile quantità di dati disponibili su svariati aspetti del problema che, di volta in volta, si vuole affrontare e alla grande capacità di calcolo oggi realizzabile. La disponibilità di dati è, a sua volta, conseguenza della diffusione di sensori accessibili a basso costo, che possono monitorare praticamente qualunque aspetto fisico e sociale del pianeta e che vanno dai sensori ad hoc dedicati al monitoraggio di particolari fenomeni fisici, ai dispositivi elettronici di uso comune come gli smartphone, i tablet e, con l'avvento dell'*Internet of Things* (IoT)<sup>4</sup>, tutti i più comuni elettrodomestici, i mezzi di trasporto e, più in generale, le infrastrutture (regionali, nazionali e urbane).

Il ML rappresenta un paradigma duale rispetto all'informatica tradizionale,

<sup>3</sup> Si veda, ad esempio, la rivista scientifica specializzata *Swarm Intelligence*, Dorigo, M. (Ed. in Chief), Springer, Berlin, D.

<sup>4</sup> Si veda, ad esempio (USGAO, 2017a); per le questioni di sicurezza sollevate dall'avvento dell'*Internet of Things* si suggerisce (Schneier, 2018).

ma anche alla IA “tradizionale” (a volte indicata dall’acronimo “GOFAI”: *Good Old-Fashioned Artificial Intelligence*). Entrambe queste ultime, per definizione hanno come obiettivo la soluzione di problemi che, per loro stessa natura, risultano difficili per gli umani, ma sono di facile automazione e quindi relativamente semplici per le macchine, ad esempio perché ripetitivi e basati su regole di inferenza logica. Viceversa, il ML è una disciplina che cerca di affrontare e risolvere quei problemi che, invece, non sono facilmente descrivibili in termini di regole logiche, né necessariamente ripetitivi e che, spesso, risultano “semplici” per gli umani, come, ad esempio, riconoscere gli oggetti che compongono una scena della vita comune (Goodfellow *et al.*, 2016).

In altri termini, mentre le attività cognitive di alto livello, come ad esempio il ragionamento, possono essere, entro certi limiti, ricreate artificialmente utilizzando le tecniche tipiche della GOFAI, quelle di livello più basso, più assimilabili all’apprendimento umano dei primi anni di vita, sono più facilmente simulabili utilizzando tecniche di ML, a patto che si abbiano dati di alta qualità e potenza di calcolo sufficienti.

Il ML è una disciplina che vede integrati aspetti e risultati scientifici dell’informatica, della statistica e dell’algebra lineare, con intuizioni provenienti da altre discipline, come le neuroscienze. La caratteristica fondamentale delle tecniche di ML è che, a differenza delle altre tecniche tipiche dell’informatica, esse affrontano il problema di programmare i computer a “imparare” partendo dai dati e dall’esperienza (Buchanan e Miller, 2017).

Gli utilizzi principali del ML includono quelli di classificazione, quelli di strutturazione di dati originariamente non strutturati e di riconoscimento di pattern. Fra i principali domini di applicazione vanno ricordati: la *computer vision*, cioè la capacità di un computer di riconoscere e identificare specifici oggetti in una immagine; l’elaborazione del linguaggio naturale, come la traduzione automatica da una lingua ad un’altra; la IoT, dove i dispositivi di uso comune possono apprendere le abitudini e le limitazioni degli utilizzatori facilitandone quindi l’uso; il supporto al design e alla ricerca scientifica, dove sistemi artificiali di supporto intelligenti possono (aiutare a) ideare soluzioni innovative; i sistemi medicali, dove sottosistemi di IA – per esempio sistemi di riconoscimento di immagini – possono fornire un valido supporto sia in fase di diagnosi che in fase di definizione delle terapie (come nella segmentazione propedeutica alla radioterapia); i sistemi di trasporto, sia per quanto riguarda gli aspetti di controllo del traffico che in relazione allo sviluppo di veicoli a guida autonoma; i sistemi di supporto ai procedimenti giudiziari, come quelli di polizia predittiva; i sistemi militari, sia come (sottosistemi di) sistemi di supporto alle decisioni, sia come componenti di armi autonome.

Le fasi di una tipica procedura di ML sono quattro:



1. *programmazione*, cioè la definizione, progettazione e implementazione di una procedura software<sup>5</sup> con la quale si istruisce un computer a “imparare” a partire da un insieme di dati (*training data set*);
2. *allenamento* (training), che consiste nell’esecuzione del programma di cui al punto precedente su un *training data set* al fine di impostare e calibrare i (molti) parametri presenti nel programma; il *training data set* è costituito da dati che possono – ma non necessariamente devono – essere “etichettati”, come vedremo più avanti;
3. *testing* del programma calibrato al punto precedente, e cioè esecuzione controllata dello stesso, su un altro insieme di dati – il *testing data set* – e relativa analisi dei risultati al fine di valutarne la qualità;
4. Infine, se la fase precedente viene completata con una valutazione positiva, l’uso del programma calibrato su nuovi dati, diversi da quelli di training e da quelli di testing.

Se la terza fase non si conclude positivamente, si dovrà invece procedere a ulteriori fasi di training ed eventualmente rivedere anche le scelte di progettazione o di acquisizione adottate nella fase di programmazione. Va notato subito che, a seconda del tipo di approccio al ML che si è scelto, è possibile che attività di training abbiano luogo anche durante l’uso del programma.

Si possono identificare vari tipi di ML, fra i quali il *supervised ML*, l’*unsupervised ML*, il *reinforcement learning* e il *deep learning*. Caratteristica principale del *supervised ML* è il fatto che il *training data set* è costituito da dati etichettati, ovvero ogni dato nel data set è accompagnato da un’“etichetta” che lo descrive e che, di norma, è creata manualmente. Facciamo un semplice esempio: uno degli usi del ML è quello del riconoscimento di testi scritti a mano (e la loro trascrizione in testo basato su un insieme di caratteri standard). Se, per semplicità, ci limitiamo al riconoscimento di cifre numeriche da 0 a 9 scritte a mano, possiamo immaginare il training data set come una grande tabella, ogni riga della quale è costituita da due campi: uno contiene un’immagine di una cifra manoscritta e l’altro l’etichetta, cioè la sua trascrizione; in figura 1 riportiamo una minima parte di una simile tabella, con due immagini diverse del numero 3 scritto a mano, ma entrambe associate al carattere “3”:

<sup>5</sup> Naturalmente, spesso è possibile sostituire questa fase con una di semplice “acquisizione” del software, sia dal mercato che attraverso l’uso di prodotti *freeware*.

Fig. 1 – Un frammento di training data set per il riconoscimento delle cifre scritte a mano

Immagine	Etichetta
	3
	3

Il *training data set* viene usato dal programma di ML per impostare e, soprattutto, calibrare i parametri caratteristici del particolare modello computazionale di ML selezionato per l'utilizzo nell'applicazione d'interesse. Esistono svariati modelli computazionali per il *ML supervised*, che vanno, solo per citarne alcuni, dalla semplice regressione lineare, alle *Support Vector Machines (SVM)*, alle reti neurali (Goodfellow *et al.*, 2016). Caratteristica comune a tutti questi modelli computazionali è il fatto di essere fortemente parametrizzati. Il “training” consiste nell'esecuzione di procedure, tipicamente iterative, per fissare i valori di questi parametri e calibrare questi ultimi per affinamenti successivi. La calibratura dei parametri deve evidentemente essere guidata da un qualche criterio che il programma di ML deve seguire; questo criterio è rappresentato tipicamente da una funzione di costo da minimizzare. Quest'ultima, in buona sostanza, rappresenta l'errore che, a seguito di una certa impostazione dei parametri, la macchina può commettere nel classificare o riconoscere i dati e che, quindi, va minimizzato. In ultima analisi, quindi, l'operazione di training altro non è che la soluzione di un problema di minimizzazione di una certa funzione matematica.

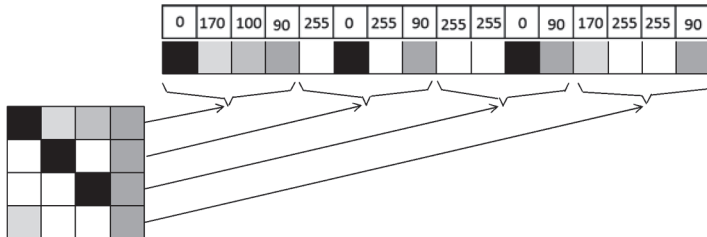
Implicito in quanto appena detto è il fatto che si abbiano rappresentazioni numeriche degli oggetti sui quali si fa ML. Ad esempio, nel caso di riconoscimento di oggetti in immagini, per semplicità in bianco e nero, la rappresentazione digitale dell'immagine è una matrice numerica bidimensionale di pixel<sup>6</sup>, ciascuno dei quali è portatore di un valore numerico che identifica l'intensità luminosa del pixel stesso; questa matrice, a sua volta, può essere rappresentata come un vettore numerico – cioè una sequenza di numeri – di dimensione pari al numero totale di pixel dell'immagine. Solo a titolo di esempio, in figura 2 riportiamo una piccola matrice di 16 pixel (4 x 4) (nei sistemi reali, si hanno matrici con migliaia o milioni di pixel!) e la sua rappresentazione come vettore, dove le righe della matrice sono semplicemente giustapposte, una a fianco all'altra. In realtà, il vettore contiene dei numeri,

<sup>6</sup> Il pixel è l'elemento più piccolo indirizzabile e controllabile di una immagine rappresentata nello schermo di un computer.



che vanno da 0, corrispondente al nero (intensità minima), a 255, corrispondente al bianco (intensità massima), come rappresentato dal vettore numerico collocato nella parte superiore della figura.

Fig. 2 – Esempio di rappresentazione numerica di immagini



Quindi, un'immagine digitale è rappresentata da un vettore numerico. Esso rappresenta l'input del modello computazionale, il cui output può a sua volta essere un vettore, ad esempio con tanti elementi quanti sono gli oggetti diversi che si vogliono identificare, nel quale ogni elemento fornisce la probabilità che una data immagine in input contenga un certo specifico oggetto.

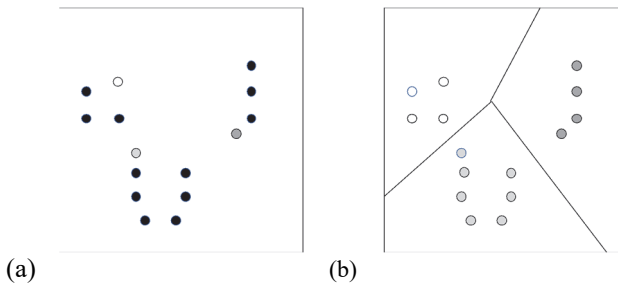
Il *ML unsupervised*, invece, viene usato tipicamente quando non si ha a disposizione dei training data set etichettati. In questo caso, sono gli algoritmi stessi che, ricevendo come input un (grande) insieme di dati non strutturato, cercano di identificare in esso dei pattern o una qualche struttura. Un esempio di questo tipo è il metodo “k-means clustering”: dato uno spazio multidimensionale, l'algoritmo lo ripartisce in  $k$  sottoinsiemi, ciascuno rappresentato dal suo centroide<sup>7</sup>, in modo tale che sia minimizzata la distanza fra ogni punto e il centroide del suo sottoinsieme di appartenenza (Buchanan e Miller 2017). La figura 3 mostra un esempio di applicazione dell'algoritmo di k-means, per  $k=3$ : in questo caso, vengono inizialmente scelti (di solito in modo casuale) 3 punti, rappresentati dai tre tondini in bianco, grigio chiaro e grigio scuro nella figura 3(a). L'algoritmo, procedendo in modo iterativo produce una partizione dell'insieme di tutti i punti secondo il criterio sopra indicato, mostrata in figura 3(b), dove ogni punto è colorato con lo stesso livello di grigio del centroide del suo insieme di appartenenza; come si può facilmente notare, ogni punto di un dato colore è più vicino al centroide dello stesso colore di quanto non lo sia ai centroidi di colore diverso.

Questa tecnica consente quindi di aggregare i dati di un certo insieme attorno ai  $k$  centroidi e quindi può risultare utile in quelle applicazioni che

<sup>7</sup> Il centroide di un insieme di punti in uno spazio multidimensionale è il punto che rappresenta la *media* dei punti nell'insieme; in altri termini, ogni coordinata del centroide è la media dei valori della stessa coordinata dei punti dell'insieme.

richiedono classificazioni dei dati come, ad esempio, l'identificazione di cellule cancerogene in un campione di tessuto, il clustering di parole con significati simili, le analisi di mercato o addirittura l'identificazione di mine in un campo di battaglia (Landman *et al.*, 2019).

Fig. 3 – Esempio di applicazione dell'algoritmo di *k-means*, con  $k=3$



Infine, uno degli usi più comuni del *ML unsupervised* è quello di scoprire una qualche struttura in insiemi di dati per poter poi utilizzare la conoscenza acquisita sulla struttura nella progettazione di sistemi di *ML supervised*.

Nel caso del *reinforcement learning* un agente artificiale (un programma in esecuzione su uno o più computer) può “imparare” semplicemente interagendo con il suo ambiente. Tipicamente l’agente esegue un’azione, in maniera conforme a certe regole, ne “osserva” (tramite opportuni sensori) l’effetto sull’ambiente e quindi determina se l’azione è stata di aiuto per il raggiungimento degli obiettivi dell’agente. L’ambiente può anche essere costituito dall’agente stesso: è questo il metodo utilizzato da AlphaZero per imparare a giocare a Go e ad altri giochi (Buchanan e Miller, 2017; UNIDIR, 2018).

Infine, il *deep learning* può essere pensato, in termini generali, come un insieme di tecniche “architetturali” attraverso le quali vengono combinate varie tipologie di ML, sia *supervised* che *unsupervised*, per l’estrazione di caratteristiche rilevanti dei dati in input e per l’apprendimento attraverso livelli multipli di rappresentazione, che corrispondono a diversi livelli di astrazione e che quindi formano una gerarchia di concetti. Ad esempio, il *deep learning* può combinare un processo *unsupervised* per apprendere le caratteristiche dei dati sottostanti, come i bordi di un viso, e quindi fornire tali informazioni a un algoritmo di apprendimento *supervised* per riconoscere le caratteristiche e produrre il risultato finale, come identificare correttamente una persona in una foto (Buchanan e Miller, 2017).

## 2.3. Limiti e problematicità del *Machine Learning*

È innanzitutto opportuno premettere che i sistemi di IA, inclusi quindi quelli di ML, sono costituiti da programmi in esecuzione in computer progettati e costruiti con tecnologie sostanzialmente tradizionali<sup>8</sup>. Di conseguenza, i sistemi di IA sono vulnerabili a tutti gli attacchi cibernetici che sfruttano le vulnerabilità dei normali sistemi informatici, come è meglio descritto nel Capitolo 3 di questo libro.

Bisogna poi sottolineare che il comportamento di un sistema di ML (*supervised*) durante la fase di uso dipende fortemente dalla qualità dei dati e delle procedure di training. Da tale qualità dipende anche la possibilità di evitare che la macchina, durante l'uso, esibisca dei pregiudizi (*bias*).

La creazione di *bias* nella fase di training può dipendere dal fatto che il sistema di ML abbia eseguito un addestramento poco accurato, cioè su dati che non rappresentano bene la popolazione di oggetti sui quali la macchina viene usata; oppure dal fatto che il training sia stato anche molto accurato, ma svolto su dati a loro volta distorti (*biased*); oppure, semplicemente, dal fatto che il sistema non sia stato sufficientemente addestrato (Buchanan e Miller, 2017).

La presenza di *bias* è un problema particolarmente insidioso:

Nel peggiore dei casi, l'apprendimento automatico può nascondere discriminazioni con l'imprimatur della scienza. Ad esempio [...] una facoltà di medicina britannica ha usato un algoritmo che scartava candidati qualificati di sesso femminile o provenienti da minoranze perché era stato addestrato sulle decisioni prese in precedenza da una commissione di valutazione non imparziale. Un'indagine di ProPublica ha rilevato che un algoritmo sviluppato dalla società Northpointe, Inc. per fornire un punteggio di valutazione del rischio [di supporto] per i giudici [nell'emissione di una] condanna era distorto rispetto alla razza e inaccurato. Gli afroamericani avevano molte più probabilità di essere etichettati come "ad alto rischio", ma [...] gli afroamericani che erano stati etichettati come "ad alto rischio" avevano [di fatto] molte meno probabilità di commettere un altro crimine rispetto ai bianchi "ad alto rischio" (Buchanan e Miller, 2017, p. 32, trad. it. a cura degli autori).

È quindi di estrema importanza poter disporre di grandi quantità di dati di alta qualità e di procedure di training altrettanto affidabili. Questo non sempre è possibile e, soprattutto, è particolarmente difficile per alcuni

<sup>8</sup> Va però detto che cominciano ad essere prodotti dei dispositivi hardware progettati e sviluppati appositamente per applicazioni di IA come il Tensor Processing Unit, un circuito integrato per reti neurali di Google (<https://cloud.google.com/tpu/docs/tpus>, accesso effettuato il 1 settembre 2022).

domini di applicazione; primi, fra questi, sono quelli collegati al campo di battaglia, soggetti, per definizione, alla *fog of war*.

È inoltre fondamentale sottolineare come dato un certo problema, per esempio, di classificazione, diversi algoritmi e modelli computazionali possono dare risultati abbastanza diversi; al riguardo, si rimanda a Buchanan e Miller (2017) e agli esempi mostrati nel sito scikit-learn<sup>9</sup> (Pedregosa *et al.*, 2011).

Se l'uso di tecniche di ML può dunque costituire un utile supporto per il decision-making (dando ad esempio delle indicazioni “di massima” su come classificare oggetti, scenari o situazioni di interesse), affidarsi a tali tecniche come unico strumento decisionale può risultare estremamente rischioso, per lo meno all'attuale stato dell'arte.

È inoltre importante sottolineare come ogni particolare modello computazionale ha i suoi punti di forza e i suoi punti deboli; di conseguenza i professionisti del ML devono spesso provare più di un modello/algoritmo per determinare quale, fra essi, risponda meglio alle esigenze poste dal problema da risolvere (Buchanan e Miller, 2017). La scelta di uno specifico modello/algoritmo di ML è tutta nelle mani degli esperti di ML e la sua adeguatezza dipende dalle loro specifiche competenze nell'ambito sia del ML che dominio di applicazione.

Anche in questo caso, quindi, risulta difficile pensare che sistemi di IA, costruiti secondo le conoscenze e le tecnologie all'attuale stato dell'arte, possano essere utilizzati per l'esecuzione di funzioni militari critiche, come decisioni autonome – cioè senza alcun significativo controllo umano – relative alla vita e la morte di avversari. Questo non solo per ragioni di natura etica e di diritto umanitario internazionale, come discusso nei Capitoli 5 e 9 del libro, ma anche sulla base di considerazioni tecniche.

Infine, nei sistemi di *ML supervised* (poiché, come si è visto, il training di un modello consiste nella calibrazione dei suoi parametri effettuata in maniera automatica, con iterazioni guidate da un'enorme quantità di dati nella fase di uso della macchina) risulta praticamente impossibile alla mente umana – incluse quelle degli stessi programmatori della macchina – comprendere perché, dato un certo input, essa produca uno specifico risultato: queste tecniche, quindi, producono sistemi di IA che vanno utilizzati come delle vere e proprie black box.

Questa caratteristica è particolarmente importante ed è anche molto critica per via del fatto che, purtroppo, i sistemi di ML a volte, ed in maniera non facilmente predicibile, producono risultati errati e totalmente inaspettati.

<sup>9</sup> [https://scikit-learn.org/stable/auto\\_examples/classification/plot\\_classifier\\_comparison.html](https://scikit-learn.org/stable/auto_examples/classification/plot_classifier_comparison.html) (accesso effettuato il 26 gennaio 2022).

Per esempio, sono stati effettuati degli esperimenti nell'area del riconoscimento automatico delle immagini in cui si è visto che leggere perturbazioni dei valori dei pixel dell'immagine di input, del tutto irrilevanti per gli umani, inducono la macchina a clamorosi errori, come quello di classificare l'immagine di uno scuolabus come se fosse quella di uno struzzo (Klarreich, 2016; Edwards, 2019; Open AI, 2019); analogamente, il sistema di riconoscimento può fallire facilmente se si agisce direttamente sugli oggetti da riconoscere nello spazio reale, del quale viene sottoposta al sistema un'immagine, per esempio una foto (Thys *et al.*, 2019).

È evidente che comportamenti e situazioni come quelli ai quali si è accennato sopra non possono essere tollerati per (sotto-)sistemi impiegati per lo svolgimento di funzioni critiche, come quelle di selezione e abbattimento del bersaglio da parte di future armi autonome.

Per applicazioni meno critiche, il problema del superamento del limite della *black box* costituisce oggi una vera e propria sub-disciplina della IA che va sotto il nome di “spiegabilità” (*explainability*) ed è attualmente oggetto di studio nel contesto di vari programmi di ricerca, come il programma *Explainable Artificial Intelligence* (XAI), della Defense Advanced Research Programs Agency (DARPA) statunitense (Gunning e Aha, 2019), e i progetti *Local Interpretable Model-Agnostic Explanations* (Ribeiro *et al.*, 2016) e *Human-Centered Artificial Intelligence* (Human AI, 2019). Trattandosi di ricerche ancora in corso è prematuro valutarne l'effettiva applicabilità sul campo dei loro risultati.

Va sottolineato che i sistemi di IA, e in particolare di ML, stanno dimostrando capacità e performance estremamente interessanti quando applicati a domini molto specifici e per l'esecuzione di compiti ben delimitati. Questo tipo di IA viene normalmente classificata come IA “stretta” (*narrow AI*). Ad esempio, nel caso delle reti neurali, si assiste al cosiddetto *catastrophic forgetting*: quando una rete cerca di apprendere nuove funzionalità o nuovi compiti, tipicamente dimentica quelli imparati in precedenza. Lo stato dell'arte in queste discipline non consente, al momento, di avere a disposizione sistemi di “IA generale”, cioè sistemi realmente intelligenti, capaci, fra l'altro, di trasferire in altri domini conoscenze apprese in un certo dominio applicativo. A maggior ragione, una “super IA”, cioè sistemi che esibiscono un'intelligenza superiore a quella naturale/umana in tutti i domini della conoscenza non è ad oggi realizzabile e si ritiene non lo sarà neppure nel prossimo futuro.

Concludiamo questa sezione ritornando brevemente sul problema delle vulnerabilità dei sistemi di IA e ML ad attacchi informatici specifici per questa classe di sistemi – genericamente denominati *adversarial attacks* – e rimandando al Capitolo 3 per una discussione più generale sui rischi di sicurezza informatica e cyberwar.

Un primo tipo di attacchi specifici per i sistemi di ML è quello dei cosiddetti *exploratory attacks*, tipici di avversari (anche umani) che si evolvono nel tempo, scoprendo, e quindi sfruttando, vari punti deboli dei programmi di ML. Ad esempio, un sistema automatico antispam potrebbe fare uso di un vocabolario per identificare gli spam; uno spammer può quindi imparare a storpiare leggermente le parole, inserendo dei semplici “errori” ortografici e, in questo modo, evitare di essere scoperto. L’essenza, quindi, di questi attacchi risiede nell’indurre la macchina a considerare legittimi input che invece non lo sono (Buchanan e Miller, 2017).

Un’altra classe di attacchi molto insidiosi è quella dei cosiddetti *causative attacks*. In questo caso, l’avversario cerca di creare delle debolezze nel sistema che sfrutterà in un secondo momento. Un tipico attacco di questo tipo è quello del cosiddetto “avvelenamento” del training data set. Questo altro non è che un meccanismo per creare ad arte una distorsione nel sistema talmente forte che, in definitiva, lo porta a imparare “le cose sbagliate” e quindi poi commettere errori, anche importanti, nella classificazione effettuata durante il suo uso (Buchanan e Miller, 2017). Ad esempio, avversari del nostro sistema antispam possono “avvelenare” i dati di training con una gran quantità di messaggi con contenuto pedo-pornografico e istruirlo in maniera da fare considerare questi messaggi legittimi; in questo modo, se l’antispam impara che la presenza di riferimenti alla pedopornografia è indizio del fatto che un messaggio non è uno spam, non sarà in grado di bloccare messaggi di quel tipo. Gli attacchi di questo tipo sono particolarmente diffusi specie contro quei sistemi di ML che fanno re-training, cioè che continuano a (ri)calibrare i loro parametri anche sulla base dei dati che ricevono durante l’uso. Naturalmente, tutti i tipi di classificatori che basano la loro funzionalità sul training possono essere soggetti ad attacchi di tipo *poisoning*.

## 2.4. Osservazioni conclusive

In questo capitolo abbiamo fornito una breve introduzione alla IA e alle tecniche di ML, ed esposto i limiti e le problematicità di queste ultime.

È attualmente in atto una vera e propria corsa agli armamenti basati sulla IA, i big-data e le armi “cyber”. A questa si aggiunge la progressiva digitalizzazione non solo del campo di battaglia, ma anche di tutte le infrastrutture militari, incluso il “complesso militare-nucleare”, dall’infrastruttura di progettazione e approvvigionamento dei componenti dei sistemi d’arma nucleare, alle armi stesse, alla logistica, fino al sistema NC3–Nuclear Command Control and Communications (Lin, 2021). Si crea così un pericoloso nesso fra il cyber-space e il complesso nucleare militare, specie se si consi-

dera, come nota Lin (2021), che le iniziative di “modernizzazione” del complesso militare-nucleare statunitense, lanciate dal presidente Obama e ancora in corso, potrebbero prevedere, come pare, l’integrazione dei sistemi C3 convenzionali con il NC3. Va sottolineato che i sistemi militari attuali non sono per nulla esenti da vulnerabilità informatiche e non c’è motivo per sperare che lo siano quelli futuri (Latella, 2021; USDOD, 2013; USGAO, 2017b; 2018; 2019; 2021)<sup>10</sup>. D’altra parte, il cyber-space è ormai considerato un vero e proprio dominio e gli attacchi cyber, quando rivolti a infrastrutture militari o civili “critiche”, vengono considerati dei veri e propri attacchi militari, ai quali eventualmente rispondere sia con altrettanti attacchi, o addirittura contemplando una risposta nucleare (USDOD, 2018; Futter, 2018; 2020; Marrone e Sabatino, 2021).

Questi elementi contribuiscono a incrementare l’incertezza, reale o percepita, durante la gestione di una crisi o di un conflitto, con il rischio concreto di escalation verso il conflitto nucleare e/o di guerra (nucleare) per errore. Il contributo che l’uso delle tecnologie della IA, anche per i limiti e le problematicità che abbiamo visto in questo capitolo, apporterà all’incremento di incertezza e confusione non sarà trascurabile (Geist e Lohn, 2018). Ad esempio, è ragionevole tenere presente che «è possibile immaginare un attacco [...] di poisoning dei dati che potrebbe portare un sensore [di un sistema di ML] a classificare un amico come nemico o a non rilevare la presenza di un nemico» (Allen e Chan, 2017, trad. it. a cura degli autori). Tutti questi elementi rendono ancora più delicata la gestione del rischio di escalation (Futter, 2019; Boulanin *et al.*, 2020; Turell *et al.*, 2020; Kubiak *et al.*, 2021).

Eppure nel rapporto della Commissione per la Sicurezza Nazionale sulla IA degli Stati Uniti – nominata dal Congresso e dall’Esecutivo e presieduta da E. Schmidt, già AD di Google e presidente esecutivo della stessa e di Alphabet Inc. – si legge: «Gli Stati Uniti devono prepararsi a difendersi dalle minacce [basate su IA] adottando velocemente e responsabilmente la IA per scopi di sicurezza nazionale e difesa» (NSCAI, 2021, p. 9) e «[d]ifendersi da avversari che dispongono di capacità IA senza utilizzare la IA è un invito al disastro» (NSCAI, 2021, p. 23). «Il dipartimento [della Difesa] deve agire adesso per integrare la IA nelle funzioni critiche, nei sistemi esistenti, nelle esercitazioni e war-games in modo da divenire una forza “AI-ready” entro il 2025» (NSCAI, 2021, p. 77, trad. it. a cura degli autori).

Queste autorevoli affermazioni fanno eco a posizioni radicali, controverse e a nostro avviso pericolose, perché attribuite a personalità di alto

<sup>10</sup> Sebbene, in generale, si faccia spesso riferimento solo alla situazione negli Stati Uniti, per la quale esiste ed è accessibile abbondante documentazione, non c’è motivo per considerare quella di altri paesi più avanzata o rassicurante.

livello, come quelle di William Roper, all'epoca capo dello Strategic Capabilities Office del Pentagono:

[I] [...] dati lavorano per te. Tu accumuli più dati possibile e li addestri a insegnare e addestrare sistemi autonomi [...]. [L]o scopo del primo o del secondo giorno [di battaglia] non sarà [più] quello di uscire e distruggere aerei nemici o altri sistemi. Esso è [invece] quello di uscire, accumulare dati, fare ricognizione di dati, così che i nostri sistemi di apprendimento diventino più intelligenti di [quelli del nemico] (Tucker, 2017 in Buchanan e Miller, 2017, pp. 21-22, trad. it. a cura degli autori).

Parnas (2017) sottolinea come sia opportuno e necessario sviluppare attività di ricerca nel campo della IA, con particolare riferimento alla *explainability* e alla sicurezza riguardo agli attacchi tradizionali e *adversarial*. Inoltre, è importante che, prima di utilizzare questi sistemi fuori dai laboratori di ricerca, vengano valutate accuratamente e in maniera rigorosa tutte le implicazioni di natura etica e sociale e, nel caso dell'utilizzo per scopi militari e di sicurezza internazionale, anche quelle del diritto internazionale<sup>11</sup>.

Si sente spesso affermare, anche in ambienti scientifici, che di fronte a un problema del quale non si conosce la soluzione, piuttosto che affrontarlo con il metodo scientifico, partendo dall'osservazione e cercando di individuare cause ed effetti per sviluppare una teoria, sia più opportuno affidarsi alla IA, perché con sufficiente potenza di calcolo e sufficienti dati essa lo risolverà. Noi invece pensiamo che questo approccio sia sbagliato e pericoloso e che la costruzione di sistemi informatici affidabili debba comunque essere guidata da solidi principi di ingegneria dei sistemi e *trustworthy computing*, come sottolineato da Cerf (2019) e Neumann (2019).

Concludiamo, quindi, affermando che condividiamo appieno i punti di vista di eminenti personalità della comunità degli informatici, quali David L. Parnas, William G. Cerf e Peter G. Neumann, sulla ricerca in IA e, più in generale, in informatica e sui rischi dell'uso di queste tecnologie, specie in campi di applicazione critici, dove si richiede il massimo possibile di affidabilità e, più in generale, di *dependability* e *trustworthiness* (Avizienis *et al.*, 2004). In particolare, riteniamo che sia necessaria un'approfondita discussione sull'utilizzo della IA in campo militare, che affronti non solo i potenziali vantaggi della militarizzazione della IA, ma anche e soprattutto i possibili rischi e la relativa governance (Stanley Center, UNODA, STIMSON, 2019; Boulanin *et al.*, 2020; Work, 2021). Allo stesso tempo, riteniamo che lo studio della IA sia sicuramente interessante, in particolare in campo civile, specie se usata in specifici domini di applicazione, per compiti ben definiti e con utili applicazioni.

<sup>11</sup> Al riguardo, si rimanda ai capitoli 5, 8 e 9 e a Tamburrini (2020) e Fossa *et al.* (2021).



## Riferimenti bibliografici

- Aiello M., Pratt-Hartmann I., van Benthem J., eds. (2007), *Handbook of Spatial Logics*, Springer, Dordrecht, NL.
- Allen G. and Chan, T. (2017), *Artificial Intelligence and National Security. STUDY 2017*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge (MA), USA.
- Amoroso D., Sauer F., Sharkey N., Suchman L., Tamburrini, G. (2018), *Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy*, The Heinrich Böll Foundation, Berlin, D.
- Andrie S.A. (1987), *Artificial Intelligence and National Defense. Applications to C<sup>3</sup>I and Beyond*, AFCEA International Press, Washington, USA.
- Avizienis A., Laprie J-C., Randell B., Landwehr C. (2004), "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*. 1(1):11-33.
- van Benthem J. and Blackburn P. (2006), *Modal Logic: A Semantic Perspective*, In: Blackburn P., van Benthem J., Wolter F., eds., *Handbook of Modal Logic*, Springer, Dordrecht, NL.
- Boulanin V. and Verbruggen M. (2017), *Mapping the Development of Autonomy in Weapon Systems*, Stockholm International Peace Research Institute (SIPRI) Stockholm, SE.
- Boulanin V., Saalman L., Topychkanov P., Su F., Carlsson M.P., Richards L. (2020), *Artificial Intelligence, Strategic Stability and Nuclear Risk*. Stockholm International Peace Research Institute (SIPRI) Stockholm, SE.
- Boulanin V., Goussac N., Bruun L., Richards L. (2020), *Responsible Military Use of Artificial Intelligence. Can the European Union Lead the Way in Developing Best Practice?* Stockholm International Peace Research Institute (SIPRI) Stockholm, SE.
- Buchanan B. and Miller, T. (2017), *Machine Learning for Policymakers. What It Is and Why It Matters. Paper 2017*, Harvard Kennedy School, Belfer Center for Science and Int. Affairs, Cambridge (MA), USA.
- Cerf V.G. (2019), "AI Is Not an Excuse!", *Communications of the ACM*, 62(10): 7.
- CRS (2018), *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, CRS Report, Congressional Research Service, Washington, USA.
- Cummings M.L. (2017), *Artificial Intelligence and the Future of Warfare*, Chatham House. The Royal Institute of International Affairs, London, UK.
- Din A.M., eds. (1986), *Arms and Artificial Intelligence. Weapon and Arms Control Applications of Artificial Intelligence*, Stockholm International Peace Research Institute (SIPRI), Stockholm, SE.
- Dyndal G.L., Berntsen T.A., Redse-Johansen S. (2017), "Autonomous military drones: no longer science fiction", *NATO Review Magazine*, 28 luglio 2017.
- van Ditmarsch H., Halpern J.Y., van der Hoek W., Kooi B., eds. (2015), *Handbook of Epistemic Logic*. London, College Publications, Rickmansworth, UK.

- Edwards C. (2019), “Hidden Messages Fool AI”, *Communications of the ACM*, 62(1): 13-14.
- Ekelof M. and Persi Paoli G. (2020), *Swarm Robotics. Technical and Operational Overview of the Next Generation of Autonomous Systems*, United Nations Institute for Disarmament Research (UNIDIR), Geneva, CH.
- Emerson E.A. (1990), *Temporal and Modal Logic*, In: van Leeuwen J., *Handbook of Theoretical Computer Science*, The MIT Press, Boston, USA.
- Fossa F., Schiaffonati V., Tamburrini G. (2021), *Automi e persone. Introduzione all’etica dell’intelligenza artificiale e della robotica*, Carocci, Roma.
- Franklin S. (2014), *History, motivation and core themes*, In: Frankish K. e Ramsey W. M. eds., *The Cambridge Handbook of Artificial Intelligence*, Cambridge University Press, Cambridge, UK.
- Futter A. (2018), *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press, Washington D.C., USA.
- Futter A. (2019), *Managing the Cyber-Nuclear Nexus*, Policy Brief, European Leadership Network, Londra, UK.
- Futter A. (2020), *What does cyber arms control look like? Four principles for managing cyber risks*, Global Security Policy Brief, European Leadership Network, Londra, UK.
- Geist E. and Lohn A. (2018), *Security 2040. How might Artificial Intelligence affect the risk of nuclear war*, RAND Corporation.
- Goodfellow I., Bengio Y.Y., Courville A. (2016), *Deep Learning*, The MIT Press, Cambridge (MA), USA.
- Gunning D., Aha D.W. (2019), “DARPA Explainable Artificial Intelligence Program”, *AI Magazine*, 40(2): 44-58.
- HumanE AI (2019), *Human-Centered Artificial Intelligence*. EU Horizon2020 funded project <https://www.humane-ai.eu> (accesso effettuato il 26 gennaio 2022).
- Klarreich E. (2016), “Learning Securely”, *Communications of the ACM*, 59(11):12-14.
- Kubiak K., Misra S., Stacey G. eds. (2021), *Nuclear weapons decision-making under technological complexity*. Pilot Workshop Report. Global Security, European Leadership Network, Londra.
- Landman N., Pang H., Williams C. (2019), “K-Means Clustering”, *Brilliant.org*, testo disponibile al sito: <https://brilliant.org/wiki/k-means-clustering/> (accesso effettuato il 26 gennaio 2022).
- Latella D. (2021), “Sicurezza informatica, armi nucleari e stabilità strategica”, *IRIAD Review*, n. 3, marzo-aprile, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Lin H. (2021), *Cyber Threats and Nuclear Weapons*, Stanford University Press, Stanford (CA), USA.
- Marrone A. and Sabatino E. (2021), *Cyber Defense in NATO Countries: Comparing Models*, IAI Papers 21, 5, Istituto Affari Internazionali, Roma
- Neumann P.G. (2019), “How Might We Increase System Trustworthiness?”, *Communications of the ACM*, 62(10): 23-25.

- NSCAI (2021), National Security Commission on Artificial Intelligence. *Final Report*.
- OpenAI (2019), *Attacking Machine Learning with Adversarial Examples*, testo disponibile al sito: <https://openai.com/blog/adversarial-example-research/> (accesso effettuato il 26 gennaio 2022).
- Parnas D.L. (2017). “The Real Risks of Artificial Intelligence”, *Communications of the ACM*, 60(10): 27-31.
- Pedregosa F., Varoquaux G., Gramfort A., Michel V., Thirion B., Grisel O., Blondel M., Prettenhofer P., Weiss R., Dubourg V., Vanderplas J., Passos A., Cournapeau D., Brucher M., Perrot M., Duchesnay, E. (2011), “Machine Learning in Python”, *Journal of Machine Learning Research*, 12: 2825-2830.
- Ribeiro M.T. and Singh S., Guestrin C. (2016), *Why Should I Trust You? Explaining the Predictions of Any Classifier*. In: Krishnapuram B., Shah M., Smola A.J., Aggarwal C.C., Shen D., Rastogi R., eds., *Proceedings of the 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, San Francisco, CA, USA, Aug. 13-17, 2016*. USA: Association for Computing Machinery (ACM).
- Rossi J.C. (2019), “Un’opera dell’uomo: le macchine autonome letali”, *IRIAD Review*, 5:2-22.
- Schneier B. (2018), *Click here to kill everybody. Security and survival in a hyper-connected world*, W.W. Norton & Company Inc., New York, N.Y., USA.
- Stanley Center, UNODA, STIMSON (2019), *The Militarization of Artificial Intelligence*, Stanley Center for Peace and Security, United Nations Office for Disarmament Affairs (UNODA), Stimson Center, UN, New York, August 2019.
- Tamburrini G. (2020), *L’etica delle macchine. Dilemmi morali per robotica e intelligenza artificiale*. Carocci, Roma.
- Thys S., van Ranst W., Goedeme T. (2019), “Fooling automated surveillance cameras: adversarial patches to attack person detection”, <https://arxiv.org/abs/1904.08653> (accesso effettuato il 26 gennaio 2022).
- Turell J. and F., Boulanin V. (2020), *Cyber-incident Management. Identifying and Dealing with the Risk of Escalation*, Stockholm International Peace Research Institute (SIPRI), Stockholm, SE.
- UNIDIR (2018), *The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence – a primer for CCW delegates*, UNIDIR Resources N. 8, United Nations Institute for Disarmament Research (UNIDIR), Geneva.
- USDOD (2013), *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, US Department of Defense, Defense Science Board, Washington, USA.
- USDOD (2016), *Report of the Defense Science Board Summer Study on Autonomy*, US Department of Defense, Defense Science Board, Washington, USA.
- USDOD (2018), *Nuclear Posture review*, US Department of Defense, Washington, USA.
- USGAO (2017a), *Internet of Things. Status and implications of an increasingly connected world*, Report to Congressional Requesters, GAO-17-75, US Government Accountability Office – GAO, Washington DC, USA.

- USGAO (2017b), *Internet of Things. Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*. Report to Congressional Committees, GAO-17-668, US Government Accountability Office – GAO, Washington DC, USA,
- USGAO (2018), *Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities*, Report to the Committee on Armed Services, U.S. Senate, GAO-19-128, US Government Accountability Office – GAO, Washington DC, USA.
- USGAO (2019), *Future Warfare. Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*, Report to Congressional Committees, GAO-19-570, US Government Accountability Office – GAO, Washington DC, USA.
- USGAO (2021), *Weapon Systems Cybersecurity. Guidance Would Help DOD Programs Better Communicate Requirements to Contractors*, Report to Congressional Committees, GAO-21-179, US Government Accountability Office – GAO, Washington DC, USA.
- Work R.O. (2021), *Principles for the Combat Employment of Weapon Systems with Autonomous Functionalities*, Center for New American Security, Washington DC, USA.

## 3. Vulnerabilità delle tecnologie informatiche, Intelligenza Artificiale e LAWS

di Gian Piero Siroli

### 3.1. Introduzione

Le tecnologie informatiche e di comunicazione (ICT) rappresentano un chiaro ed esplicito esempio di tecnologie a doppio uso, militare e civile. Gli sviluppi iniziali delle comunicazioni via rete e i relativi protocolli di trasmissione dati (TCP/IP in particolare) furono difatti condotti dal Dipartimento della Difesa degli Stati Uniti attraverso la sua agenzia di ricerca DARPA (*Defense Advanced Research Projects Agency*), con il pionieristico progetto ARPANET alla fine degli anni '60. Durante la guerra fredda ci fu un uso esteso di supercomputer delle generazioni più avanzate e delle reti di trasmissione a scopi bellici e questa co-evoluzione, pur nelle mutate condizioni storiche, è proseguita fino ad oggi.

Il relativamente recente sviluppo dei sistemi di arma autonomi e la quasi contemporanea esplosione delle tecniche di IA non possono che avere una inevitabile convergenza verso dispositivi capaci di operare con sempre maggiore indipendenza dal controllo umano, passando dal cosiddetto *man-in-the-loop* (controllo umano diretto), attraverso il *man-on-the-loop* (controllo umano indiretto) fino eventualmente a cercare di raggiungere lo stato di *man-off-the-loop*, ovvero di una completa autonomia del sistema dal controllo umano. Da notare che, se ci limitiamo al solo mondo digitale, questa autonomia è già stata raggiunta da circa due decenni attraverso l'uso dei cosiddetti *worm*, segmenti di codice in grado di moltiplicarsi e propagarsi autonomamente in rete senza necessità di controllo umano nella ricerca del bersaglio e nel successivo attacco (a differenza dei computer *virus*, non autonomi nella propagazione); i *worm* sono già da tempo utilizzati per scopi di guerra cibernetica.

Ritornando alle tecniche di IA, recentemente e in brevissimo tempo alcuni algoritmi sono stati in grado di apprendere autonomamente e senza

addestramento umano giochi di strategia molto complessi. Apparentemente queste tecniche di auto-apprendimento sono giunte ad un grado di generalità molto elevato, tanto da sembrare in grado di gestire e risolvere autonomamente problemi ben definiti, in un ambiente sufficientemente delimitato, con uno scopo ben preciso ed interazioni simulabili, che permettono ai sistemi di apprendere con il passare del tempo (UNIDIR, 2018).

Nel caso particolare dei LAWS subentra un ulteriore importante fattore da considerare: i tempi caratteristici di funzionamento e risposta di tali sistemi, in particolare con funzionalità IA, sono molto più brevi di quelli umani, restringendo drasticamente il tempo del ciclo osservazione-decisione-azione (tipico delle operazioni militari) e con conseguenti regole di ingaggio inevitabilmente più rapide ed una velocità delle operazioni molto più elevata che un umano non sarebbe in grado di affrontare, ancor meno nel caso di sciami di sistemi autonomi che operino collettivamente. Sistemi autonomi di questo tipo possono probabilmente essere contrastati solo con una tecnologia equivalente, oppure con altre opzioni a livello cibernetico, il cui controllo umano in tempo reale risulta comunque estremamente limitato.

È essenziale mantenere sempre ben presente che ci si trova ad affrontare un contesto, sia tecnologico sia di conoscenze, in rapidissima evoluzione e forse con pochi precedenti nella storia, dove le previsioni o le proiezioni nel futuro sono molto difficili ed il “futuro” stesso va inteso a relativamente breve termine. Dal punto di vista strettamente scientifico, ad oggi gli algoritmi di IA, e le reti neurali in particolare, mancano ancora di un fondamento teorico solido, proprio mentre le applicazioni tecnologiche decollano a ritmo incontrollato.

In questo scenario è fondamentale cercare di analizzare ad ampio spettro, oltre alle considerazioni puramente tecnologiche, gli associati aspetti legali, etici e strategici, obiettivo che ci poniamo in questo libro.

### **3.2. Vulnerabilità intrinseche delle tecnologie informatiche**

L’affidabilità dei sistemi cibernetici imbarcati nei LAWS, con le sue numerose componenti, inclusa anche la funzionalità di IA, non può prescindere dalla considerazione che questi sistemi sono costituiti, in larga parte, da programmi software in esecuzione in computer tradizionali. Essi sono pertanto suscettibili di tutte le principali vulnerabilità associate alle tecnologie informatiche e di comunicazione (ICT) che saranno qui di seguito brevemente descritte, allo scopo di tratteggiare il panorama globale o almeno la sua parte più tradizionale.

Innanzitutto, si deve tenere presente che durante l’evoluzione iniziale e lo sviluppo del futuro ecosistema cibernetico globale, avviato in USA negli

anni '70, le problematiche di sicurezza digitale furono relativamente sottovalutate, se non quasi trascurate, poiché computer e reti della Difesa degli Stati Uniti erano sotto il completo controllo militare. Solamente in seguito si è avuto il graduale passaggio delle infrastrutture di rete verso il mondo civile e commerciale di cui siamo testimoni oggi. Questa disattenzione e trascuratezza, il basso livello di consapevolezza delle potenziali conseguenze e il comportamento istintivamente collaborativo dei primi utilizzatori hanno consentito e, purtroppo, orientato verso la costruzione di strumenti e di protocolli che in certi casi non possedevano alcune delle caratteristiche e degli strumenti necessari alla protezione digitale.

Questa pesante eredità è tutt'ora molto pertinente e causa di molti dei problemi e vulnerabilità del mondo digitale odierno, estesosi nel frattempo a livello planetario. Ciò ha determinato una situazione di ancor più difficile risoluzione che nel passato a causa dell'iper-sviluppo e della proliferazione delle infrastrutture di calcolo a livello globale, ormai difficili da aggiornare anche solo per il numero elevatissimo e la diversificazione degli apparati installati, creando una grave inerzia a qualsiasi tentativo di rilevante modifica di alcuni basilari protocolli di comunicazione.

Alle problematiche intrinseche di sicurezza indotte da certi protocolli "deboli" (a livello di progettazione o implementazione), va aggiunta la attuale incapacità tecnologica di scrivere software immuni da difetti logici o errori (*bug*), la cui entità è stimata nell'ordine di qualche decina ogni 1000 linee di codice, e che sono la causa primaria delle vulnerabilità comunemente sfruttate nelle tecniche di attacco cibernetico.

Tutto ciò crea un sistema globale dove il cosiddetto *malware* può assumere moltissimi aspetti diversi. *Worms* e *virus* sono segmenti di codice in grado di riprodursi e propagarsi in rete e dotati di istruzioni di attacco specifico per il bersaglio prescelto (ad esempio l'esfiltrazione di dati o l'intromissione illecita e il controllo remoto di computer). I *denial of service* permettono il sovraccarico, fino a giungere al blocco, di segmenti di rete o di particolari servizi. *Rootkit* e *backdoor* sono in grado di nascondere la presenza di software ostili sui nodi compromessi e permetterne l'accesso permanente non autorizzato a determinate funzionalità. I *botnet* sono grandi reti di computer illegalmente penetrati, presi sotto il completo controllo remoto di organizzazioni fantasma e utilizzati per vari scopi. Di particolare rilevanza sono le cosiddette vulnerabilità *zero-day*, completamente sconosciute anche agli stessi sviluppatori del software in questione e spesso disponibili ad elevate cifre sul mercato nero cibernetico. Le *zero-day* sono utilizzabili per gli attacchi finché non sono creati e distribuiti dai produttori del software gli specifici meccanismi di protezione e possono permanere nell'ecosistema digitale anche per anni prima di essere scoperte e corrette.

Questo è solo un brevissimo elenco, non esaustivo, di meccanismi di attacco. Le vulnerabilità possono però avere anche un'origine diversa, con un conseguente aumento dei vettori e della superficie di attacco dei sistemi digitali. Non solo il software, ma anche l'hardware e il firmware (quale il BIOS/UEFI) possono contenere vulnerabilità, in questo caso situate ad un livello molto più difficile da rilevare e potenzialmente con un profondo impatto. Una *backdoor* a livello hardware permette, infatti, un accesso completo all'apparato in questione, aggirando completamente i sistemi di controllo e autenticazione e protezione.

A fine 2017 sono state scoperte due vulnerabilità di questo tipo che hanno interessato una frazione elevatissima dei microprocessori installati sui computer costruiti durante gli ultimi venti anni. Tutti i più importanti e diffusi sistemi operativi erano esposti, tanto da rendere a rischio di attacco anche apparati mobili, smart TV, stampanti e dispositivi di rete, quindi tutto l'ambiente digitale. Le vulnerabilità erano così fondamentali e globalmente diffuse da essere considerate catastrofiche dagli analisti di *security*.

*Spectre e Meltdown* (Google, 2018) – questi i nomi dati alle diverse varianti di queste vulnerabilità – permettevano ad un attaccante di fare accesso a meccanismi interni dei processori e a zone di memoria riservate del sistema operativo operante su computer dotati di specifici, ma diffusissimi, processori Intel, IBM e di altre architetture che i sistemi operativi assicuravano di tenere assolutamente protette, separate e non comunicabili. Attraverso questo “canale” aperto a livello hardware strutturale, le protezioni a livello software superiore risultavano inutili e inefficaci.

La soluzione definitiva a questo problema, come dichiarato successivamente anche dai produttori, era la riprogettazione delle unità di elaborazione centrale (CPU) in oggetto.

Purtroppo questo tipo di problematica non è limitata alle CPU, ma si estende ad altri microcircuiti specializzati inclusi nell'architettura di base dei computer, quali, ad esempio, i processori grafici (GPU, Graphics Processing Unit), adibiti a velocizzare l'elaborazione delle immagini e la gestione video. In virtù della loro alta efficienza in calcoli paralleli, tali unità sono sempre più utilizzate anche per scopi diversi dalla gestione grafica e, ovviamente, non sono esenti da vulnerabilità della stessa natura di *Spectre e Meltdown*, come dimostrato dai numerosi aggiornamenti di sicurezza frequentemente distribuiti dai produttori di tali circuiti.

In proiezione, entrando nel contesto specifico dell'attuale rapida espansione delle tecniche della IA, si sta sviluppando un'altra classe particolare di circuiti integrati chiamati *Tensor Processing Unit* (TPU) adibiti specificatamente per l'uso delle reti neurali, strutture che sono alla base dei meccanismi di apprendimento della IA. Naturalmente questa ulteriore struttura hardware,



anche se inclusa in sistemi dedicati, difficilmente sarà esente dallo stesso tipo di rischi.

Questi tipi di vulnerabilità hardware mettono in luce un ulteriore livello di potenziale pericolo di manipolazione o di intrusione nei sistemi cibernetici, quello della cosiddetta *supply chain*, cioè la catena di produzione dei micro-dispositivi hardware (CPU, unità logiche, interfacce, ecc.) inseriti all'interno di computer e apparati di rete.

Se gli apparati in uso non possono essere considerati affidabili perché contenenti particolari sottosistemi elettronici vulnerabili o manipolabili, eventualmente prodotti o modificati con scopi ostili in paesi antagonisti, le conseguenze possono essere molto gravi a vari livelli. Immaginiamo solamente la potenziale perdita di controllo di complessi sistemi industriali o di infrastrutture critiche a livello nazionale, in un contesto sia civile sia militare, incluso quello dei sistemi d'arma più avanzati a livello cibernetico, senza dimenticarne il possibile impiego da parte di servizi di intelligence stranieri.

In determinati contesti particolarmente delicati è il meccanismo stesso di *outsourcing* degli apparati o di alcune specifiche componenti che può essere messo in discussione, così come il controllo dettagliato della catena di approvvigionamento che dovrebbe assicurare l'integrità dalla produzione alla distribuzione, per prevenire la proliferazione di tecniche e strumenti ICT occulti ed ostili.

Ci troviamo di fronte a uno degli argomenti chiave discussi anche a livello internazionale nel contesto delle ICT, a causa delle importanti conseguenze nell'ambito della sicurezza (ONU, 2015).

Va inoltre considerata sotto questa luce anche la prospettiva della futura dinamica della *Internet of Things* (IoT), la proliferazione della interconnessione in rete di apparati di uso comune, che pone problematiche molto complesse dal punto di vista della sicurezza informatica in generale.

Per completezza si aggiunge, infine, un'ulteriore dimensione delle tecnologie di attacco, questa volta non connessa alle infrastrutture tecniche, ma mirata a quello che a volte risulta l'anello più debole della catena di difesa: l'elemento umano. Il cosiddetto *social engineering* si inserisce a livello comportamentale umano e include la manipolazione fraudolenta di dati o informazioni trasmesse al soggetto bersaglio (utente o amministratore di sistema). Lo scopo, spesso raggiunto, è di modificare e guidare inconsciamente le sue azioni (contro il suo stesso interesse) o divulgare informazioni confidenziali che compromettano la sicurezza globale dell'infrastruttura sotto attacco. Si tratta di una manipolazione psicologica, a livello individuale o sociale, più attribuibile al contesto della *information-security* che della *cyber-security*, ma da tenere sempre in considerazione.

### 3.3. Vulnerabilità specifiche delle tecnologie IA/ML

Nel contesto dei AWS, ed in particolare dei sistemi d'arma letali, la prospettiva di un uso sempre più massiccio e diffuso delle tecniche della IA e degli algoritmi di *Machine Learning* appare una tendenza evolutiva inevitabile nel breve-medio termine, poiché questi algoritmi possono favorire ed estendere l'autonomia dal controllo umano. Purtroppo in questo nuovo spazio che si apre, la panoramica delle vulnerabilità software e hardware precedentemente descritta diventa troppo limitata per descrivere la complessità del fenomeno: l'IA apre una nuova superficie di attacco precedentemente inesistente e che diventerà sempre più rilevante con la diffusione di queste nuove tecnologie.

Le tecniche di ML o *Deep Learning* (DL), basate su reti neurali più o meno profonde, sono in grado di individuare schemi o regolarità di un determinato fenomeno in esame utilizzando un insieme di dati di addestramento da cui estrarre una sorta di modello, per poi eseguire delle operazioni sulla base di questa conoscenza. Possono quindi essere in grado di fare previsioni o prendere decisioni senza un'esplicita e specifica programmazione algoritmica, in certi casi praticamente impossibile allo stato attuale. Questi sistemi sono usati per risolvere varie classi di problemi, tra i più importanti si possono citare la computer vision (identificazione di immagini, supporto alla guida autonoma di veicoli), la classificazione e il riconoscimento di oggetti, la comprensione e l'interpretazione del linguaggio, il supporto alla diagnosi medica ed alcuni meccanismi cibernetici di protezione o rivelazione di attività anomale. Molti sistemi IA sono usati anche come supporto al *decision-making* umano, ma in questo contesto specifico diventa particolarmente rilevante e critica la relazione uomo-macchina in termini di affidabilità. Durante la fase di apprendimento (*supervised learning*), la rete neurale "apprende" e memorizza quali sono i risultati desiderati (o la soluzione) di un particolare problema e in una seconda fase è in grado di replicare tale comportamento su dati successivamente sottoposti al sistema risolvendo il problema stesso. In alcuni casi è anche possibile eliminare la fase iniziale di apprendimento (*unsupervised/reinforcement learning*) poiché queste tecniche sono in grado di "auto apprendere" senza supervisione, soprattutto in sistemi ben definiti e descritti con regole precise e formalizzabili. La più recente evoluzione di queste tecniche è dovuta principalmente alla disponibilità di un elevato ed economico potere computazionale, unito a una grande abbondanza di dati su cui operare l'apprendimento e le successive analisi ed applicazioni.

Per comprendere la potenza di queste tecnologie si prenda in considerazione il caso del progetto Alpha Zero, della compagnia Deep Mind: svilup-

pato con tecniche di IA e utilizzando TPU *ad-hoc*, senza fase di apprendimento supervisionato da umani, ma semplicemente conoscendo le regole del gioco e giocando contro se stesso, è stato in grado di raggiungere un livello super-umano nel gioco del Go, forse il più difficile gioco di strategia da scacchiera. Alpha Zero (Science, 2018) è stato progettato per imparare anche gli scacchi e il Shogi, un gioco della stessa famiglia degli scacchi, quindi le sue capacità sembrano essere sufficientemente astratte da essere applicabili a contesti diversi. Nel febbraio 2022 la stessa Deep Mind ha reso pubblico Alpha Code, un sistema basato su IA, apparentemente ancor più evoluto, in grado di creare autonomamente del codice sorgente di qualità paragonabile a quella di un programmatore medio, utilizzato nel contesto specifico di gare di programmazione competitiva umana.

Le reti neurali, sui cui si fonda il ML, sono sistemi altamente non lineari e complessi le cui basi scientifiche sono ancora da determinare con precisione, con la conseguenza che molti di questi modelli sono a tutti gli effetti delle “black box”, il cui comportamento sfida la comprensione umana ed i cui risultati o decisioni risultano al momento non interpretabili e inesplicabili. Da questa complessità e indeterminazione nascono le vulnerabilità sfruttabili da eventuali attaccanti, potenzialmente anche con gravi conseguenze.

Si parla di *Adversarial AI* (o *Adversarial Attacks*) quando un aggressore riesce a determinare un particolare comportamento della *black box* (la rete neurale) ignoto ai suoi stessi sviluppatori, per poi sfruttarlo per i propri scopi. Se si riesce a predire il modello di apprendimento di un particolare sistema, può essere possibile, in molti casi, manipolare i dati per ottenere o forzare il risultato desiderato anziché le decisioni corrette, o in alternativa creare delle vulnerabilità da sfruttare in seguito.

Un serio rischio in questo contesto è quello del *Poisoning Attack* che può essere messo in atto quando si riesce ad influenzare direttamente il processo di apprendimento delle reti neurali, come nel caso del *supervised learning*. Il *training data set* viene contaminato da informazioni non pertinenti oppure opportunamente costruite allo scopo di indurre il sistema a commettere errori di valutazione o rispondere in un modo pre-programmato ed errato.

A seguito di questo tipo di attacco su di un'automobile a guida autonoma, un segnale stradale di stop è stato classificato dalla rete neurale come un segnale differente, con tutte le potenziali conseguenze del caso. Un altro esempio riguarda i sistemi antispam basati su reti neurali: un “avvelenamento” dei dati di training con contenuti di un certo tipo potrebbe istruire il sistema a considerare legittime delle email che andrebbero invece scartate; questo tipo di attacchi sono particolarmente diffusi nei sistemi di *reinforcement-learning*, che ricalibrano i loro parametri sulla base dei dati analizzati.

Da un punto di vista generale, all'aumentare della pervasività dei sistemi di IA e ML consegue la necessità di comprenderne limiti, vulnerabilità e meccanismi di malfunzionamento. A questo ultimo scopo si possono distinguere due grandi classi: i malfunzionamenti intenzionali, causati da una attività ostile che opera manomissioni esplicite a livello di classificazione, addestramento o algoritmo, e i malfunzionamenti non intenzionali dove il sistema produce un risultato formalmente corretto, ma completamente inapplicabile, insicuro o incoerente con la realtà, a tutti gli effetti sbagliato. Al momento gli analisti hanno caratterizzato circa una decina di metodologie diverse per provocare malfunzionamenti indotti ed un numero più ridotto per quelli non intenzionali (Microsoft, 2019).

Esempi di malfunzionamenti indotti sono la contaminazione (“*poisoning*”) dei dati o delle procedure di training (di cui abbiamo già parlato), l’inserzione di eventuali *backdoor* attivate da dati, opportunamente manipolati e configurati, sottoposti al sistema allo scopo di ottenere la risposta voluta, oppure la dipendenza o l’inoculazione di segmenti di codice vulnerabile (in questo caso un meccanismo di attacco tradizionale, ma applicato nel nuovo contesto IA).

Tra i meccanismi non intenzionali di malfunzionamento, trattasi di fatto di vulnerabilità interne, si possono includere test incompleti del sistema di ML che non comprendono tutte le condizioni realistiche di funzionamento, oppure l’incapacità del sistema di adattarsi alle condizioni ambientali, in particolare con lente variazioni temporali o semplicemente in presenza di dati di ingresso con alta variabilità o perturbati, come rumore, immagini deformate o sporche ecc.

Un altro meccanismo di attacco, apparso relativamente recentemente, consiste nel nascondere del codice malevolo di attacco (payload) all’interno delle reti neurali, in modo da renderlo invisibile al meccanismo di controllo *anti-malware*. In sostanza una forma di steganografia che nasconde un oggetto dentro ad un altro (ad esempio, un testo all’interno della codifica di una foto). I meccanismi di *deep learning*, costituiti da milioni di parametri numerici, permetterebbero questa tecnica, denominata *EvilModel*. Spezzettando il malware in piccoli segmenti e codificandoli in questi parametri non si distrugge la funzionalità essenziale del sistema IA ma si può trasmettere il codice di attacco assieme alla rete neurale senza che la sua presenza sia rivelabile, malware che sarebbe poi riassembleto a destinazione ed attivato sul bersaglio.

Sempre più spesso sistemi IA preaddestrati vengono pubblicamente condivisi in rete tra gli sviluppatori di software, allo scopo di essere integrati in diverse applicazioni ed usati senza che sia necessaria una fase di addestramento, poiché già funzionali e operativamente utilizzabili; l’*EvilModel* permetterebbe quindi la propagazione occulta del malware.

Un modo per contrastare questa tecnica di attacco è eliminare il malware eseguendo una successiva nuova fase di apprendimento, una sorta di *post-learning*, una regolazione fine del sistema IA nel nuovo ambiente applicativo, modificando e sovrascrivendo in tal modo il contenuto (avvelenato) dei parametri originali, a spese però di una maggiore necessità di risorse di calcolo.

Oltre a utilizzare la tecnologia IA per propagare in modo nascosto il malware, i parametri e la risposta di una rete neurale possono anche essere manipolati ed usati per selezionare ed attivare un attacco sul bersaglio predefinito, facendolo identificare dallo stesso sistema IA, come ha dimostrato pochi anni fa IBM con il meccanismo *DeepLocker*.

Globalmente, appare abbastanza evidente che tutto ciò richieda l'attenta verifica e soprattutto la protezione dei modelli di reti neurali e la creazione di meccanismi che assicurino affidabilità nella catena di creazione e distribuzione del software nei processi di apprendimento automatico di IA.

Appare chiaro quindi che i meccanismi di perturbazione o corruzione di questi sistemi non mancano, da qui la necessità di porre la dovuta attenzione nello sviluppo di opportune contromisure che rendano le tecnologie di IA/ML più robuste e sicure allo scopo di evitare conseguenze negative. Va sottolineato il fatto che eventuali malfunzionamenti e manipolazioni di questi algoritmi possono proiettarsi con un effetto a cascata su servizi, applicazioni o prodotti che interagiscono o dipendono da essi e di cui esiste già un'ampia casistica nel mondo digitale, con la conseguenza di compromettere a valle un ecosistema ben più vasto di quello specifico IA, che include non solo il dominio cibernetico, ma anche quello fisico.

La comunità scientifica, sia in ambito civile che militare, sta affrontando alcuni degli aspetti più problematici recentemente emersi, in particolare quelli che riguardano la attuale caratteristica tipo *black-box* precedentemente citata, molto rilevante soprattutto nel contesto specifico dei LAWS, connessa con l'opacità delle reti neurali e le sue potenziali conseguenze.

La potenza delle tecniche usate nelle procedure decisionali basate su IA appare considerevole, ma l'attuale incapacità tecnica del sistema di fornire agli stessi progettisti una spiegazione su come sia giunto ad una specifica scelta può risultare un fattore molto limitante per lo sviluppo futuro.

Attualmente stiamo assistendo, da parte di grandi compagnie ICT, all'uso sempre più esteso della IA proprio in questo contesto di *decision-making*, con effetti che già influenzano più o meno direttamente i nostri comportamenti.

Affidare decisioni che possono avere conseguenze dirette sulla vita umana (quali diagnosi mediche o sistemi d'arma letali) a un sistema che non è in grado di spiegare sé stesso presenta, però, evidenti rischi e pericoli che appaiono difficilmente accettabili.

Questo tema ha sollevato un dibattito internazionale attualmente in corso che sta esaminando un nuovo approccio verso quella che viene definita *eXplainable Artificial Intelligence* (XAI), allo scopo di sviluppare modelli o architetture più trasparenti ed interpretabili e quindi con un maggior grado di affidabilità, pur cercando di mantenere elevati livelli di performance. Si tratta di un tema di ricerca interdisciplinare di estrema importanza nell'ecosistema IA, i cui sviluppi possono potenzialmente coinvolgere ed influenzare uno spettro di applicazioni molto vasto. Al momento ci si trova in una fase iniziale di definizione e di formulazione del problema in termini sufficientemente precisi da permettere un successivo sviluppo, in un panorama dove probabilmente non è ancora stato approfondito a sufficienza il ruolo dell'essere umano nei meccanismi di spiegabilità (IEEE, 2018). Gli approcci potrebbero essere diversi: dalla modifica strutturale delle attuali modalità di *machine learning* e delle reti neurali, ad un diverso ed innovativo metodo di "explanation by design".

In ogni caso, la capacità di interpretazione umana sarà indispensabile per comprendere, gestire e poter responsabilmente fare affidamento sulla prossima generazione di tecnologie emergenti in questo campo. Potremmo insomma stare entrando in una nuova era di applicazioni IA.

Sull'argomento specifico XAI, l'agenzia della difesa statunitense DARPA sta finanziando numerosi gruppi di ricerca e si può solo immaginare che valenza possa avere a livello dei sistemi d'arma autonoma.

### **3.4. Dibattito internazionale**

Nel 2016 nel contesto della *Convention on Certain Conventional Weapons* (CCW) delle Nazioni Unite fu incaricato un gruppo di esperti governativi (GGE) per approfondire l'argomento delle tecnologie emergenti nell'ambito specifico dei LAWS, con un focus particolare sul diritto internazionale umanitario (DIU), le cui riunioni si sono periodicamente susseguite almeno fino al momento della scrittura di questo testo.

È apparsa subito evidente la difficoltà di comprendere con precisione il concetto di autonomia, un termine che varia continuamente in virtù di un vasto spettro di capacità tecnologiche e del tipo specifico di interazione uomo-macchina.

Considerata la validità e l'applicabilità del diritto umanitario a tutti i sistemi d'arma, la centralità delle scelte e della responsabilità umana risulta fondamentale, ma le tecnologie imbarcate nei sistemi d'arma, includendo anche l'effettivo livello di autonomia e le eventuali tempistiche di comunicazione, mettono questo presupposto a rischio. La natura dei LAWS, con

l'eventuale uso di sistemi di IA/ML, pongono dunque nuove sfide alla conformità di tali sistemi al diritto internazionale (ONU, 2019).

I punti critici da prendere in considerazione sono numerosi: la attuale opacità degli algoritmi di ML e la loro effettiva affidabilità, il potenziale di auto-apprendimento con la capacità di evolvere e ridefinire obiettivi operativi in termini di bersagli e regole di ingaggio in modo indipendente dal controllo dell'uomo, responsabile ultimo. Tutto questo è associato ad una possibile imprevedibilità di comportamento. Sono altresì importanti le modalità dei canali di comunicazione con la catena di comando e controllo responsabile durante le operazioni, che però potrebbe non avere più contatto diretto con il sistema dopo l'attivazione. E naturalmente non va trascurata l'importanza di ulteriori considerazioni etiche correlate.

Questo panorama si sovrappone a quello più ampio degli sciami di sistemi autonomi individuali che interagiscono tra loro e in grado di operare in modo collettivo verso un obiettivo comune. Si tratta dei cosiddetti *swarms* (sciami, ad esempio di droni aerei), attualmente di grande interesse militare, che possono porre un serio rischio di violazione del diritto umanitario (EU Non-Proliferation Consortium, 2019).

Questi aspetti tecnologici del dominio cibernetico sono in realtà presi in considerazione anche nell'ambito più generale di altre iniziative ONU che si occupano dello sviluppo delle ICT nel contesto della sicurezza internazionale, dinamica che ha preso l'avvio sin dal 1998 con una serie ininterrotta di risoluzioni dell'Assemblea Generale (*Developments in the field of information and telecommunications in the context of international security*) e rapporti da parte di vari paesi.

Più recentemente, nel dicembre 2018, l'Assemblea Generale dell'ONU ha stabilito due linee di attività parallele, e sperabilmente convergenti, attraverso la creazione di due entità: un gruppo di esperti governativi (*cyber GGE*), con partecipazione selezionata e limitata a 25 paesi e che non comprende l'Italia, e un *Open Ended Working Group* (OEWG) che include tutti i paesi membri delle Nazioni Unite.

Il cyber-GGE si focalizza sulle minacce attuali e future provenienti dal dominio ICT, sull'applicazione del diritto internazionale in questo contesto, sulla proposta di norme e principi internazionali a tal riguardo, sulle possibili misure di *confidence building* e di potenziamento delle capacità tecnologiche per i paesi meno sviluppati; il GGE prevede anche di tenere consultazioni con organizzazioni e attori regionali.

L'OEWG prosegue la linea iniziata nel 1998 su argomenti sovrapposti al GGE, ma in un forum nuovo e più ampio (*multistakeholder*) non limitato ai rappresentanti delle varie nazioni, con periodici meeting consultativi che includono il coordinatore del cyber-GGE, ma anche rappresentanti di

grandi compagnie del settore ICT, del mondo accademico e della società civile.

La dinamica complessiva cyber GGE-OEWG tuttora in sviluppo e, come si diceva, i LAWS fanno sicuramente parte anche di questo panorama. Nel frattempo, l'OEWG ha iniziato il secondo mandato (2021-2025), affrontando in particolare la questione tutt'ora aperta della partecipazione degli attori non statali ai lavori del gruppo stesso.

A queste iniziative internazionali si aggiungono altre importanti proposte e contributi indipendenti di diversa origine, con grandi corporation ICT coinvolte, tra le quali Microsoft, Siemens e Kaspersky. Nel contesto specifico della IA è utile citare una lettera aperta indirizzata alla Convenzione CCW dell'ONU sopraccitata, resa pubblica da alcune decine di compagnie del mondo della robotica e della IA, che mette in allarme sulle conseguenze delle tecnologie che loro stessi stanno sviluppando:

Lethal autonomous weapons threaten to become the third revolution in warfare. Once developed, they will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways. We do not have long to act. Once this Pandora's box is opened, it will be hard to close. We therefore implore the High Contracting Parties to find a way to protect us all from these dangers (Future of Life Institute, 2017).

La stessa organizzazione ha anche suggerito dei principi generali noti come *Asilomar AI principles* (che dovrebbero guidare il futuro sviluppo di queste tecnologie (Future of Life Institute, Asilomar AI Principles, 2017).

Un altro importante contributo a livello internazionale proviene dall'*International Committee for Robot Arms Control* (ICRAC), che raccoglie un gruppo di scienziati in sostegno ad un uso pacifico della robotica, attivo in particolare attraverso consultazioni informali nell'ambito del gruppo di esperti governativi sui LAWS (CCW); ICRAC ha anche prodotto una dettagliata analisi proprio sul concetto di controllo umano significativo, di cui è firmatario uno degli autori di questo rapporto, Guglielmo Tamburrini.

Altri importanti contributi della società civile provengono dall'*International Panel on the Regulation of Autonomous Weapons* (iPRAW), un gruppo interdisciplinare di scienziati che si occupa esplicitamente di LAWS partecipando al dibattito in seno alla convenzione CCW delle Nazioni Unite.



### 3.5. Osservazioni conclusive

Il passato mostra come la sicurezza e le minacce cibernetiche si evolvano con lo sviluppo delle tecnologie stesse. La creazione stessa del Web, l'uso esteso di database, lo sviluppo di IoT e la proliferazione dei social media sono stati accompagnati dalla comparsa di nuovi meccanismi e strumenti di attacco, sia a livello tecnologico che semantico. Internet ha aperto il vaso di Pandora dei rischi e pericoli della (in)sicurezza digitale. La IA e le reti neurali non fanno eccezione, oltre agli esempi di *DeepLocker* ed *EvilModel* questi sistemi possono contenere pregiudizi difficilmente percepibili o una nascosta capacità di persuasione a livello sociale e politico.

Il recente notevole sviluppo della IA ha sicuramente molti aspetti positivi ed in certi casi sembra in grado di risolvere taluni problemi con maggiore efficacia di un essere umano, tuttavia è indubbio che queste tecnologie allo stato attuale mostrino nuove vulnerabilità e limitazioni significative. Quello che manca in modo particolare è la capacità di affrontare un "ragionamento" a livello sufficientemente astratto o la capacità di trasferire l'esperienza acquisita verso compiti differenti.

Si tratta insomma di una "intelligenza" relativamente fragile, limitata e ristretta ad uno specifico settore, da cui consegue che resta fondamentale il ruolo e la responsabilità dell'uomo di decidere come, quando e dove utilizzare questi sistemi in modo appropriato, comprendendone le limitazioni, in particolar modo nel contesto militare.

Gli algoritmi IA/ML, il cui sviluppo è recentemente ri-esploso dopo un passato meno appariscente, mancano a vario livello di interpretabilità, predicibilità, verificabilità e affidabilità. Naturalmente si tratta di un dominio in rapida evoluzione e quindi è certamente possibile che la situazione migliori nel prossimo futuro, ma questa è la situazione attuale. È stato dimostrato che è possibile alimentare questi sistemi con dati scorretti, manipolati o non equilibrati da vari punti di vista, in modo da indurre un comportamento e risultati errati ed in certi casi pericolosi. La proiezione di questa situazione complessiva sui LAWS deve essere analizzata con attenzione, tenendo in considerazione anche la necessità di un comportamento ragionevolmente sicuro e trasparente dei sistemi e della responsabilità del fattore umano. Non si deve dimenticare che a volte l'uomo è l'anello più debole nella catena di sicurezza cibernetica, e soprattutto nella prospettiva di un uso futuro sempre più diffuso a livello globale, con l'inevitabile coinvolgimento di aspetti etici.

Tutto ciò ricoprirà un ruolo ancora più importante nel contesto militare: la guerra ha luogo in un habitat antagonistico e ostile, dove le capacità di adattamento e flessibilità sono caratteristiche primarie e ciò pone una sfida formidabile per il dispiegamento e l'uso di sistemi d'arma letali dotati di

funzionalità IA, in situazioni difficilmente prevedibili e potenzialmente fuori dagli schemi di apprendimento, dove gli insuccessi potrebbero condurre a tragiche conseguenze.

A tutto ciò vanno aggiunti ancora due fattori importanti: la sempre più complessa gestione della relazione uomo-macchina e la velocità alla quale i sistemi cibernetici autonomi possono operare, molto più alta della capacità di reazione e intervento umano in tempo reale. Va rivolta una particolare attenzione anche al comportamento collettivo di sistemi autonomi intelligenti, quale lo *swarming* precedentemente citato.

Il dibattito internazionale attualmente in corso e brevemente sintetizzato nel paragrafo precedente si sta sviluppando a diversi livelli – ONU, organizzazioni regionali, contatti bilaterali e multilaterali – e deve essere attentamente approfondito ed analizzato nei suoi vari aspetti (UNIDIR, 2018).

Appare indispensabile un ampio confronto sul tema delle tecnologie autonome in campo militare da svolgersi a livello interdisciplinare, che includa aspetti etici e legali, coinvolgendo la partecipazione di accademici, militari, diplomatici, esperti legali e membri della società civile. Giungere ad una visione globale che includa diverse prospettive sarà fondamentale per lo sviluppo e un uso corretto e responsabile di queste tecnologie emergenti (UNIDIR, 2018).

## Riferimenti bibliografici

- DeepMind (2022), *Competitive programming with AlphaCode*, testo disponibile al sito: <https://deepmind.com/blog/article/Competitive-programming-with-AlphaCode>.
- EU Non-Proliferation Consortium (2019), *The Question of Swarms Control: Challenge to Ensuring Human Control Over Military Swarms*, testo disponibile al sito: <https://www.nonproliferation.eu/the-question-of-swarms-control-challenges-to-ensuring-human-control-over-military-swarms/>.
- Future of Life Institute (2017), *An Open Letter to the United Nations Convention on Certain Conventional Weapons*, testo disponibile al sito: <https://futureoflife.org/autonomous-weapons-open-letter-2017/>.
- Future of Life Institute (2017), *Asilomar AI Principles*, testo disponibile al sito: <https://futureoflife.org/ai-principles/>.
- Google (2018), *Reading privileged memory with a side-channel* (<https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>).
- IEEE (2018). “Peeking inside the black box: a survey on explainable artificial intelligence”, *IEEE Access*, vol.6, testo disponibile al sito: <https://ieeexplore.ieee.org/document/8466590>.
- Microsoft (2019), “Failure Modes”, *Machine Learning*, testo disponibile al sito: <https://arxiv.org/ftp/arxiv/papers/1911/1911.11034.pdf>.

- ONU (2015), *Developments in the field of information and telecommunications in the context of international security*, Risoluzione Assemblea Generale, A/70/174, testo disponibile al sito: [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).
- ONU (2019), *Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems – Addendum*, testo disponibile al sito: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/931FC63728F1B052C12584AD004A6628/\\$file/1919338E.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/931FC63728F1B052C12584AD004A6628/$file/1919338E.pdf).
- Schrittwieser J., Antonoglou I., Hubert T., Simonyan K., Sifre L., Schmitt S., Guez A., Lockhart E., Hassabis D., Graepel T., Lillicrap T., Silver D. (2019), *Mastering Atari, Go, Chess and Shogi by Planning with a Learned Model*, testo disponibile al sito: <https://arxiv.org/abs/1911.08265>.
- Science (2018), “A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play”, *Science*, 362: 6419, testo disponibile al sito: <https://science.sciencemag.org/content/362/6419/1140>.
- Security Intelligence (2018), *DeepLocker: How AI Can Power a Stealthy New Breed of Malware*, testo disponibile al sito: <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>.
- UNIDIR (2018), *The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence – Autonomous Weapon Systems and Cyber Operations*, UNIDIR Resources, n. 7, testo disponibile al sito: <https://unidir.org/sites/default/files/publication/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf>.
- UNIDIR (2018), *The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence*. UNIDIR Resources, n. 8. Geneva, United Nations Institute for Disarmament Research, testo disponibile al sito: <https://www.unidir.org/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf>

## 4. Sviluppo e applicazioni delle armi semi-autonome e autonome letali

di Michael Malinconi, Juan Carlos Rossi

### 4.1. Introduzione

Armi autonome e robot killer richiamano alle nostre menti scenari fantascientifici spesso oggetto della filmografia distopica, come il Terminator di Schwarzenegger o i robot-alieni di Transformers. Immaginazioni di un futuro ritenuto lontano. Come spesso accade, però, la realtà supera la fantasia. Nel maggio del 2021 un rapporto ONU<sup>1</sup> informava sul possibile primo uso di droni autonomi in combattimento. Il rapporto parlava dei droni turchi STM Kargu-2 che nei campi da battaglia libici avrebbero ingaggiato autonomamente il bersaglio senza necessità di connessione dati con un operatore.

Lo sviluppo tecnologico nel campo della robotica militare, grazie anche ai progressi in campo digitale, consentirà in un futuro non troppo distante di realizzare robot capaci di svolgere compiti e azioni tipici dell'intelligenza umana. Stiamo parlando dei LAWS sistemi d'arma in grado di selezionare e attaccare gli obiettivi senza l'intervento umano, considerando molteplici variabili contemporaneamente al fine di intraprendere la scelta migliore in ogni situazione (Scharre e Horowitz, 2015, p. 5). In base a profili biometrici e dati raccolti tramite sensori di bordo, tali armi potrebbero dunque identificare, selezionare e attaccare in totale autonomia qualsiasi obiettivo. Il rischio di omicidi mirati (*targeted killings*), decisi e condotti da macchine non è mai stato così alto.

I sistemi autonomi letali sono in fase di crescente sviluppo. Secondo Paul Scharre (2020), vicepresidente e Direttore degli studi del think tank americano CNAS, l'autonomia di una macchina può essere suddivisa in tre livelli: nel primo la macchina si definisce automatica (*automatic*) in quanto è capace

<sup>1</sup> United Nations Security Council, Final Report of the Panel of Experts on Lybia established pursuant to Security Council resolutions 1973 (2011). UN Doc. S/2021/229, 8 marzo 2021, p. 17.

di svolgere compiti semplici e ripetitivi. Nel secondo si definisce automatizzata (*automated*) e comprende le macchine che svolgono compiti complessi basati su regole preimpostate. Infine, nel terzo si definiscono autonome (*autonomous*) le tecnologie capaci di assolvere compiti senza l'apporto umano. La particolarità di tale step è l'impostazione *goal-oriented*: le macchine sono quindi programmate al perseguimento di obiettivi complessi. È su questa terza dimensione che gli Stati si stanno misurando. Non è stato ancora raggiunto, infatti, un livello di sviluppo tale da poter dispiegare armi autonome letali in contesti operativi senza un alto rischio di errore fatale. Per questo motivo persiste una qualche forma di controllo umano su alcune delle loro funzioni operative. Questo non significa, tuttavia, che molti Stati non stiano puntando su tali sistemi per renderli operativi in contesti complessi già nell'arco dei prossimi due decenni (Wyatt, 2021, p. 45).

La corsa tra le grandi potenze verso la dotazione di armamenti sempre più autonomi e letali è già iniziata. Attori come Stati Uniti, Federazione Russa, Israele, Cina, India ed alcuni paesi della NATO, infatti, già da tempo hanno intrapreso questo nuovo percorso, sostenendo i benefici di tali armi, quali la maggior precisione e la conseguente "riduzione di perdite umane". Apparentemente incuranti delle loro ambiguità etiche e legali e dei rischi legati a un eventuale malfunzionamento, essi finanziano e sostengono numerosi progetti, coinvolgendo anche settori dell'industria tecnologica privata e dipartimenti universitari.

È chiara anche la volontà di rimuovere qualsiasi ostacolo che possa frenare lo sviluppo dei LAWS di ultima generazione. Ne è dimostrazione la Sesta Conferenza di Revisione della Convenzione delle Nazioni Unite sulle armi convenzionali (CCW) del dicembre 2021<sup>2</sup>, di cui si tratterà più approfonditamente nei capitoli 9 e 10. Approfittando del fatto che la Convenzione utilizza il metodo del consenso<sup>3</sup>, i veti incrociati di Stati Uniti, Russia e India hanno ostacolato qualsiasi limitazione effettiva sull'uso di armi autonome letali. Nessun accordo è stato raggiunto nemmeno sulle raccomandazioni. Le grandi potenze non hanno voluto legarsi a un documento vincolante e hanno proposto un "code of conduct", cioè un documento non legalmente valido.

<sup>2</sup> UN Office for Disarmament Affairs, Final Document of the Sixth Review Conference, UN Doc. CCW/Conf.VI/11, 10 gennaio 2022; Human Rights Watch, Killer Robots: Military Powers Stymie Ban, 19 dicembre 2021.

<sup>3</sup> Pratica diffusasi in seno alla Nazioni Unite che non richiede una votazione formale per l'approvazione di una risoluzione. Per prevenire un accordo, è sufficiente che uno Stato presenti obiezioni alla risoluzione. L'accordo generalizzato deve essere constatato dal Presidente dell'organo.

## 4.2. Sviluppo e investimenti sui LAWS a livello internazionale

Al fine di comprendere come le maggiori potenze mondiali vogliano utilizzare le armi autonome nei conflitti armati, è utile analizzare i programmi e le strategie dedicate al loro potenziamento.

Negli Stati Uniti, relativamente più trasparenti in materia di difesa, i punti chiave della politica di difesa e sicurezza, inclusi i finanziamenti e le priorità nella Ricerca e Sviluppo (R&S) della IA, sono appannaggio del Department of Defense (DoD). Il DoD ha investito più di 18 miliardi di dollari tra il 2015 e il 2020 nel settore delle tecnologie autonome (Boulanin e Verbrugen, 2017). Nel settembre 2018, il Pentagono si è impegnato a compiere il più grande investimento fino ad allora mai registrato nel campo dell'automazione, per "sviluppare la prossima ondata di tecnologie di IA", impegnandosi a spendere diversi miliardi di dollari nei prossimi anni attraverso la DARPA (Defense Advanced Research Projects Agency) (PAX, 2019a, p. 4). Il budget del Dipartimento della Difesa per il 2020 includeva quasi 4 miliardi di dollari per i sistemi autonomi e 927 milioni per la IA. La volontà statunitense di essere all'avanguardia nel campo delle armi autonome letali era già chiara nell'*Offset strategy* del 2014, la terza nella storia americana (Petroni, 2015, p. 143)<sup>4</sup>. L'obiettivo di questa strategia, secondo l'allora Segretario alla Difesa Robert O. Work, è quello di sfruttare tutti i progressi dell'intelligenza artificiale e dell'autonomia per poi acquisire vantaggi strategici sul campo di battaglia, rafforzando le prestazioni e la deterrenza a stelle e strisce<sup>5</sup>.

È importante poi ricordare che le sinergie tra aziende civili e il DoD sono continue e finanziariamente proficue. Gli Stati Uniti sponsorizzano numerosi progetti in enti di ricerca civili e università. Tra questi, si segnala la National Robotic Initiative, che ha finanziato progetti di robotica con varie agenzie governative dal 2011. La DARPA ha sviluppato anche un'efficace competizione tra enti civili con ingenti premi in denaro che è stata ripresa in seguito da numerosi Stati, inclusi Russia, Cina e Regno Unito (Wyatt, 2001, p. 98).

Il ruolo cruciale della IA era già stato riconosciuto nel 2018 con l'istituzione del centro di eccellenza della Difesa, il Joint Artificial Intelligence Center (JAIC), e nel 2019 quando il Congresso ha voluto istituire la National Security Commission on Artificial Intelligence, composta da esperti indipendenti. Nel report finale del 2021, la Commissione ha richiamato il governo statunitense, ma anche gli alleati della NATO, a investire ingenti risorse in tale campo per non perdere il vantaggio relativo acquisito. Il JAIC ha il

<sup>4</sup> La prima imperniata sulle armi nucleari negli anni '50; la seconda, invece, sul bombardamento di precisione.

<sup>5</sup> Department of Defense, "Remarks by Deputy Secretary Work on Third Offset Strategy", 28 aprile 2016.

compito di fornire la competenza necessaria a identificare, prioritizzare e rendere operativi gli sforzi del DoD nel campo della IA. Mentre la DARPA si concentra su progetti a lungo termine, il JAIC opera su quelli a breve termine che mostrano capacità applicabili in contesti di conflitto armato.

Alcuni tra i programmi più ambiziosi in fase di sviluppo sono:

- il *Collaborative Operations in Denied Environment* (CODE), che mira a sviluppare nuovi algoritmi o software per gli Unmanned Aerial Vehicles (UAV) già esistenti. Tale programma estenderebbe la capacità di missione dei droni e migliorerebbe la capacità delle forze statunitensi di condurre un attacco in uno spazio aereo ostile. Il controllo di un operatore resta pur sempre necessario. Tuttavia, i velivoli dotati di tale sistema sarebbero in grado non solo di scovare e ingaggiare gli obiettivi, ma anche di adattarsi a situazioni dinamiche come l'emergere di minacce impreviste;
- il programma ATLAS, un sistema automatizzato avanzato di targeting che prevede l'utilizzo della IA e dell'apprendimento automatico per fornire ai veicoli di terra capacità di bersagli autonomi in modo da consentire alle armi di acquisire, identificare e ingaggiare un obiettivo in tempi almeno tre volte più rapidi dell'attuale processo manuale;
- il progetto *Ghost Fleet Overlord* dello Strategic Capabilities Office (SCO) che ha come obiettivo la costruzione della prima nave da guerra senza pilota prodotta in larga scala. Tali navi, gli Unmanned Surface Vehicles (USV), sarebbero totalmente autonome, in grado di compiere missioni di monitoraggio ma anche di combattimento in alto mare senza equipaggio;
- il progetto *Global Information Dominance Experiment* (GIDE) che utilizza l'IA e il machine learning per combinare dati raccolti da altre fonti e formulare previsioni. Tali previsioni potrebbero conferire alle forze statunitensi un vantaggio temporale non di ore ma di giorni.

Per quanto riguarda i Paesi membri della NATO, il Regno Unito è tra quelli che più investono nel settore delle armi autonome. Nel dicembre del 2018, un rapporto del Ministero della Difesa ha promosso un maggiore uso della IA per respingere eventuali ritorsioni militari (PAX, 2019a, p. 19). A condurre la ricerca in questo ambito sono soprattutto l'azienda privata Qinetiq e la DSTL (Defence Science and Technology Laboratory), agenzia esecutiva del Ministero della Difesa (Boulain e Verbruggen, 2017, p. 97).

Tra i vari sforzi del Ministero della Difesa britannico, va segnalato, inoltre, il programma *Autonomy*, volto proprio ad accrescere le capacità belliche del Paese. Per implementarlo, è sorto il *Defence Capability for Autonomous and Novel Technologies* (DECANT), ovvero una struttura dedicata alla costruzione di una rete di fornitori per le tecnologie dei sistemi autonomi.

Ancor più indicativo dell'interesse di Londra nei confronti delle nuove tecnologie è la cooperazione tra settore pubblico e privato già da tempo in

atto. Le iniziative intraprese, infatti, pur partendo con lo sviluppo di semplici applicazioni di sicurezza, potrebbero costituire un eventuale trampolino di lancio per un più ampio uso militare. Ne è esempio l'Euroswarm di DSTL che punta allo sviluppo di uno swarm di droni a basso costo da utilizzare in operazioni di sorveglianza. Inoltre, il Ministero della Difesa al suo interno può contare anche sul Defence and Security Accelerator (DASA), che ha il compito di individuare e finanziare quelle innovazioni in grado di supportare la sicurezza e la difesa del Paese, al fine di mantenere così un vantaggio strategico nei confronti di Stati concorrenti.

Anche la Francia sta finanziando tramite fondi governativi la ricerca accademica e industriale per le applicazioni militari. Nel marzo del 2018, ha presentato un piano quinquennale di sviluppo e potenziamento dell'intelligenza artificiale nazionale con un budget di 1,5 miliardi di euro. La strategia nazionale francese, preparata dal matematico Cédric Villani, ha preso il nome di *AI Policy Report* e si concentra su quattro settori prioritari per lo sviluppo della IA: sanità, mobilità e trasporti, ambiente, difesa e sicurezza. Nel 2021, è stato annunciato un nuovo progetto di raccolta di dati e dataset per l'IA. Da qui la necessità di costruire sinergie attorno all'innovazione civile e militare nell'ambito dell'intelligenza artificiale. Investimenti che, facenti parte di una strategia più ampia, mirano a implementare quei sistemi di IA che fanno uso del DL.

Israele è da anni pioniera nel campo delle armi autonome con i droni "kamikaze", i robot da battaglia Robattle, i veicoli senza pilota e la mitragliatrice automatica Sentry-Tech. Ci sono pochi dubbi sul fatto che il complesso militare industriale guidi il successo tecnologico di Tel Aviv, combinando sviluppo autoctono e vendite estere. Non a caso, l'operazione "Guardiani delle Mura" del 2021 è stata definita da Israele la prima guerra dell'intelligenza artificiale, dato il pesante contributo del *machine learning* nell'individuazione di obiettivi di Hamas o della Jihad Islamica Palestinese da colpire. Le forze di difesa israeliane (IDF) utilizzano da anni l'intelligenza artificiale per centralizzare e analizzare tutti i dati raccolti sulle minacce alla sicurezza del paese. Gli investimenti sulla IA continuano. Israele investirà più di 1,6 miliardi di dollari nei prossimi cinque anni.

La Corea del Sud, settima al mondo per consistenza delle forze armate, non ha trascurato il settore delle armi autonome. Grazie a numerosi investimenti, Seul si è affermata come leader nel campo dei robot industriali e, nel 2016, ha deciso di investire 840 milioni di dollari per incrementare la ricerca e lo sviluppo sull'intelligenza artificiale. Gli investimenti governativi vanno di pari passo con l'istituzione della ricerca a guida civile (Boulanin e Verbruggen, 2017, p. 101). Il governo di Seul ha affidato a varie organizzazioni la gestione dell'innovazione militare: la *Defense Acquisition Programme Administration*,



responsabile della compravendita di sistemi d'arma e tecnologie; l'*Agency for Defense Development*, il principale centro di ricerca e di sviluppo sull'intelligenza artificiale che ha l'obiettivo di modernizzare le proprie applicazioni militari con l'IA e di sviluppare la prossima generazione di armi da combattimento<sup>6</sup>; e il *Korea Institute for Defense Analyses*, che ha più una funzione consultiva. La collaborazione con enti privati, all'avanguardia in Corea del Sud, e con università rappresenta un altro importante fattore di competitività. Nel febbraio 2018 il *Korea Advanced Institute of Science and Technology* (KAIST), sede dell'*Unmanned Systems Research Group*, ha annunciato che avrebbe collaborato con Hanwha Systems<sup>7</sup>. Proprio l'industria militare sudcoreana, la dodicesima al mondo con un fatturato superiore ai tre miliardi nel 2017, fornisce una spinta essenziale al settore delle armi autonome. Questa cooperazione ha dato vita al Centro di ricerca per la Convergenza della Difesa Nazionale e dell'Intelligenza Artificiale (Saalman, 2019, p. 34), il quale conduce ricerche relative sia alla guerra informatica sia alla robotica IA.

Con lo sviluppo di LAWS la Corea del Sud aspira a disporre di un'ulteriore arma per contrastare le provocazioni non nucleari della Corea del Nord riducendo il costo di vittime umane (Saalman, 2019, p. 34).

Anche la Federazione Russa sta investendo molto nello sviluppo di armi letali autonome nel quadro della sua nuova dottrina militare mirante a raggiungere una parità strategica con USA e NATO. Nel 2017 il Presidente russo Putin ha affermato che la nazione che diventerà leader nel campo dell'intelligenza artificiale "governerà il mondo". Armi autonome russe sono già state impiegate in combattimento in Siria e Libia. La strategia russa di sviluppo della IA non è guidata direttamente dal governo, bensì da imprese governative, come la Yandex e la banca Sberbank (Petrella, Miller, Cooper, 2021). Ciononostante, la robotica militare svolge ormai da tempo un ruolo prioritario nella nuova politica di riarmo della Russia, con un budget stimato di circa di 346 miliardi di dollari per il periodo 2016-2025 (Boulanin e Verbruggen, 2017, p. 98). Sviluppi significativi, in questo contesto, sono stati il lancio del programma Robotics 2025 e la creazione dello Skolkovo Robotics Center (SRC) nel 2014. Il primo, il Robotics 2025, è implementato dal Ministero della Difesa e dalla Foundation for Advanced Studies (FPI), nuovo centro di ricerca ed equivalente russa del DARPA (Boulanin e Verbruggen, 2017, p. 98). Il SRC, invece, nasce con l'intento di migliorare la sinergia tra decine di istituti di ricerca statali, universitari e aziendali nel campo della robotica. Dove lo sviluppo autoctono non riesce ad arrivare, Mosca compen-

<sup>6</sup> Soprattutto di UAV, identificati come uno dei nuovi settori per il rafforzamento del suo apparato militare.

<sup>7</sup> La divisione della Difesa del Gruppo Hanwha, per la ricerca e lo sviluppo di armi di intelligenza artificiale.

sa con il commercio internazionale, soprattutto attraverso l'importazione di sistemi d'arma israeliani.

Progressi significativi sono quelli ottenuti da Kalashnikov, il più grande produttore di armi della Russia, che nel 2017 ha annunciato di aver sviluppato un modulo di combattimento completamente automatizzato basato su tecnologie di reti neurali che, se confermato, consentirebbero sia di identificare obiettivi sia di prendere decisioni autonomamente. Tuttavia, ad oggi la Kalashnikov non ne ha presentato sul mercato alcun modello.

Anche la Cina attribuisce alla IA un'alta priorità per accrescere il proprio prestigio internazionale e promuovere l'ammodernamento dell'Esercito di Liberazione Popolare (Kania, 2020). Non sono disponibili stime ufficiali, tuttavia è chiaro che Pechino stia puntando molto su questo settore sino ad investire nel solo 2022 circa 1,3 miliardi di dollari (Wyatt, 2021, p. 98).

Pechino ha iniziato a muovere i primi passi nel settore delle armi autonome già dal 1986, con il programma 863, piano di sviluppo di alto livello statale, dove veniva stabilita la base delle attività di R&S per la IA e la robotica, con l'obiettivo di sviluppare un'innovazione nei settori tecnologici più avanzati, in particolare l'informatica e l'automazione. Dal 2014, poi, è stata formulata una serie di piani economici e scientifici, tra cui il tredicesimo piano quinquennale per lo sviluppo economico e sociale della Repubblica Popolare Cinese (2016-2020), tesi a promuovere lo sviluppo tecnologico. Nel 2016 la Cina ha pubblicato due piani dedicati alla IA e alla robotica: il piano dello sviluppo dell'industria della robotica (2015-2016) e la guida triennale per internet plus (2016-2018). Quest'ultimo ha poi aperto la strada a tre centri di ricerca congiunti, guidati da Baidu, l'equivalente cinese di Google per il *deep learning*, i *big data* e la IA.

Infine, il Piano di sviluppo per una nuova generazione d'intelligenza artificiale del 2017 delinea la strategia cinese in tre mosse: la prima riguarda il mantenimento della tecnologia globale e l'applicazione della IA a un livello avanzato entro il 2020; nella seconda si prevede di ottenere rilevanti scoperte in termini di teoria della IA base entro il 2025; ed infine, l'affermazione entro il 2030 del Paese come leader mondiale in questo settore.

A preoccupare i suoi avversari è il rapido sviluppo tecnologico della Repubblica Popolare. L'ex capo software del Pentagono ha recentemente dichiarato che la Cina avrebbe già vinto la corsa all'intelligenza artificiale<sup>8</sup>. Inoltre, vi è diffusa preoccupazione che Pechino adotti anche per i LAWS, come in passato per altri tipi di armi, una politica di vendita flessibile, rifor-

<sup>8</sup> Beals M. (2021) "Former Pentagon official says China has won artificial intelligence battle" The Hill. Disponibile anche a <https://thehill.com/policy/cybersecurity/576213-former-pentagon-official-says-china-has-won-artificial-intelligence>.

nendo Stati definiti «problematici» a causa delle loro sistematiche violazioni dei diritti umani.

Veniamo infine all'India, che ha effettuato ingenti investimenti nel campo della IA, della robotica, dei LAWS e delle tecnologie quantiche allo scopo di migliorare le proprie capacità belliche, soprattutto sulle frontiere pakistana e cinese (Shashank, 2016). In particolare, si è concentrata nell'acquistare droni armati e missile sonici, nonché sullo sviluppo autonomo come con il progetto *Artificial Intelligence Offensive Drone Operations*. Lo sviluppo tecnologico domestico si basa sulla partnership tra aziende governative e startups private, in particolare Bharat Electronics Limited, e si sta concentrando su riconoscimento facciale e robotica.

### 4.3. Caratteristiche e prospettive dei nuovi sistemi d'arma

Come abbiamo visto, molti Stati già detengono e utilizzano armi in grado di svolgere operazioni in semi-autonomia. Appare ora opportuno approfondire le loro funzionalità e capacità tecniche, sottolineando le caratteristiche proprie di ciascuna tipologia di sistema d'arma autonoma (o semi-autonoma). Per ogni tipologia è poi possibile individuare specifici modelli sviluppati dai singoli Stati. Per consultarne una lista si rimanda all'Appendice.

#### 4.3.1. Munizioni loitering

Pur mancando una definizione precisa, con il termine di munizioni *loitering*, cioè circuitanti, si fa generalmente riferimento a munizioni da bombardamento o “droni-kamikaze”. Una sorta di ibrido tra un *Unmanned Aerial System* (UAS) e un missile guidato. Le munizioni *loitering* sono disponibili in varie dimensioni<sup>9</sup>. Queste armi sono dotate di telecamere elettro-ottiche e a infrarossi che consentono di localizzare, sorvegliare e guidare il velivolo verso il bersaglio designato. La caratteristica operativa che le contraddistingue è la capacità di volare per un tempo prolungato, dando così la possibilità di individuare e colpire un bersaglio sul campo di battaglia senza alcun intervento umano. Sono utilizzabili sia in missioni offensive sia in missioni difensive. Alcuni modelli, inoltre, come quelli utilizzati in operazioni SEAD

<sup>9</sup> Alcuni, quelli più piccoli, possono essere trasportati in uno zaino dalle truppe, mentre quelli più grandi hanno una dimensione pari a quella dei missili con un peso fino a 32 kg. I modelli più grandi, inoltre, hanno potenzialmente la capacità di tornare alla base se non trovano alcun obiettivo o se la missione viene interrotta. Tuttavia, la maggior parte dei circuitanti si autodistrugge in volo.

(Suppression of Enemy Air Defences), possono funzionare addirittura in completa autonomia dopo il lancio.

Dato il loro basso costo, a differenza degli Unmanned Combat Aerial Vehicles (UCAV) o degli Unmanned Underwater Vehicles (UUV), sono sempre più utilizzati da un vasto gruppo di attori statali e non statali. A primeggiare nel settore sono gli Stati Uniti che, con Israele, hanno aperto la strada allo sviluppo di questo genere di armi. Le munizioni *loitering* sono diventate armi di primaria importanza nel conflitto in Ucraina dove entrambe le parti ne hanno fatto ampio uso. Sorprendente è stato anche lo sviluppo delle munizioni *loitering* turche, utilizzate con grande efficacia in Siria, Libia e dall'Azerbaijan in Nagorno-Karabakh.

#### **4.3.2. I sistemi d'arma ravvicinati o a corto raggio (CIWS)**

I sistemi d'arma ravvicinati (*Close-in weapon system*) sono apparati mobili per la difesa antiaerea e antimissilistica. I CIWS esistono già da molto tempo: il Mark 56, primo del suo genere, è stato ideato durante la Seconda guerra mondiale. Ben 89 Paesi oggi dispongono di tale tipologia di armi e ben 63 di questi ne hanno schierate, col tempo, diverse varianti (Boulanin e Verbruggen, 2017, p. 37).

Oggi essi sono capaci di intercettare e distruggere autonomamente proiettili negli ultimi secondi di volo dei medesimi prima dell'impatto. A differenza di altri sistemi per la difesa, i CIWS sono concepiti per cercare di fermare qualunque minaccia a obiettivi ritenuti particolarmente costosi, delicati ed importanti. Per questo, sono soprattutto utilizzati per la difesa di unità marine. Tuttavia, i CIWS possono essere utilizzati anche su terraferma in funzione antimissile, di artiglieria o di mortaio.

I CIWS difensivi possono essere classificati come automatici, in quanto programmati per individuare proiettili potenzialmente ostili, calcolarne la traiettoria, trasferire quest'informazione al centro di controllo e determinare il luogo d'impatto previsto. Se il proiettile costituisce un'effettiva minaccia, il sistema spara un missile intercettore per provocare la detonazione del missile lontano dall'area d'impatto. In genere, le caratteristiche di velocità reattiva e di difesa anche a distanze ridottissime richiedono che le munizioni siano d'artiglieria. La gittata utile è di circa 2-3 km, ma gli ingaggi contro i principali obiettivi, come i missili antinave, per esempio, avvengono spesso anche a distanze minori. Il loro obiettivo in tutti questi casi è quello di rilevare, tracciare, selezionare le priorità e rispondere alla minaccia in modo più rapido e preciso di quanto potrebbe fare un operatore umano.

Esistono due varianti di CIWS: una a base di armi multiple a canne rotanti

e l'altra basata su missili. I sistemi a canne rotanti possiedono tuttavia una bassa gittata e non assicurano generalmente l'abbattimento del proiettile nemico. Infatti, modelli come i Goal Keeper o i Phalanx, a canne rotanti, sono stati sviluppati per difendere una zona limitata, mentre i sistemi di difesa missilistica come l'Iron Dome possono fornire protezione su una più ampia area geografica. Inoltre, i CIWS terrestri, come il Centurion C-RAM (Counter Rocket artillery and mortar), sono stati ideati contro proiettili in arrivo, mentre il Phalanx, che opera su navi, può difendersi anche da veicoli di superficie. Recentemente, è degno di nota lo sviluppo di CIWS basati su tecnologia laser<sup>10</sup>, che renderebbe più precisa l'individuazione e l'abbattimento.

La maggior parte di CIWS sopra elencati adotta principalmente come tipo di contromisura, misure *Hard Kill*, per abbattere le minacce in arrivo. Alcuni, più sofisticati modelli possono utilizzare invece misure cosiddette di *Soft Kill*<sup>11</sup>.

Simili ai CIWS ma di calibro inferiore, vi sono le cosiddette “sentinelle robotiche”, definite anche come armi antiuomo. La robotica è diventata una caratteristica fondamentale delle tecnologie destinate al controllo delle frontiere, anche se questi strumenti sono ancora abbastanza rari e si possono citare solo tre modelli (v. Appendice). I più utilizzati in questo settore sono senza dubbio i droni aerei, capaci di pattugliare per diverse ore ampie porzioni di territorio.

### **4.3.3. Veicoli aerei da combattimento senza equipaggio-Unmanned Combat Aerial Vehicles (UCAV)**

Ciò che viene comunemente definito drone è un veicolo senza pilota, guidato in ambiente ostile tramite pilotaggio remoto o attraverso un computer di bordo. La tipologia maggiormente diffusa, prodotta e utilizzata di droni è quella aerea: gli UAV.

Quando sono armati vengono generalmente definiti UCAV. In genere, i droni militari vengono utilizzati per scopi di sorveglianza, ricognizione e intelligence<sup>12</sup>.

Con gli attuali progressi in questo campo, c'è una pressione su tutte le forze militari aeree per sviluppare ed implementare gli UCAV e renderli completa-

<sup>10</sup> All'avanguardia su questo tipo di tecnologia sono la Marina statunitense e quella turca.

<sup>11</sup> Con il termine *Hard Kill* si intendono tutte quelle misure che fisicamente contrattaccano una minaccia in arrivo, mentre, con *Soft Kill* quelle contromisure elettroniche che modificano la firma elettromagnetica o di altro tipo del sistema mirato, alterando così il rilevamento della minaccia in arrivo (es. missile guidato).

<sup>12</sup> Per un resoconto più esaustivo sul funzionamento e sulla legalità dei droni si rimanda a Malinconi, 2021.

mente autonomi nell'individuazione e attacco del bersaglio. Pur essendo di varie dimensioni, i droni più resistenti e letali sono i cosiddetti “droni strategici”. Questi possono raggiungere velocità superiori ai 600 km/h, possiedono un'autonomia superiore alle 24 ore e possono raggiungere anche altezze di 15.000 metri con una capacità di carico anche di alcune tonnellate di chili. Raggiungono svariati metri di lunghezza e sono dotati di piattaforme multi-missione. In genere, possiedono nel muso una varietà di sensori: sensori di ripresa che permettono di avere numerosi campi visivi in tempo reale, radar in grado di individuare il bersaglio (quali il *moving target indication* o il *stationary target indication*), laser di puntamento, intensificatori d'immagini e telecamere a infrarossi in caso di condizioni atmosferiche avverse.

Ogni drone tattico o strategico comunica con la propria stazione di controllo a terra attraverso onde radio o attraverso un satellite quando è fuori raggio<sup>13</sup>. Se il drone opera a lunga distanza dalla base operativa i dati gli vengono comunicati da basi militari o avamposti posti a metà strada tra il pilota e l'area di operazione. Il decollo e l'atterraggio sono manovrati localmente dall'operatore, così come il puntamento e il lancio dei missili. Inoltre, le immagini del drone possono essere visionate in diretta dalle truppe a terra, attraverso comunicazioni satellitari, per avere una visuale migliore dell'ambiente e fornire informazioni logistiche. Le armi più comuni che vengono caricate sui droni sono missili Hellfire e bombe laser. Esistono anche droni, definiti droni-kamikaze, pensati non per sganciare armamenti ma per esplodere una volta raggiunto il bersaglio. Recentemente è stata utilizzata una variante non esplosiva di missili Hellfire (R9X) con testata cinetica e lame a scomparsa, destinata a ridurre i danni collaterali.

Ad oggi, almeno sedici Stati e attori non statali hanno condotto operazioni militari implicanti l'uso della forza con droni armati (Malinconi, 2021, pp. 20-32).

#### **4.3.4. Munizioni guidate di precisione**

Conosciute anche come “bombe intelligenti”, sono proiettili esplosivi che, in volo e in tempo reale, possono correggere il bersaglio iniziale o eventuali errori successivi (Scharre e Horowitz, 2015, p. 11). Il loro primo utilizzo risale alla prima metà del secolo scorso, quando i prototipi erano guidati tramite onde radio. Nel tempo, sono stati sviluppati esemplari guidati da impulsi

<sup>13</sup> Ciò può presentare importanti limiti, poiché il segnale satellitare può essere facilmente intercettato, interrotto o falsificato per via della distanza in cui si trova ad operare rispetto alle fonti di disturbo nemiche.

a infrarossi, laser e radar. Gli ultimi modelli sono guidati tramite comunicazioni satellitari, in particolare tramite GPS.

Le ultime ricerche tendono a sviluppare munizioni guidate capaci di colpire bersagli in movimento anche senza GPS. Composte da quattro componenti di sistema (targeting/guida, sistema di volo, motore e testata), possono essere usate per molteplici scopi, tra i quali missili balistici, missili cruiser, missili anti-nave, missili anti-carro (PAX, 2017, p. 11).

#### ***4.3.5. Veicoli terrestri senza equipaggio-Unmanned Ground Vehicles (UGV)***

In grado di operare senza la necessità di un controllo umano, gli UGV (Unmanned Ground Vehicles) sono utilizzati in diverse operazioni quali la ricognizione, il pattugliamento, il supporto di fuoco diretto, lo sminamento, il carico e lo scarico di armi. Mentre i veicoli aerei e marini senza equipaggio operano in ambienti privi di ostacoli, i sistemi terrestri si trovano invece ad agire in ambienti logisticamente imprevedibili. Ciò spiega come mai per anni gli UGV siano stati ignorati dal settore bellico. I progressi dell'ultimo decennio, tuttavia, hanno permesso di colmare un divario che sembrava impensabile.

Per rilevare gli ostacoli gli UGV devono calcolare la geometria e la composizione del terreno, in qualunque tipo di condizione e/o di scarsa visibilità (Matthies, Kelly, Litwin e Tharp, 1996). I veicoli terrestri fanno così molto affidamento sul GPS, rendendoli di fatto vulnerabili a eventuali tecnologie di disturbo del segnale, e sulla necessaria supervisione umana.

La Russia, grazie ai suoi numerosi progetti, si sta sempre più imponendo come nuovo leader del settore.

#### ***4.3.6. Veicoli marini senza equipaggio-Unmanned Marine Vehicles (UMV)***

I veicoli marini senza equipaggio possono operare sia in superficie (Unmanned Surface Vehicle, USV) sia sott'acqua, UUV. Sono tecnologie semi-autonome capaci di raggiungere aree non facilmente accessibili all'uomo, assicurando un rischio più basso o minimo per gli operatori, e dotate di capacità sia offensive sia difensive. Il loro aspetto più rivoluzionario è il fatto di operare come moltiplicatori della forza, aumentando la capacità di ricognizione, sorveglianza e protezione delle truppe (Wyatt, 2021, p. 69). Si pensi, ad esempio, all'utilizzo di sottomarini autonomi statunitensi per la bonifica da ordigni bellici del porto di Umm Qasr in Iraq nel 2003. Anche la

NATO ha puntato molto sugli UMV, ritenendoli un punto di svolta per affrontare le molteplici minacce nel settore marittimo.

Gli UUV sono ampiamente utilizzati per l'esplorazione e la ricerca dei fondali marini. Nondimeno, possono essere molto utili in missioni di ricognizione, ricerca e salvataggio, sorveglianza, combattimento marino e guerra asimmetrica. Mentre gli USV si basano su comunicazioni di tipo standard, soprattutto satellitari, la comunicazione tra operatori e UUV rimane un fattore di rischio. Data l'impossibilità di utilizzare metodi standard di navigazione (ad esempio il GPS), gli UUV si affidano a onde acustiche anziché alle classiche onde elettromagnetiche. I segnali acustici possono essere facilmente disturbati dall'acqua e sono più lenti di altri tipi di onde, rendendo l'intera comunicazione operatore-mezzo più complessa. Proprio per questo motivo, la maggior parte di questi UUV, privi di equipaggio, richiede un certo grado di autonomia (UNIDIR, 2015, pp. 3-4).

#### 4.4. Lo *swarm*

Lo *swarm*, o sciame, rappresenta un passo in avanti verso nuovi livelli di autonomia. Composto di unità più simili ai droni che ai LAWS, lo *swarm* si basa sulla possibilità di utilizzare un gruppo di singoli sistemi che interagiscono ed operano come un unico attore collettivo. Lo sciame ha il principale vantaggio di superare i limiti imposti dalla dinamica drone-pilota, permettendo a molteplici unità di essere sotto il controllo di un unico operatore (UKDJ, 2019).

A distinguerlo sono due elementi essenziali: la comunicazione interna e il coordinamento. Ciò nonostante, le singole unità (UAS, UGV, etc.), o nodi, che lo compongono, pur non essendo ciascuno in sé particolarmente avanzato, insieme consentono, attraverso il coordinamento e la distribuzione delle attività, l'esecuzione di missioni complesse.

Generalmente, lo *swarm* viene identificato come una raccolta di sistemi, tanto semplici quanto complessi, omogenei ed eterogenei, spesso privi di equipaggio<sup>14</sup>, con quattro principali strutture di comando includibili a loro volta in due grandi categorie: centralizzati e decentralizzati (Verbruggen, 2019, p.4). Quelli centralizzati sono divisibili in controllo generalizzato, dove un'unità leader guida e controlla tutti i singoli nodi senza un coordinamento gerarchico. Tra i loro vantaggi vi è quello di trovare soluzioni in maniera più rapida ai vari ostacoli, con una maggiore fluidità e semplicità nella manovra. Come principale svantaggio presentano una maggiore sensibilità a una eventuale perdita dell'unità leader.

<sup>14</sup> Possono essere previsti anche sistemi con equipaggio o comandi a sensori ottici.



I secondi, invece, sono caratterizzati da un coordinamento per consenso, dove i nodi decidono collettivamente come muoversi per eseguire le missioni, in continua comunicazione. In quest'ultimo caso, ogni singolo nodo risponde alle varie unità che lo circondano, come nei branchi animali<sup>15</sup>. Più facili da espandere in termini di dimensioni, possono operare con una larghezza di banda e sono abili nel trovare soluzioni originali e complesse ai vari problemi presentati. In particolare, le decisioni che ciascun nodo prende si basano su informazioni localizzate anziché su informazioni aggregate a livello globale (Scharre, 2020, 14-23).

Le applicazioni degli *swarm* sono molteplici, dalla nano-robotica alle operazioni di ricerca e soccorso. Nonostante siano ancora in fase di sviluppo e svolgano compiti elementari, potrebbero presto essere utilizzati in operazioni di posizionamento di mine o per comporre unità di killer robots totalmente autonome. In quest'ottica, sono già stati testati in modalità da combattimento i primi *swarm* di UCAV e USV.

Nonostante ciò, risulta innegabile che un loro eventuale utilizzo consentirà in futuro notevoli vantaggi tattici: sono scalabili, possono cioè cambiare il numero delle loro unità in base alla missione da compiere; sono adattabili a varie tipologie di missioni; sono robusti, e se un singolo nodo fallisce, altri possono subentrare; sono relativamente economici, possedendo un basso costo unitario (Verbruggen, 2019, p. 3).

Particolarmente promettenti nel loro sviluppo sono quelli di tipo decentralizzato, poiché non necessitano di una comunicazione costante con l'operatore e mostrano una maggiore resistenza alle armi elettromagnetiche.

Ciononostante, un "controllo" degli *swarm* può essere esercitato in quattro principali modalità (Chakraborty *et al.*, 2016, pp. 8-9):

- tramite algoritmi che ne specificano il comportamento, gli operatori possono scegliere tra diversi pacchetti degli stessi, pre-programmati a seconda del comportamento desiderato.
- Attraverso la modifica dei parametri del loro algoritmo, funzione che permette di cambiare tanto il loro raggio di azione quanto la distanza massima o minima tra i diversi nodi.
- Con un controllo remoto dei nodi leader tramite input o messaggi intermittenti. Il nodo selezionato può così inviare i comandi agli altri nodi. Tuttavia, ciò rimane possibile solo se non vi sono ritardi nelle trasmissioni del segnale e con continui aggiornamenti sullo stato dello *swarm*.
- Alterando l'ambiente per influenzarne il suo comportamento. In que-

<sup>15</sup> Per un'efficace analisi della autoregolazione di prossimità tra esemplari della stessa specie, v. gli studi sugli stormi di stormi del premio Nobel per la fisica Giorgio Parisi (2021).

st'ultimo caso, tramite l'utilizzo di "feromoni virtuali"<sup>16</sup> viene indicato ai nodi quale area esplorare e quale evitare. Il comportamento non deriva da specifici comandi dell'operatore bensì dall'ambiente circostante o dalle modifiche apportate alle modalità con cui i nodi interagiscono tra loro.

Risulta evidente che, qualunque metodo si consideri, un controllo umano sicuro e affidabile rimane pur sempre una reale difficoltà operativa. Il problema è accentuato sia da quelle dinamiche poco lineari che limitano la valutazione effettiva delle sue prestazioni, sia dalle interazioni tra i diversi nodi che non possono essere completamente controllate dall'operatore durante la loro formazione. Inoltre, comandi non tempestivi rischiano di produrre non solo effetti opposti a quelli sperati, ma addirittura provocare conseguenze negative. Per un effettivo controllo, infatti un operatore potrebbe trovarsi nella situazione di dover optare per il concetto di "negligenza benevola": un metodo altamente controintuitivo che consiste nell'attendere e non dare istruzioni. Questi rischi sottolineano come gli *swarm* di tipo militare siano ancora poco adatti a eseguire funzioni altamente complesse.

Nonostante tutte le problematiche fin qui esposte, diversi Stati hanno già intrapreso progetti dimostrativi volti a sviluppare e migliorare questa tecnologia in ambito bellico. Tra i programmi attualmente in sviluppo e per i quali si hanno maggiori informazioni, vi sono: il programma OFFSET (Offensive Swarm Enabled Tactics) di DARPA, che mira a utilizzare sciame di centinaia di UAS e/o di UGV per compiere missioni in ambienti complessi come quelli urbani. Ne sono esempi il programma *US Navy Super Swarm Project*, che studia le modalità più efficaci di coordinamento tra unità, e il programma LOCUST (*Low-Cost UAV Swarming Technology*), che punta sul basso costo dello swarm per colpire le difese nemiche con un numero di unità superiore alle loro capacità di affrontarli.

Sempre della DARPA, il programma Gremlins mira a sviluppare UAS a basso costo riutilizzabili, basati su un'architettura che consente l'impiego di diverse tecnologie come payload avanzati in operazioni autonome. I Gremlins verrebbero lanciati al di fuori dal campo nemico e, una volta completata la missione, verrebbero recuperati in aria per poi tornare alla base operativa ed essere riprogrammati per una nuova operazione. Inoltre, durante il progetto CODE, sempre sviluppato dalla DARPA, *swarm* di droni sono stati capaci di compiere autonomamente le missioni assegnate senza collegamento con l'operatore.

<sup>16</sup> I dispositivi, come formiche in cerca di cibo, lasciano sul percorso una scia di dati ("feromoni") per guidare le altre unità dello swarm. Questi "feromoni virtuali" si basano sulle interazioni con l'ambiente e dalla posizione e, come veri feromoni, possono persistere nel tempo o svanire lentamente.

Israele ha utilizzato efficacemente *swarm* di droni durante l'operazione *Guardiani delle Mura* per individuare, localizzare e colpire militanti di Hamas a Gaza.

Anche a livello europeo sono presenti diversi programmi per lo sviluppo degli *swarm*. Il Roborder, progetto di Horizon 2020, ha l'obiettivo di sviluppare UAS eterogenei ed autonomi per il controllo delle frontiere, e l'Euroswarm, un progetto di Pilot Project, è volto a testare l'utilità degli *swarm* eterogenei per operazioni di sorveglianza e ricognizione (Verbruggen, 2019, p. 10).

Infine, anche la Cina sperimenta tecnologie simili. Nel 2017 la China Electronics Technology Group Corporation (CETC), società di proprietà statale, ha eseguito il lancio di 119 droni in grado di eseguire sia il decollo sia la formazione in volo. Secondo il CETC, infatti, "l'intelligenza dello sciame" è considerata il nucleo ed il futuro dei sistemi senza pilota.

## 4.5. Droni armati in azione: la guerra in Ucraina

Ogni guerra offre l'occasione di dispiegare e sperimentare nuovi sistemi d'arma. In questo senso, l'invasione russa dell'Ucraina nel febbraio 2022 non fa eccezione.

I droni, insieme alle munizioni *loitering* circuitanti, sono diventati uno strumento fondamentale e ubiquo del conflitto armato in Ucraina. Tali sistemi d'arma vengono utilizzati nelle loro due tradizionali funzioni: missioni ISR (intelligence, sorveglianza e ricognizione), a cui spesso si è aggiunta la video-registrazione di azioni di combattimento da diffondere per scopi propagandistici, e attacco. I droni, oltre a colpire direttamente i bersagli, hanno svolto importanti funzioni di combattimento quali il *buddy lasing* (che consiste nel segnalare il bersaglio tramite laser affinché l'artiglieria o altri veicoli lo colpiscano), l'individuazione del bersaglio (l'attacco elettronico in cui i droni interrompono, disturbano o distruggono sistemi elettronici armati nemici) e l'*artillery spotting* (fare da vedetta per l'artiglieria). Talvolta, a causa della mancanza diUCAV, entrambe le parti hanno utilizzato droni da ricognizione per sganciare materiale esplosivo sopra obiettivi nemici.

Anche le munizioni *loitering* hanno ricevuto particolare attenzione. Esse rappresentano un'arma formidabile in contesti di conflitto armato ravvicinato, data la loro dimensione variabile e la loro capacità di volare sui bersagli, fornendo contemporaneamente un riscontro video in diretta all'operatore, prima di schiantarsi con la loro carica esplosiva.

Una lista degli UAV/UCAV utilizzati nel conflitto armato in Ucraina non può essere esaustiva ed è soggetta ad essere provvisoria dato che, nel momento in cui si scrive, i combattimenti sono ancora in corso e le informazioni

sull'utilizzo dei droni in azioni di combattimento non sono sempre accessibili. Entrambe le parti ne possiedono sicuramente un ingente numero di varianti.

Il conflitto in Donbass, in corso dal 2014, aveva già visto un ampio impiego di UAV da parte di entrambe le parti. I ribelli filorusi delle Repubbliche Popolari di Donesk e di Lugansk avevano operato per lo più con piccoli droni commerciali utilizzati per scopi di sorveglianza e ricognizione. Nondimeno, attraverso l'aggancio di materiale esplosivo e in qualità di droni kamikaze, sono anche stati utilizzati per attaccare truppe ucraine, infrastrutture o depositi di munizioni. Con il tempo, poi, le forze filorusse avevano ricevuto UAV più sofisticati da Mosca, come lo Zastava.

Dopo l'invasione della Crimea, il governo ucraino, che possedeva solo droni da ricognizione ad alta altitudine Tu-141 e Tu-143 dell'epoca sovietica, ha investito ingenti risorse allo sviluppo autoctono di droni, soprattutto tramite iniziative di crowd-sourcing aumentate dopo l'invasione. Sono così stati sviluppati il PD-1, il PD-2, l'A1-CM Fury e il Leleka-100, l'UJ-22 e il AN-BK-1 Horlytsia per scopi di sorveglianza, ricognizione e acquisizione del bersaglio, mentre lo Yatagan-2 (Scimitar), l'UJ-31 Zlyva e il RAM sono stati predisposti per l'attacco essendo munizioni *loitering*.

Importanti sono anche gliUCAV ucraini, come i mini-UCAV Punisher, che compiono missioni in base a coordinate preimpostate e in coppia con lo UAV Spectre, e lo R-18. Parallelamente, Kiev ha acquistato dal 2018 decine di droni armati turchi Bayraktar TB-2, dispiegati in combattimento a partire dal 2020 (Gettinger, 2020, pp. 76-77). Il Bayraktar TB-2 si è dimostrato straordinariamente letale in Libia, al servizio delle truppe del Governo di Accordo Nazionale (GNA), e nel conflitto del 2020 in Nagorno-Karabakh dalla parte azera. Inoltre, la sua relativa economicità, soprattutto rispetto ai costosi droni di fabbricazione statunitensi, lo hanno reso appetibile per molte potenze di medio rango.

Inoltre, dopo l'invasione, l'Ucraina ha ricevuto un cruciale aiuto militare dagli Stati Uniti e dai paesi NATO. I pacchetti di aiuti militari varati dall'Amministrazione Biden comprendono svariate centinaia di droni. Gli Stati Uniti hanno fornito a Kiev gli UAV Golden Eagle e Skydio X2 insieme a centinaia di droni *loitering* Switchblade-300, Switchblade-600 e Phoenix Ghost, versione modificata dello Switchblade a colpo singolo e basato su un riscontro continuo dal campo di operazioni. Washington ha anche inviato gli RQ-20 Puma, piccoli UAV a batteria molto efficienti nella ricognizione, sorveglianza e raccolta informazioni. La Polonia ha invece procurato alle forze ucraine la *loitering* munition WB Electronics Warmate, usata in coppia con l'UAV Warmate FlyEye, mentre la Lituania ha inviato i moderni droni da ricognizione estoni EOS C-VTOL "Magyla". Inoltre, molti produttori di droni occidentali hanno donato decine di droni di piccole dimensioni per scopi umanitari.

Insieme ai droni cinesi DJI Mavic-3 e EVO II e ai droni turchi Bayraktar MINI IHA, una versione non armata e più piccola del TB-2, l'Ucraina ha beneficiato notevolmente, per operazioni ISR, di droni commerciali, economici, disponibili su piattaforme internet e facilmente acquistabili. Non sono mancati, inoltre, casi di droni prodotti da stampanti 3D e operati da civili per individuare forze russe o lanciare molotov. Questa innovativa combinazione di economici droni commerciali e sofisticati droni tecnologici consente di localizzare e colpire truppe o materiale nemico dal valore di migliaia e milioni di dollari, con droni e prodotti esplosivi che ne costano poche centinaia.

Dal canto loro le forze armate russe operano in Ucraina diversi tipi di droni. Per quanto riguarda UAV per missioni di ISR, vengono impiegati gli stessi droni cinesi DJI Mavic-3 e Evo II, l'Eleron-3SV, l'Orlan-10, l'Orlan-30, lo Zala 421-16E5, il mini-UAV Takhion e il Granat-2, usato anche in operazioni di guerra elettronica. In azioni di attacco, invece, sono stati operati gli UCAV Kronshtadt Orion e il Forpost-R11, modello più sofisticato a disposizione dell'esercito russo, equipaggiato con testate termobariche e missili anticarro, così come le munizioni *loitering* ZALA Kub-BLA.

Nei primi mesi di guerra, le forze militari russe hanno mostrato una certa cautela nell'utilizzare i propri droni armati. Una possibile spiegazione può consistere nel volerli mantenere come riserva per un utilizzo più massiccio in caso di allargamento del conflitto. Un'ulteriore spiegazione punta il dito contro l'inefficiente catena logistica russa che ha avuto ingenti problemi a far arrivare mezzi qualitativamente all'avanguardia in Ucraina. Inoltre, è possibile che i comandanti militari russi non ripongano grande fiducia nelle armi più tecnologiche. Le esperienze militari russe in Siria, Libia e Donbass ci mostrano come i droni vengano utilizzati più come "occhi e orecchie" per raccolta informazioni e ricognizione dei bersagli (Bendett, 2022).

Sicuramente, le sanzioni internazionali imposte alla Russia dopo l'invasione della Crimea nel 2014 hanno danneggiato l'approvvigionamento di tecnologie all'avanguardia nello sviluppo di droni, soprattutto per quanto riguarda semiconduttori e microprocessori, cruciali nei settori dell'ottica e dell'elettronica. L'incapacità di approvvigionarsi di tali materiali fondamentali, insieme a una base industriale russa stagnante in molti aspetti strategici, in un momento storico in cui l'evoluzione e lo sviluppo nel campo dei droni militari è stato ingente, ha comportato un sostanziale freno alla modernizzazione dell'Intelligenza Artificiale e dei droni militari russi (Jie e Sohn, 2022).

Infatti i droni russi utilizzati sul campo hanno subito gravi ed inaspettate perdite. Le armi NATO fornite all'Ucraina si sono invece dimostrate qualitativamente superiori a quelle russe in quanto più difficili da abbattere e particolarmente efficaci contro i velivoli russi (Clark e Patt, 2022).

Questa relativa arretratezza è riscontrabile anche negli scarsi strumenti

anti-drone che Mosca ha inizialmente utilizzato in Ucraina e che, in una certa misura, ha permesso ai droni ucraini di registrare un alto livello di letalità. Grazie all'aiuto militare NATO, al momento Kiev detiene un relativo vantaggio qualitativo nella tecnologia anti-drone. Tale tecnologia si è sviluppata di pari passo a quella dei droni: man mano che gli UAV/UCAV diventavano più sofisticati, anche la tecnologia anti-drone, basata soprattutto su interferenze elettromagnetiche, si è aggiornata. Mentre l'industria militare russa è stata frenata da embarghi internazionali e da difficoltà economiche interne, i Paesi NATO, che oggi riforniscono l'Ucraina di strumenti anti-drone di ultima generazione, hanno mantenuto il passo, spesso includendole nelle capacità del drone stesso.

Efficace è stato l'uso operativo da parte delle forze armate ucraine del MANPAD Starstreak britannico, del localizzatore danese di droni Wolfpack 210 e del Skywiper EDM4S (Electronic Drone Mitigation System) di produzione lituana. Quest'ultimo emette impulsi elettro-magnetici che interrompono le comunicazioni drone-operatore in UAV di piccola e media grandezza. Con il tempo le forze russe hanno saputo reagire dislocando sul campo i loro strumenti di guerra elettronica, soprattutto tramite il sistema di interruzione segnale Krasukha-4. Tuttavia, Mosca preferisce affidarsi ancora a sistemi missilistici terra-aria come il Pantsir-S1.

Inoltre, un'ulteriore chiave dell'iniziale successo ucraino risiede nell'aver ottimizzato la cooperazione tra drone e operatore. In questa prospettiva rientrano l'ampio ed efficace uso fatto dalle forze ucraine delle munizioni *loitering*: il drone ricerca automaticamente bersagli da colpire riducendo la quantità delle comunicazioni con l'operatore e il rischio che tali contatti siano rilevati e attaccati. Al contrario, le forze russe tendono a vedere gli UAV quali meri strumenti in mano ad un operatore e facenti parte di sistemi militari più ampi e complessi che richiedono una costante ed efficace comunicazione drone-operatore anche a lunga distanza. Ciò inevitabilmente espone i droni di Mosca ad azioni di disturbo ucraine.

#### 4.6. Osservazioni conclusive

L'umanità è di fronte a una serie di quesiti fondamentali: dovremmo consentire a macchine autonome di prendere decisioni sulla vita e sulla morte degli individui? Ciò è legale? È eticamente giusto? I LAWS, pur essendo già patrimonio di molti arsenali militari, non sono ancora militarmente operativi; tuttavia, questa tecnologia in un futuro non troppo lontano renderà lo scontro sui campi di battaglia inesorabilmente più rapido e letale. Nonostante una certa reticenza negli ambienti militari ad affidare alle armi autonome letali

anche compiti offensivi, nei prossimi anni assisteremo presumibilmente allo sviluppo di prassi operative e strategiche basate sulle caratteristiche uniche dei LAWS (Wyatt, 2021, p. 46).

Diverse grandi potenze hanno già iniziato a investire su numerosi progetti, coinvolgendo diversi ambiti tecnologici, non solo nel settore pubblico ma anche in quello privato e accademico. Mentre Paesi come gli Stati Uniti e alcuni membri dell'Unione Europea mostrano una maggiore trasparenza nella R&S in materia di difesa, altri, come la Russia e la Cina, ancora oggi mantengono il più assoluto riserbo sulla maggior parte dei loro progetti.

Oltre a ciò, quello che risulta evidente è che nessuno di questi attori rinuncerà alla corsa agli armamenti in un settore percepito come cruciale per i futuri equilibri politici e strategici.

Modelli come il UCAV X-47B, il CIWS Pantsir-M e lo ASW (Anti-Submarine Warfare) Sea Hunter, evidenziano non solo gli sforzi economici da parte delle grandi potenze, ma mostrano anche l'elevato livello di sviluppo qualitativo raggiunto dalle nuove tecnologie belliche.

Tuttavia, tra tutti i sistemi presentati, lo *swarm* rappresenta senza dubbio la vera frontiera dei sistemi d'arma autonomi. La possibilità di utilizzare singoli sistemi che interagiscono ed operano come un gruppo rappresenta un evidente vantaggio tattico ed un moltiplicatore offensivo/difensivo considerevole per chi per primo riuscirà a realizzarlo.

## Riferimenti bibliografici

- Amoroso D., Sauer F., Sharkey N., Suchman L., Tamburini G. (2018), *Autonomy in Weapon Systems the Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy*, Heinrich Böll Foundation, Heinrich Böll Stiftung, Publication Series on Democracy, vol. 49.
- Bendett S. (2022), "Where Are Russia's Drones?", *DefenseOne*, 1 Marzo 2022, testo disponibile al sito: <https://www.defenseone.com/ideas/2022/03/where-are-russias-drones/362612/>
- Boulanin V., Verbruggen M. (2017), "Mapping the development of autonomy in weapon systems", *Stockholm International Peace Research Institute*, Report, November 2017.
- Boulanin V. *et al.* (2019), "The Impact of Artificial Intelligence on strategic stability and nuclear risk, Euro-Atlantic Perspectives", *Stockholm International Peace Research Institute*.
- Chakraborty N., Kolling A., Lewis M., Sycara K., Walker P., (2016), "Human interaction with robot swarms: a survey", *IEEE*, vol. 46, n. 1: 1-19.
- Clark B., Patt D. (2022), "Ukraine Embraces the 'Messy Middle' to Win the Drone War", *The National Interest*, 13 Maggio 2022, testo disponibile al sito:

- <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/ukraine-embraces-%E2%80%98messy-middle%E2%80%99-win>.
- Gallo B. (2019), “I Killer Robots e l’arte della guerra. Le implicazioni della robotica sui campi di battaglia”, *IRIAD Review*, n. 10, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Gettinger D. (2020), *The Drone Databook*, The Center for the Study of the Drone at Bard College.
- Human Rights Watch (2012), “Losing of Humanity, the case against Killer Robots”, *Human Rights Watch*, testo disponibile al sito: [www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots](http://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots).
- Jie Y., Sohn J. (2022), “Chip Sanctions Challenge Russia’s Tech Ambitions” *The Wall Street Journal*, 19 marzo 2022, testo disponibile al sito: <https://www.wsj.com/articles/chip-sanctions-challenge-russias-tech-ambitions-11647682202>.
- Kania E. (2020), “AI weapons in Chinese Military Innovation”, Brookings, testo disponibile al sito: [www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/](http://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/).
- Kelly A., Matthies L., Litwin T., Sharp G. (1996), “Obstacle Detection for Unmanned Ground Vehicles: A Progress Report”, in Giralt G., Hirzinger G., eds., *Robotics Research*, Springer, Londra.
- Lele A. (2019), *Disruptive Technologies for the Militaries and Security*, Springer, Singapore.
- Malinconci M. (2021), *I droni che uccidono. La tutela dei diritti umani e l’atto politico di Stato nelle operazioni con droni amati*, Multimage, Firenze.
- Parisi G. (2021), *In un volo di stormi. Le meraviglie dei sistemi complessi*, Rizzoli, Milano.
- PAX (2017), “Where to draw the line, Increasing Autonomy in Weapon Systems – Technology and Trends”, novembre 2017.
- PAX (2019a), “State of the AI. Artificial Intelligence the military and increasingly autonomous weapons”, aprile 2019.
- PAX (2019b), “Don’t be Evil, A survey of the tech sector’s stance on lethal autonomous weapons”, agosto 2019.
- PAX (2019c), “Slippery Slope, The arms industry and increasingly autonomous weapons”, novembre 2019.
- Petrella S., Miller C., Cooper B. (2021), “Russia’s Artificial Intelligence Strategy: The Role of State-Owned Firms”, *Orbis*, vol. 65, n. 1: 75-100.
- Petroni F. (2015), “Compensa e domina: Il Pentagono e la Terza Offset Strategy”, *Limes*, Gennaio 2015: 141-147.
- Rossi J.C. (2019), “Intelligenza Artificiale e robotica alla guerra”, *IRIAD Review*, n. 5, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Rossi J.C. (2016), “La guerra che verrà”, *Sistema informativo a Schede*, n. 11, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Saalman L. (2019), *The Impact of Artificial Intelligence on strategic stability and nuclear risk*, Volume II, East Asian Perspectives. Stockholm International Peace Research Institute.
- Scharre P., Horowitz M. (2015), “An Introduction to Autonomy in Weapon Systems”, *Center for a New American Security*.



- Sharre P. (2019), *Army of None: Autonomous Weapons and the Future of War*, W.W. Norton & Company, New York.
- Shashank R. (2016), *India and the Challenge of Autonomous Weapons*, Carnegie India, New Delhi.
- Simoncelli M., et al. (2020), “La questione delle armi letali autonome e le possibili azioni italiane ed europee per un accordo internazionale”, *IRIAD Review*, n. 7-8, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- United Kingdom Defence Journal – UKDJ (2019), *The rise of the drone swarm*, 15 febbraio 2019, testo disponibile al sito: <https://ukdefencejournal.org.uk/the-rise-of-the-drone-swarm/>.
- United Nations Institute for Disarmament Research – UNIDIR (2015), *The Weaponization of Increasing Autonomous Technologies in the Maritime Environment: Testing the Waters*, n. 4.
- Verbruggen M. (2019), “The Question of Swarms Control: Challenges to Ensuring Human Control over Military Swarms”, *Stockholm International Peace Research Institute*, Non-Proliferation and Disarmament Paper, n. 65, december 2019.
- Wyatt A. (2021), *The Disruptive Impact of Lethal Autonomous Weapons Systems Diffusion*, Routledge, London.

## 5. Il dibattito etico sulle armi autonome

di *Guglielmo Tamburrini*

### 5.1. Le fonti normative del dibattito etico sulle armi autonome

Il dibattito etico intorno alla realizzazione, al dispiegamento e all'utilizzazione delle armi autonome si è sviluppato principalmente nella cornice offerta da due delle principali impostazioni teoriche all'interno dell'etica normativa, e cioè dall'*etica dei doveri* (detta anche etica deontologica) e dall'*etica delle conseguenze* (detta anche etica consequenzialista) (Tamburrini, 2016; Tamburrini, 2020, cap. 4).

L'*etica dei doveri* si interroga su quali siano gli obblighi morali ai quali attenersi per giudicare il valore morale di azioni già compiute oppure per guidare scelte e azioni ancora da compiere. Dalla prospettiva dell'etica dei doveri, la questione principale che riguarda le armi autonome è la seguente: «l'autonomia dei sistemi d'arma impedisce di rispettare gli obblighi morali che vincolano il comportamento dei vari attori coinvolti in un conflitto bellico?».

L'*etica delle conseguenze* si focalizza invece sui criteri per distinguere tra conseguenze moralmente buone e conseguenze moralmente cattive delle azioni, prescrivendo di giudicare la bontà delle azioni solo in base a un bilancio di tali conseguenze. La linea di condotta moralmente preferibile deve essere individuata partendo da giudizi di questo genere. Dalla prospettiva dell'etica delle conseguenze, la questione principale che riguarda le armi autonome è la seguente: «in base a una valutazione delle conseguenze attese, è moralmente preferibile impiegare armi autonome in guerra oppure astenersi dal loro impiego?».

Questo capitolo fornisce una sintesi dei principali tentativi di fornire delle risposte a entrambi gli interrogativi, esplorandone le implicazioni per quanto riguarda l'ammissibilità morale delle armi autonome, una regolamentazione del loro uso o perfino la loro messa al bando.

Il dibattito etico sulle armi autonome prende le mosse dall'identificazione delle principali proprietà *funzionali* delle armi autonome. Secondo il Dipartimento della Difesa degli Stati Uniti, perché un sistema d'arma sia da considerarsi autonomo, esso deve essere capace di selezionare e attaccare un obiettivo senza richiedere ulteriori interventi da parte di operatori umani dopo la sua attivazione (DoD, 2012, pp. 13-14). Un'idea simile è stata espressa dal Comitato Internazionale della Croce Rossa (CICR). Secondo il CICR un'arma è autonoma solo se è in grado di selezionare e attaccare degli obiettivi «in modo indipendente» (CICR 2016, p. 1). Analogamente, la ONG *Human Rights Watch* descrive le armi autonome come armi che potrebbero selezionare e attaccare degli obiettivi senza richiedere alcun intervento umano (HRW 2012, p. 1). Per poter svolgere tali funzioni, è necessario che il sistema d'arma percepisca in qualche misura l'ambiente circostante, selezioni dei potenziali obiettivi tra gli oggetti presenti nella scena, ragioni sulle scelte operative che può compiere, pianifichi e infine esegua le manovre di attacco. È pertanto evidente che la IA e la robotica costituiscono una fonte primaria di conoscenze scientifiche e di tecnologie per lo sviluppo delle armi autonome. Come vedremo, la riflessione sulle attuali potenzialità e limitazioni delle tecnologie robotiche e della IA (già richiamate su un piano più generale nei capitoli 2 e 3) gioca un ruolo importante nel dibattito etico sulle armi autonome.

## **5.2. La guerra giusta e i principi di distinzione e proporzionalità**

Sono emerse nel quadro dell'*etica dei doveri* le principali obiezioni morali al dispiegamento e all'utilizzazione di armi capaci di selezionare e attaccare un obiettivo senza richiedere ulteriori interventi da parte di operatori umani dopo la loro attivazione. In base a una tale impostazione, ben consolidata nel quadro dell'etica normativa, è stato sostenuto che le armi autonome ostacolano o impediscono del tutto il rispetto di obblighi morali che incombono su tutti gli attori di un conflitto armato tra stati.

Gli obblighi morali in questione riguardano:

1. il rispetto dei principi della guerra giusta, che offrono un fondamento etico per le norme del Diritto Internazionale Umanitario (DIU);
2. il mantenimento della catena delle responsabilità nelle azioni belliche;
3. il rispetto della dignità degli esseri umani coinvolti nelle azioni belliche.

Procediamo a discutere nell'ordine questi punti, prendendo anzitutto in considerazione le ragioni offerte per sostenere che l'impiego delle armi autonome minaccia il rispetto dei principi della guerra giusta (Walzer, 2009) e delle norme del DIU. La teoria della guerra giusta ammette che in determi-

nate situazioni il ricorso alle armi sia moralmente giustificato. Nondimeno, essa prescrive che tutte le parti coinvolte in un conflitto debbano ottemperare ad alcuni vincoli morali nella conduzione delle operazioni belliche. In particolare, bisogna rispettare l'immunità dei non combattenti e bisogna astenersi dall'infliggere danni sproporzionati in relazione agli obiettivi militari da conseguire (Walzer, 2009, tr. it. pp. 175-216). Queste richieste sono state incorporate, rispettivamente, nel principio di distinzione e nel principio di proporzionalità del DIU (entrambi i principi sono codificati nei protocolli aggiuntivi alle Convenzioni di Ginevra del 1949; [https://www.icrc.org/eng/assets/files/other/icrc\\_002\\_0321.pdf](https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf)).

Il principio di distinzione impone di limitare strettamente gli attacchi agli obiettivi militari che – per loro natura, ubicazione, scopo o uso – forniscono un contributo effettivo all'azione bellica e la cui distruzione, conquista o neutralizzazione offre un chiaro vantaggio militare nelle circostanze date (Protocollo I del 1977, art. 52). Per applicare correttamente il principio di distinzione è necessario discriminare tra i combattenti attivi e i nemici fuori combattimento, così come tra i combattenti e la popolazione civile inerme. È necessario altresì riconoscere e salvaguardare il personale militare sanitario e religioso, le unità sanitarie e i mezzi di trasporto civili o militari.

Consideriamo tra questi vari compiti, che le parti attivamente coinvolte in una guerra devono sistematicamente eseguire, il problema di riconoscere un nemico fuori combattimento. In base ai Protocolli aggiuntivi alle Convenzioni di Ginevra si ritiene fuori combattimento un nemico che si astiene da ogni tentativo di fuga e soddisfa almeno una delle seguenti condizioni: a) si trova nelle mani di una delle parti avverse; b) esprime chiaramente l'intenzione di arrendersi; c) è in uno stato di assenza di coscienza oppure è stato neutralizzato da ferite o malattie che lo rendono incapace di difendersi (Protocollo I, art. 41). Nello svolgimento delle funzioni critiche di selezione e ingaggio di un obiettivo, un'arma autonoma deve perciò identificare le persone descritte dalle condizioni sopra elencate e astenersi dal dirigere un attacco contro di esse.

Il problema di sviluppare sistemi che sappiano decidere in base a tali criteri non ammette, nella sua generalità, soluzioni a portata delle attuali tecnologie della IA e della robotica. È difficile anche specificare chiaramente sotto forma di istruzioni algoritmiche come eseguire un compito del genere. Come si possono specificare in modo chiaro ed esaustivo gli indizi percettivi che consentono di riconoscere tutti o anche solo la maggior parte di quei comportamenti che esprimono – in modi variegati e talora anche poco convenzionali – l'intenzione di arrendersi attraverso segnali, gesti del corpo o comunicazioni verbali? Come sviluppare un sistema artificiale capace di fare ciò senza incorrere in errori madornali basandosi solo su indizi percettivi e senza poter contare sulla

condivisione tacita tra esseri umani di contesti culturali e antropologici per la loro interpretazione?

A fronte di queste difficoltà di esplicitazione algoritmica del compito richiesto e di un suo adeguato svolgimento da parte di una macchina, è legittimo obiettare che anche gli esseri umani alle prese con lo stesso compito discriminativo non hanno prestazioni perfette e possono incorrere in errori. Ma l'obiezione non è particolarmente rilevante allo stato attuale delle conoscenze scientifiche e tecnologiche, poiché i confronti tra le prestazioni dei sistemi percettivi della IA e quelle di un soldato competente e ben addestrato (nonché equipaggiato con sistemi tecnologici di supporto alla percezione) hanno finora avuto un esito decisamente sfavorevole per i sistemi percettivi della IA (Tonin, 2019, p. 6). I problemi di discriminazione percettiva sollevati dal principio di distinzione non ammettono una soluzione tecnologica soddisfacente e generale in base alle attuali tecnologie della IA (e cioè in base a ciò che in inglese si indica come *educated guess*). Non sembra nemmeno a portata di mano una soluzione tecnologica nel breve periodo dello sviluppo tecnologico.

Le caratteristiche degli ambienti bellici e dei campi di battaglia sollevano ulteriori dubbi a proposito della capacità di un'arma autonoma di rispettare il principio di distinzione. Un campo di battaglia non è quel mondo ben ordinato, ripetitivo e privo di sorprese che caratterizza la catena di montaggio robotizzata, dal quale sono state eliminate tutte le possibili fonti di perturbazione dell'azione robotica. Si tratta piuttosto di un ambiente dinamico e poco strutturato, nel quale gli attori coinvolti sfidano intenzionalmente la capacità di previsione degli avversari, con iniziative e manovre a sorpresa, azioni di hackeraggio, *jamming* e *spoofing* e altri tentativi di perturbare il comportamento delle armi autonome. Questa caratteristica degli ambienti operativi delle armi autonome – tanto diversi dagli ambienti prevedibili e poco dinamici nei quali si esplica l'azione degli attuali robot industriali o di servizio dotati di qualche forma di autonomia operativa – introduce notevoli difficoltà per la progettazione di test empirici che siano veramente adeguati a valutare la capacità delle armi autonome di affrontare correttamente le situazioni impreviste che possono insorgere sul campo di battaglia (Cummings, 2021). Un comandante militare ben addestrato dovrà essere consapevole di questo problema e delle sue implicazioni operative per valutare il grado di fiducia che può riporre nella capacità di un'arma autonoma di rispettare le consegne nel corso di un'azione bellica.

I problemi di previsione del comportamento di un'arma autonoma che abbiamo finora ricordato nascono dalle caratteristiche e dall'evoluzione dinamica dell'ambiente esterno nel quale essa è collocata. Problemi previsionali altrettanto complicati nascono dalle interazioni tra le varie componenti interne all'arma autonoma e dalle modalità di funzionamento di ciascuna di esse. Consideriamo da questa prospettiva l'uso diffuso delle tecnologie per

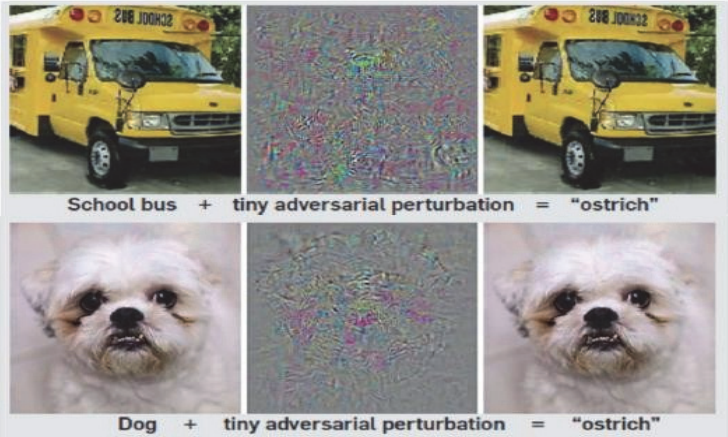
l'apprendimento automatico (*machine learning*) nello sviluppo dei moduli interni a un'arma autonoma che sovrintendano ai compiti di percezione artificiale e di decisione (vedi anche capitoli 2 e 3) per la selezione e l'ingaggio di un obiettivo. E torniamo a considerare più specificamente in questo ambito il problema di stabilire se un'arma autonoma ha *appreso* correttamente a distinguere obiettivi militari legittimi da persone e cose che non lo sono. Per illustrare il problema, esaminiamo due casi particolari, ben noti nella letteratura scientifica di settore.

Il primo di questi casi riguarda il riconoscimento visivo di un pulmino scolastico e della sua conseguente esclusione – in conformità con il principio di distinzione e in circostanze di uso normale del pulmino – dalla lista degli obiettivi da attaccare. Da un test eseguito su un sistema percettivo della IA, formato da una rete neurale profonda (in inglese *Deep neural network*), sono scaturiti risultati piuttosto allarmanti. Il sistema in questione è stato addestrato con metodi di apprendimento automatico a classificare delle immagini in ingresso come immagini di pulmino scolastico, di cane o di struzzo. Le reti neurali profonde per la classificazione visiva raggiungono spesso, nel loro funzionamento a regime, percentuali molto alte di classificazione corretta delle immagini in ingresso, con prestazioni anche superiori a quelle degli esseri umani. Tuttavia, esse possono ancora incorrere in errori rari, che appaiono stravaganti e madornali rispetto alle capacità di classificazione percettiva di un essere umano. Nei test eseguiti dopo la fase di apprendimento, l'immagine di un pulmino scolastico è stata inizialmente classificata in modo corretto dalla rete neurale profonda in questione. In seguito, sono state apportate piccole modifiche mirate alla stessa immagine, applicando una metodologia di test antagonista (*adversarial testing*) che ha lo scopo di mettere in luce una mancanza di robustezza del sistema a certe piccole modifiche percettive (Goodfellow *et al.*, 2018). Tali modifiche sono così piccole da risultare impercettibili al sistema visivo umano integro, il quale continuerà a classificare correttamente la nuova immagine come quella di un pulmino scolastico. La rete neurale classifica invece come uno struzzo l'oggetto presente nella nuova immagine (v. fig. 1, riga in alto). Evidentemente, ai fini di una corretta applicazione del principio di distinzione, un pulmino scolastico ha una rilevanza ben maggiore, anzi incomparabile, rispetto a quella di uno struzzo o di un altro animale simile. Risultati altrettanto sorprendenti, se valutati considerando la robustezza del sistema visivo umano alle medesime piccole perturbazioni, sono stati ottenuti su immagini di cani: modifiche impercettibili per l'occhio umano hanno nuovamente indotto il sistema a cambiare la classificazione iniziale corretta in quella di struzzo (fig. 1, riga in basso).

Nella colonna di sinistra della figura 1 le immagini sono classificate correttamente dal sistema; al centro la perturbazione introdotta (e ingrandita 10x per renderla visibile a occhio nudo) per passare dalle immagini della colonna

di sinistra a quelle della colonna di destra; e infine, nella colonna di destra, le immagini così ottenute, che il sistema ha classificato come “struzzo”.

Fig. 1 – Esempi di adversarial testing



Fonte: Szegedi et al., 2013

Il secondo esempio di *adversarial testing* (v. fig. 2), riguarda le piccole modifiche costruttive, del tutto ininfluenti per il sistema visivo umano, che hanno indotto un sistema percettivo della IA a classificare come fucile automatico la riproduzione di una tartaruga ottenuta utilizzando una stampante 3D. I modelli nei riquadri in rosso sono stati classificati come “fucile”; quelli nei riquadri in nero come “altro” rispetto alle classi “tartaruga” e “fucile”. Il sistema aveva ottenuto una percentuale vicina al 100% di classificazioni corrette su modelli di tartaruga non modificati con tecniche di *adversarial testing*.

Fig. 2 – Adversarial testing su modelli 3D di tartaruga



Fonte: Athalye et al., 2018

Evidentemente, il sistema percettivo umano non è sensibile alle perturbazioni che hanno indotto le diverse classificazioni indicate nella figura 2, ma queste possibilità di perturbazione del comportamento del sistema artificiale, che non riescono a ingannare il sistema visivo umano, sollevano interrogativi importanti a proposito del rispetto del principio di distinzione da parte di un'arma autonoma (Amoroso, Garcia, Tamburrini 2022). Ronald Arkin, un docente di robotica che ha effettuato ricerche militari in ambito robotico, ha dichiarato senza mezzi termini che il dispiegamento e l'uso di armi autonome capaci di rispettare il principio di distinzione non è una meta tecnologicamente raggiungibile nel breve periodo: «Vi sono profonde sfide tecnologiche ancora da risolvere, che riguardano tra l'altro la discriminazione efficace *in situ* degli obiettivi e il riconoscimento di chi è fuori combattimento» (Arkin, 2013 e 2015). In base a questa valutazione, Arkin ha proposto di introdurre una moratoria internazionale sulle armi autonome – cioè una sospensione temporanea di qualsiasi attività finalizzata allo sviluppo, al dispiegamento e all'uso di armi autonome. Per Arkin, la moratoria dovrebbe rimanere in vigore fin quando non siano state raccolte prove sperimentali sufficienti per affermare, con un grado di fiducia sufficientemente elevato, che un'arma autonoma è in grado di rispettare il DIU almeno altrettanto bene di soldati competenti e ben addestrati.

Passiamo ora a considerare, in relazione all'autonomia dei sistemi d'arma, il principio di proporzionalità. Questo principio impone di non sferrare un attacco che abbia un costo atteso eccessivo – in termini di morti e feriti tra i civili o di danni a installazioni civili – rispetto al vantaggio militare concreto e diretto che ne potrebbe derivare (Protocollo I del 1977, art. 51.5.b). Il principio di proporzionalità richiede di bilanciare i vantaggi militari con i costi che il loro raggiungimento potrebbe comportare per la popolazione civile. Ma un bilancio preventivo di questo tipo può comportare l'uso di capacità cognitive ed emotive, di competenze sociali ed esperienziali che non sono alla portata di un sistema della IA e della robotica. Un giudizio di proporzionalità da parte di un comandante richiede, tra l'altro, una valutazione degli effetti sul morale dei propri sottoposti o sul comportamento del nemico derivanti da un attacco che comporta il sacrificio di un gruppo di civili. Ma questo tipo di valutazione non è alla portata di un sistema della IA (Amoroso e Tamburrini, 2017; Amoroso, 2021, pp. 76-96). Allo stato di sviluppo tecnologico attuale, si può prefigurare l'utilizzazione di un sistema della IA solo come strumento di supporto per valutazioni di proporzionalità che devono rimanere in capo ai comandanti militari.

In definitiva, di fronte agli obblighi posti congiuntamente dai principi di discriminazione e di proporzionalità, è difficile contestare la conclusione sintetizzata dal docente di robotica Noel Sharkey: «i robot autonomi o i



sistemi della IA non hanno – né ora né in un futuro prevedibile – le proprietà che consentono di discriminare tra combattenti e civili o di prendere decisioni sulla proporzionalità degli attacchi» (Sharkey, 2010, p. 378).

### **5.3. Responsabilità degli operatori militari e dignità delle vittime**

Le tecniche per lo sviluppo di test antagonistici menzionate nel paragrafo precedente rivelano errori percettivi commessi da un sistema della IA che potrebbero sfociare in un «disastro della IA»: una decisione errata con gravi conseguenze dal punto di vista morale o legale. Un'arma autonoma che prenda un pulmino scolastico per uno struzzo, o una tartaruga per un fucile automatico, potrebbe avere conseguenze materiali riconducibili a crimini di guerra se alla loro origine ci fossero le decisioni di esseri umani invece dell'autonomia operativa di una macchina.

Chi sarà ritenuto responsabile dell'attacco di un'arma autonoma di un pulmino scolastico utilizzato normalmente come sistema di trasporto civile e della morte delle persone che si trovano a bordo? Escludiamo da subito l'arma autonoma: non potendo essere considerata come agente morale, non le si possono addossare responsabilità di alcun tipo per il verificarsi dell'evento in questione. Bisogna restringere la ricerca degli eventuali responsabili alle persone che hanno giocato un qualche ruolo nelle decisioni che hanno portato all'attivazione dell'arma autonoma e sono sfociate nell'attacco al pulmino scolastico. La lista delle persone coinvolte è piuttosto lunga. Vi sono gli ingegneri informatici, robotici e di altri settori che hanno contribuito a sviluppare l'arma autonoma; i responsabili della ditta produttrice; il personale politico che ha dato l'impulso all'acquisizione dell'arma autonoma da parte delle Forze armate; i consulenti e i dipendenti del ministero della Difesa che hanno stilato e approvato il piano di acquisizione; i militari incaricati dell'approvvigionamento dei sistemi d'arma, quelli che hanno stilato i manuali d'uso, il comandante in capo all'operazione militare, il personale militare incaricato di supervisionare il funzionamento dell'arma autonoma dopo la sua attivazione (Wagner, 2016). Più lunga è la lista, più facilmente la ricerca dei responsabili porterà al cosiddetto «problema delle molte mani»: ogni attore coinvolto in questi passaggi potrebbe concorrere in qualche modo al verificarsi dell'evento, senza però avere un ruolo tanto rilevante da giustificare l'accusa di essere individualmente responsabile di un crimine di guerra (Amoroso e Tamburrini, 2017; Bhuta e Pantazopoulos, 2016). Come è già accaduto in incidenti dovuti al malfunzionamento dei sistemi informatici (Nissenbaum, 1996, p. 25), si arriva ad appurare che numerose persone hanno concorso a vario titolo al verificarsi dell'incidente, ma si arriva pure

a concludere che nessuna delle persone coinvolte ha dato un contributo individuale davvero significativo al verificarsi dell'incidente. L'impiego delle armi autonome può perciò generare un nuovo tipo di problema delle molte mani, con la conseguente difficoltà di attribuire responsabilità morali e penali nel caso di azioni compiute da un'arma autonoma che per i loro effetti materiali equivalgono a un crimine di guerra.

L'ultimo degli argomenti sviluppati contro le armi autonome nel quadro dell'etica dei doveri si basa sul rispetto della dignità umana (Amoroso *et al.*, 2018; Amoroso, 2021). Questo argomento fornisce una motivazione razionale per la ripugnanza istintiva che suscita l'idea di affidare a una macchina il potere di vita o di morte su un essere umano (UNIDIR, 2015, pp. 7-8). Il filosofo Peter Asaro ha sostenuto che dal rispetto della dignità umana discende il diritto di ogni essere umano a non essere privato arbitrariamente della vita. E affinché una decisione di vita o di morte soddisfi questo requisito, ha affermato Asaro, essa deve essere presa da un altro essere umano, da un *qualcuno* che possa provare empatia e avere compassione per chi è oggetto di una simile decisione. Un'arma autonoma è invece un *qualcosa*, una macchina che non ha la capacità di apprezzare il valore di una vita umana e di valutare adeguatamente il significato della sua perdita. Per questo motivo, affidare a una macchina la decisione di togliere la vita a un essere umano, ha concluso Asaro, costituisce una violazione della dignità umana (Asaro, 2012).

L'argomento proposto da Asaro è stato efficacemente riformulato da Christof Heyns (in un rapporto stilato nella sua qualità di Relatore speciale delle Nazioni Unite per le esecuzioni extragiudiziarie, sommarie o arbitrarie) passando dalla prospettiva di una macchina che prende una decisione di vita o di morte alla prospettiva della vittima designata che subisce una tale decisione. La vittima non ha la possibilità di fare appello all'umanità condivisa di qualcuno che si trovi dall'altra parte. Il valore intrinseco di un essere umano (ciò che gli conferisce dignità in quanto agente morale consapevole) sarebbe perciò negato a priori, se si affida il suo destino alla discrezionalità di una macchina (Heyns, 2016).

## 5.4. Armi autonome ed etica delle conseguenze

Agli argomenti basati sull'etica dei doveri che abbiamo finora passato in rassegna, sono state affiancate nel dibattito etico sull'autonomia dei sistemi d'arma delle valutazioni morali che si basano invece sull'etica delle conseguenze. Da questa prospettiva teorica, nell'ambito dell'etica normativa sono stati sviluppati argomenti sia a favore sia contro lo sviluppo e il dispiega-

mento delle armi autonome. Cominciamo dagli argomenti di stampo consequenzialista a favore delle armi autonome. Tali argomenti fanno leva su considerazioni di tre tipi. È opportuno sottolineare subito che tali considerazioni presuppongono sviluppi notevoli delle tecnologie robotiche e della IA nel lungo periodo che vanno ben al di là dello stato dell'arte scientifico e tecnologico.

Si ipotizza innanzitutto che le armi autonome potranno garantire maggiore precisione nell'attacco agli obiettivi militari in alcuni scenari bellici futuri, allorché esse avranno superato test severi, volti a dimostrare il possesso di capacità di giudizio e di classificazione percettiva da parte della macchina che siano uguali o superiori a quelle di soldati competenti e ben addestrati.

Si sottolinea inoltre che, una volta superati i test relativi al rispetto dei principi di distinzione e proporzionalità, le armi autonome non saranno soggette a invalidanti perturbazioni emotive, al contrario di quanto può accadere a un comune soldato. Per questo motivo, esse potranno vantaggiosamente rimpiazzare i comuni soldati, poiché consentiranno di ridurre le vittime negli eserciti che le dispiegano e di evitare quelle violazioni del DIU dovute allo stress e alle dure prove emotive alle quali sono sottoposti i soldati sul campo di battaglia.

Si afferma infine che le armi autonome potranno essere programmate per rispettare regole d'ingaggio più restrittive di quelle pensate per un comune soldato, poiché la protezione della vita di un soldato ha un valore morale incomparabilmente più alto di quello attribuito alla protezione della ferraglia di un'arma autonoma. In definitiva, un'arma autonoma potrà essere programmata per lanciare i suoi attacchi solo in circostanze che non lasciano dubbi sulle intenzioni ostili del nemico e contro obiettivi ammessi dalla teoria della guerra giusta e dalle norme del DIU.

Il peso morale di tali considerazioni non può essere sottovalutato, poiché si prefigurano situazioni di riduzione delle vittime sul campo di battaglia, non solo nei ranghi del proprio esercito, ma anche tra i nemici e gli astanti innocenti. Bisogna tuttavia ribadire che tali considerazioni riguardano solo un futuro indeterminato, che si realizzerà se e quando lo sviluppo tecnologico consentirà di realizzare armi autonome in grado di esercitare capacità di giudizio e di classificazione percettiva uguali o superiori a quelle di soldati competenti e ben addestrati. È ancora più importante rilevare, dalla stessa prospettiva consequenzialista, che l'orizzonte delle conseguenze attese esaminate è ristretto in sostanza ai singoli campi di battaglia. Perché limitarsi a considerare tra le conseguenze attese l'eventuale riduzione delle vittime su ogni singolo campo di battaglia? E perché concentrarsi selettivamente su ciò che una singola arma autonoma può fare in termini di precisione o di conte-

nimento del volume di fuoco e dei suoi effetti? L'etica delle conseguenze non impone di restringere in questo modo la valutazione morale delle conseguenze attese, ignorando le interazioni di ciascuna arma autonoma con altri agenti umani o artificiali e le implicazioni strategiche derivanti dal loro dispiegamento. Uno sguardo più ampio sulle conseguenze attese terrà conto delle perturbazioni sul funzionamento corretto delle armi autonome, che possono essere indotte da interazioni con altri agenti umani o artificiali, degli incentivi che le armi autonome potrebbero offrire per iniziare nuovi conflitti, di come le armi autonome potrebbero influire sul mantenimento della stabilità e della pace tra le nazioni, di una nuova corsa alle armi autonome e dei processi di destabilizzazione che esse potrebbero innescare su scala regionale o globale.

Noel Sharkey (2010) ha sollecitato un tale allargamento della valutazione delle conseguenze attese dal dispiegamento delle armi autonome, valicando i confini dei singoli campi di battaglia e di impieghi puntuali di una singola arma autonoma: un'eventuale riduzione di perdite nel proprio esercito può indebolire l'opposizione dell'opinione pubblica al coinvolgimento del proprio paese in un conflitto, incentivando così i decisori politici a iniziare una guerra; la riduzione attesa di vittime sui singoli campi di battaglia potrebbe essere controbilanciata dal numero più alto di vittime, proprie o altrui, che i nuovi conflitti facilitati dalle armi autonome possono indurre nel lungo periodo. L'aspettativa stessa di una riduzione delle perdite sul singolo campo di battaglia potrebbe essere vanificata da episodi di "fuoco amico" provocati dall'hackeraggio di un'arma autonoma, da cyberattacchi che investono l'infrastruttura informatica necessaria (vedi cap. 3), da malfunzionamenti e da interazioni imprevedute con altri sistemi d'arma. Infine, le armi autonome portano con sé la minaccia di un ritmo accelerato dei conflitti, che potrebbe diventare incompatibile con i tempi di reazione degli operatori umani e sfuggire alle loro capacità di controllo (Altmann e Sauer, 2017).

Le interazioni imprevedute tra sistemi della IA hanno generato già situazioni critiche in altri settori, a partire dal "flash crash" del mercato finanziario del 6 maggio 2010, allorché l'indice Dow Jones della borsa valori di New York registrò un ribasso del 9% nel giro di pochi minuti. Algoritmi dello stesso tipo sono stati additati come le cause più probabili del ribasso sostanzioso e repentino del valore della sterlina inglese avvenuto nell'ottobre 2016. Possibilità analoghe di interazioni competitive incontrollate si estendono anche ai sistemi d'arma autonomi basati sulla robotica e la IA, come ha evidenziato lo stesso Sharkey (2020) in un recente articolo per la rivista *Scientific American*, sfruttando un parallelo con gli esiti di interazioni competitive osservati nel caso di algoritmi progettati per modificare il prezzo delle merci in funzione della domanda. Nell'aprile 2011, due piattaforme per la vendita di

libri online, bordeebook e profnath, entrarono in una competizione al rialzo per la vendita del libro esaurito *The making of a fly*, pubblicato nel 1992. Abitualmente il libro era reperibile al prezzo di 50 dollari più le spese di spedizione. Ma accadde qualcosa di molto strano. Ad un primo incremento di prezzo sul listino di bordeebook, profnath rispose con un ulteriore incremento di prezzo, provocando a sua volta un altro aumento di prezzo da parte di bordeebook, e così via. Nel giro di una settimana, senza che nessuno se ne accorgesse, bordeebook arrivò a mettere il libro in vendita per una cifra di oltre 23 milioni di dollari (più le spese di spedizione per 3,99 dollari). E così l'interazione di due algoritmi semplici e generalmente prevedibili sfuggì completamente al controllo. Per analogia, Sharkey si chiede «che cosa potrebbe accadere se gli algoritmi complessi che governano il combattimento di due sciami di armi autonome interagissero a velocità sostenuta. In aggiunta alle incertezze causate dall'uso di immagini antagoniste, del jamming, spoofing, diversivi e cyberattacchi, bisogna affrontare l'impossibilità di prevedere il risultato allorché gli algoritmi si danno battaglia. Si deve capire che queste armi alterano molto pericolosamente la natura dei conflitti bellici. Dei conflitti accidentali potrebbero scoppiare tanto velocemente da sottrarre ai comandanti il tempo di comprendere o di reagire a quanto le loro armi stanno facendo, lasciando devastazione nella loro scia» (Sharkey, 2020, pp. 56-57).

Jürgen Altmann ha ampliato ancor più l'inventario di conseguenze attese dal dispiegamento delle armi autonome, passando dalla prospettiva dei singoli campi di battaglia, che potrebbe essere favorevole all'impiego di armi autonome, seppure in circostanze molto specifiche e ristrette, a una prospettiva che tenga conto degli equilibri geopolitici globali: «Il peso dei vantaggi militari ipotizzati nel breve periodo dovrebbe essere contrapposto alle conseguenze probabili di lungo periodo per la sicurezza nazionale e, in modo particolare, per quella internazionale» (Altmann, 2013, p. 137). Poiché i sistemi della robotica e della IA hanno costi di sviluppo e produzione relativamente bassi rispetto ad altre armi convenzionali, una corsa alle armi autonome potrebbe coinvolgere un numero consistente di stati e avere un forte impatto destabilizzante sugli attuali equilibri militari. Per lo stesso motivo, è ragionevole prevedere la loro acquisizione sul mercato illegale da parte di organizzazioni terroristiche.

Bisogna infine osservare che le armi autonome potrebbero avere un effetto destabilizzante anche sulle relazioni tra potenze nucleari. La nave *Sea Hunter* (vedi cap. 4), così come altri mezzi sottomarini autonomi in via di sviluppo, potrebbero essere utilizzati per identificare, tracciare ed eventualmente attaccare i sottomarini del nemico armati di missili balistici con testate nucleari. Poiché la possibilità di risposta a un attacco nucleare si basa

anche sui sottomarini armati di missili balistici con testate nucleari, le armi autonome potrebbero essere un fattore destabilizzante, contribuendo a erodere le fondamenta della deterrenza nucleare imperniata sull'idea di una distruzione reciproca assicurata (nota come deterrenza MAD, dall'acronimo inglese di *Mutually Assured Destruction*).

In conclusione, è opportuno sottolineare che l'etica delle conseguenze fornisce, al contrario dell'etica dei doveri, un panorama di argomenti e posizioni che non sono univocamente indirizzati contro le armi autonome. Il dispiegamento futuro delle armi autonome, infatti, è stato argomentato con una prospettiva consequenzialista indicando la possibilità di ridurre le vittime sui campi di battaglia a causa della maggiore precisione delle armi autonome e di regole di ingaggio più conservative. È tuttavia importante notare che tale possibilità dipende da progressi notevoli delle tecnologie robotiche e della IA, per il conseguimento dei quali, come ha sottolineato Ronald C. Arkin, sussistono «profonde sfide tecnologiche ancora da risolvere, che riguardano tra l'altro la discriminazione efficace *in situ* degli obiettivi e il riconoscimento di chi è fuori combattimento» (Arkin, 2013; 2015). Ed è ancora più importante notare che gli argomenti consequenzialisti a favore delle armi autonome assumono implicitamente che esse non avranno un impatto significativo al di là dei singoli campi di battaglia. Abbandonando questa ipotesi poco plausibile, un bilancio allargato dei costi e dei benefici attesi dovrà prendere in considerazione anche l'aspettativa di un ricorso più facile alle armi e di una conseguente moltiplicazione dei campi di battaglia, di hackeraggi malevoli, di nuovi incentivi a una nuova corsa agli armamenti, di rischi consistenti di destabilizzazione regionale e globale, e perfino di un indebolimento dei tradizionali meccanismi di deterrenza nucleare basati sulla MAD (Tamburrini, 2016).

In definitiva, un bilancio allargato delle conseguenze attese rafforza gli argomenti deontologici presentati nei paragrafi precedenti, che riguardano il rispetto dello *jus in bello*, e in particolare dei principi di distinzione e di proporzionalità, il mantenimento della catena di responsabilità morali e penali nel caso di una loro violazione e il rispetto della dignità umana delle potenziali vittime. Pertanto, lo sviluppo, la produzione e l'impiego delle armi autonome possono essere messi in discussione da prospettive multiple nel quadro dell'etica normativa, sia dalla prospettiva dell'etica dei doveri, sia dalla prospettiva dell'etica delle conseguenze, specialmente quando si prendono in considerazione conseguenze attese che travalicano i confini dei singoli campi di battaglia e delle singole armi autonome. Come vedremo nel cap. 9, gli argomenti di carattere etico qui riassunti hanno giocato un ruolo molto significativo nelle discussioni diplomatiche e politiche che si sono sviluppate in seno alla *Convention on Certain Conventional*

*Weapons* (CCW) presso la sede di Ginevra delle Nazioni Unite, sulla scia della proposta, avanzata da un nutrito gruppo di ONG, di una messa al bando delle armi autonome.

## Riferimenti bibliografici

- Altmann J. (2013), “Arms control for armed uninhabited vehicles: an ethical issue”. *Ethics and Information Technology*, 15: 137-152.
- Altmann J. and Sauer F. (2017), “Autonomous Weapon Systems and Strategic Stability”, *Survival. Global Politics and Strategy*, 59: 117-142.
- Amoroso, D. (2021), *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, Edizioni Scientifiche Italiane e Nomos Verlag, Napoli e Baden-Baden.
- Amoroso D., Garcia D., Tamburrini G. (2022), “The Weapon that Mistook a School Bus for an Ostrich”, *Science & Diplomacy*, <https://www.sciencediplomacy.org/article/2022/weapon-mistook-school-bus-for-ostrich>
- Amoroso D., Sauer F., Sharkey N., Suchman L., Tamburrini G. (2018), *Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany’s New Foreign and Security Policy*. Heinrich Böll Foundation, Berlino.
- Amoroso D. and Tamburrini G. (2017), “The Ethical and Legal Case Against Autonomy in Weapons Systems”, *Global Jurist*, 17, 3: 1-20.
- Arkin R.C. (2013), “Lethal autonomous systems and the plight of the non-combatant”, *AISB Quarterly*, 137: 1-9.
- Arkin R. C. (2015), “The case for banning autonomous weapons: counterpoint”, *Communications of the ACM*, 58(12): 48-49.
- Asaro P. (2012), “On banning autonomous weapon systems: human rights, automation, and the de-humanization of lethal decision-making”, *International Review of the Red Cross*, 94: 687-709.
- Athalye A., Engstrom L, Ilyas A., Kwok K. (2018), “Synthesizing robust adversarial examples”. *Proceedings of the 35th International Conference on Machine Learning*, PMLR 80: 284-93.
- Bhuta N., Beck S., Geiss R., Liu H.-Y., Kress C., eds. (2016), *Autonomous weapons systems: law, ethics, policy*, Cambridge University Press, Cambridge.
- Bhuta N. and Pantazopoulos S.E. (2016), “Autonomy and uncertainty: increasingly autonomous weapons systems and the international legal regulation of risk in Autonomous Weapons Systems”, in Bhuta N., Beck S., Geiss R., Liu H.-Y., Kress C., eds. (2016), *Autonomous weapons systems: law, ethics, policy*, Cambridge University Press, Cambridge: 284-300.
- CICR (2016), “Views of the International Committee of the Red Cross on autonomous weapon system”, paper submitted by the International Committee of the Red Cross (ICRC) to the Informal meeting of experts on lethal autonomous weapons systems of the Convention on Certain Conventional Weapons (CCW), Geneva, 11 April 2016.

- Cummings M. L. (2021), “Rethinking the Maturity of Artificial Intelligence in Safety-Critical Settings”, *AI Magazine*, 42, 1: 6-15.
- DoD (US Department of Defense) (2012), *Directive 3000.09, Autonomy in Weapons Systems* (21 November 2012).
- Goodfellow I., McDaniel P., Papernot N. (2018), “Making machine learning robust against adversarial testing”. *Communications of the ACM*, 61, 7: 56-66.
- Heyns C. (2016), “Autonomous weapons systems: living a dignified life and dying a dignified death”, in Bhuta N., Beck S., Geiss R., Liu H.-Y., Kress C., eds. (2016), *Autonomous weaponssystems: law, ethics, policy*, Cambridge University Press, Cambridge: 3-19.
- HRW (2012), Human Rights Watch, *Losing Humanity. The Case against Killer Robots*, Londra 19 November 2012.
- Nissenbaum H. (1996), “Accountability in a computerized society”, *Science and Engineering Ethics*, 2: 25-42.
- Sharkey N. (2010), “Saying ‘no!’ to lethal autonomous targeting”, *Journal of Military Ethics*, 9: 369-383.
- Sharkey N. (2020), “Autonomous Warfare”, *Scientific American*, February 2020: 52-57.
- Szegedi C., Zaremba W., Sutskever I., Bruna J., Erhan D., Goodfellow I., Fergus R. (2013), “Intriguing properties of Neural Networks”, arXiv:1312.6199, Cornell University, Ithaca, testo disponibile al sito: <https://arxiv.org/abs/1312.6199>.
- Tamburrini G. (2016), “On banning autonomous weapons systems: from deontological to wide consequentialist reasons”, in Bhuta N., Beck S., Geiss R., Liu H.-Y., Kress C., eds. (2016), *Autonomous weaponssystems: law, ethics, policy*, Cambridge University Press, Cambridge: 122-142.
- Tamburrini G. (2020), *Etica delle macchine. Dilemmi morali per la robotica e l'intelligenza artificiale*, Carocci, Roma.
- Tonin M. (2019), *Artificial Intelligence: implications for NATO's armed forces*. Report 5 april 2019, NATO Parliamentary Assembly, Science and Technology Committee, Bruxelles, testo disponibiela al sito: <https://www.nato-pa.int/document/2019-stctts-report-artificial-intelligence-tonin-088-stctts-19-e>.
- UNIDIR (2015), *The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values*. UNIDIR Resources n. 7, United Nations Institute for Disarmament Research, New York, testo disponibile al sito: <https://www.unidir.org/publication/weaponization-increasingly-autonomous-technologies-autonomous-weapon-systems-and-cyber>.
- Wagner M. (2016), “Autonomous Weapon Systems”, Wolfrum R., ed., *Max Planck Encyclopedia of Public International Law*, Oxford University Press, Oxford.
- Walzer M. (2009), *Guerre giuste e ingiuste. Un discorso morale con esemplificazioni storiche*, tr. it. Liguori Editore, Napoli.



## 6. *L'opinione pubblica e i droni*

di *Francesca Farruggia*

### 6.1. Opinione pubblica e uso della forza

Erano passati appena quattordici anni dalla vittoria dell'Occidente nella Guerra Fredda, quando si è affacciata sulla scena internazionale quella che il *New York Times* ha definito la nuova 'superpotenza' internazionale, ossia l'opinione pubblica. Ancora in età "moderna", cioè negli anni '50 e '60 del XX secolo, questa entità veniva descritta da politologi, sociologi ed esperti della comunicazione come volatile, disinformata e sostanzialmente indifferente di fronte ai grandi temi politici, specialmente a quelli di carattere internazionale, in quanto remoti rispetto alle conoscenze e agli interessi dell'«uomo della strada» (Isernia, 1996). Analisi successive si sono distaccate da questo iniziale scetticismo, mostrando come, indotti a misurarsi su temi complessi come l'uso della forza, i cittadini sono in grado di valutare in modo coerente e pertinente (Isernia e Everts, 2003 e 2004). Inoltre, nella società post-moderna, con il declinare delle ideologie, la propensione a cambiare idea viene valutata positivamente. Quella che ancora cinquant'anni fa era connotata negativamente come 'volatilità' oggi tende a essere letta come flessibilità e libertà di giudizio, cioè come capacità del pubblico di adattare il proprio pensiero alle diverse situazioni, senza più subordinarlo alle appartenenze culturali, politiche e religiose e all'ambiente di riferimento (Battistelli, Galantino, Lucianetti, Striuli, 2012).

Uno dei temi più sentiti a livello individuale e collettivo è, nelle società industriali avanzate, il diritto alla vita e di conseguenza diventano cruciali tutte quelle decisioni che possono metterlo a repentaglio come accade nel caso degli interventi militari.

Il sempre più agguerrito «scrutinio» (Burk, 1998) dell'opinione pubblica, infatti, coinvolge l'insieme degli attori incaricati della sicurezza interna ed esterna e ha per protagonisti tutti coloro che hanno a disposizione un pc o

uno smartphone, cioè poco meno della totalità dei cittadini elettori. L’“intrusione” di questi ultimi si configura come un dato politico che può essere anche manipolato dal potere ma che non può essere impedito, condizionando così potentemente la scelta dei governi.

Per uno scopo impopolare come l’uso della forza i governi devono garantire alle proprie decisioni la legittimazione, cioè una risorsa che necessita del consenso dell’opinione pubblica. Per ottenere il consenso, o perlomeno l’acquiescenza, dell’opinione pubblica è necessario limitare drasticamente gli effetti letali della guerra. Come si è visto nel capitolo 1 di questo libro, negli eserciti delle maggiori potenze la parola d’ordine vincente è quella delle «perdite zero». A partire dalla «rivoluzione degli affari militari», resa possibile, a cavallo tra il XX e il XXI secolo, dai progressi tecnologici realizzati nel complesso di capacità ISTAR, il “sogno” di politici e strateghi di poter combattere e vincere le guerre risparmiando la vita delle proprie truppe sembra destinato ad avverarsi.

## 6.2. I droni e l’opinione pubblica italiana

È così che un’arma semi-autonoma come i velivoli senza pilota, noti come droni, viene privilegiata dai politici e dai militari dell’Occidente, grazie ai suoi costi contenuti in termini economici e, apparentemente, politici. Tuttavia i droni hanno due avversari: il diritto internazionale e l’opinione pubblica. Gli interrogativi che l’impiego dei droni pone al diritto internazionale sono molti e complessi, così come sono crescenti le preoccupazioni espresse dalla società civile nei diversi paesi. A queste ultime intendiamo dar voce in questo capitolo, descrivendo il livello di conoscenza e il tenore delle opinioni che gli italiani fanno propri circa l’impiego dei droni in ambito civile e, soprattutto, militare.

Nell’ambito di una ricerca promossa da Archivio Disarmo sul ruolo dell’opinione pubblica di fronte alle armi semi-autonome, abbiamo iniziato reclinando un sondaggio nel quale, seguendo il modello Difebarometro<sup>1</sup>, abbiamo sottoposto un questionario appositamente costruito a un campione di 1000 intervistati di età superiore ai 18 anni, rappresentativo della popolazione italiana per genere, età e residenza geografica<sup>2</sup>.

<sup>1</sup> Difebarometro: rilevazione periodica Archivio Disarmo-SWG 1995-2008

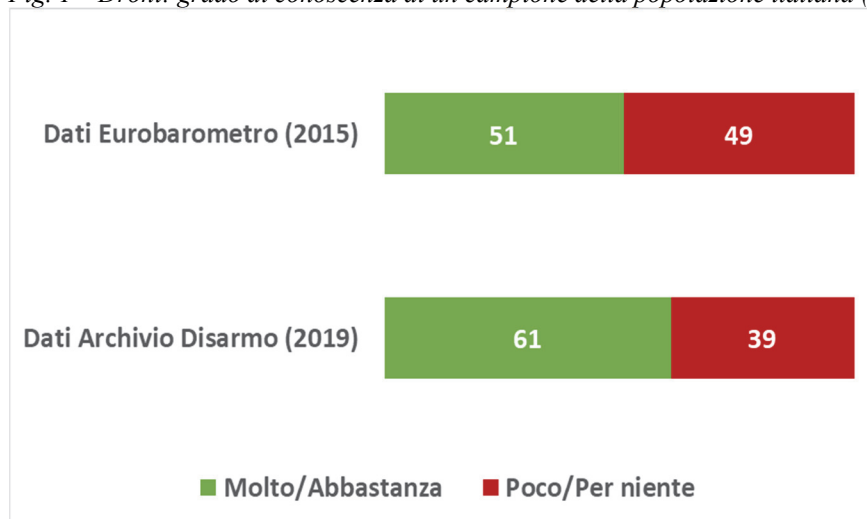
<sup>2</sup> La rilevazione è stata effettuata nel periodo 8-12 febbraio 2019 dalla società Demetra di Venezia, attraverso il metodo mixed-mode CATI – Computer Assisted Telephone Interviewing (50%) e CAWI – Computer Assisted Web Interviewing (50%).

### 6.3. Il fenomeno droni: livello di conoscenza e tenore delle opinioni

Il primo dato di merito che è emerso dal sondaggio è il livello di conoscenza dichiarato dal campione in riferimento ai velivoli a pilotaggio remoto. Per mostrare l'evoluzione del grado di conoscenza dei droni, il dato è messo a confronto con quello rilevato da Eurobarometro nel 2015.

La figura 1 (v.) mostra come, dalla rilevazione di Archivio Disarmo (2019), i droni siano conosciuti molto (13%) o abbastanza (48%) da una maggioranza del 61% degli intervistati. Non è peraltro da sottovalutare il significato di un'ampia minoranza (39%), formata da coloro che dichiarano di conoscere poco o di non conoscere per niente questo "nuovo" prodotto della tecnologia. Peraltro il dato si discosta positivamente (+10%) da quello rilevato due anni prima da Eurobarometro che, riguardo alla conoscenza dei droni (civili) da parte degli italiani, registrava un 49% di risposte negative (Eurobarometro 2015, cit. in IRIAD 2019, pp. 128-130).

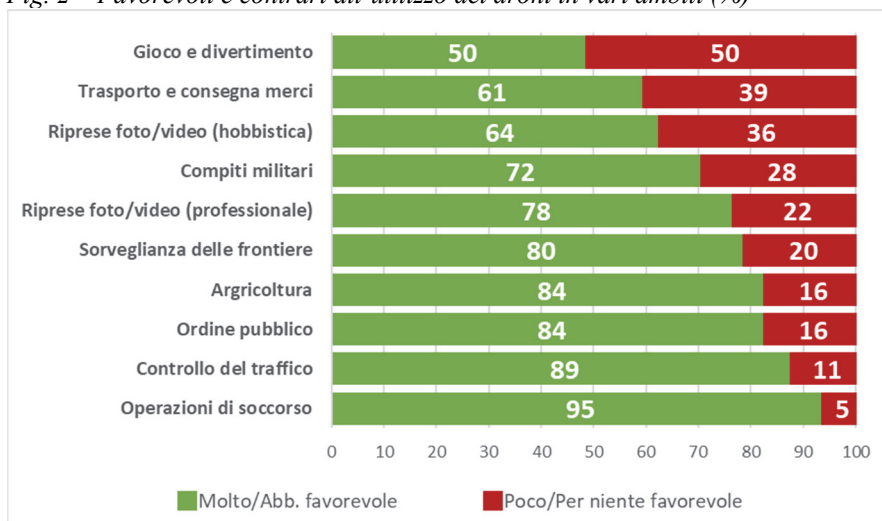
Fig. 1 – Droni: grado di conoscenza di un campione della popolazione italiana (%)



Fonte: Eurobarometro 2015 e Archivio Disarmo – Demetra 2019

Le prime opinioni rilevate dall'indagine demoscopica riguardano l'atteggiamento favorevole o contrario nei confronti dell'utilizzo dei droni. In proporzioni che differiscono notevolmente nei diversi settori d'impiego, i favorevoli superano di larga misura i contrari in ordine alla maggior parte di essi (v. figura 2).

Fig. 2 – Favorevoli e contrari all’utilizzo dei droni in vari ambiti (%)\*



\*La variabile è stata ricodificata depurata dai “Non so”

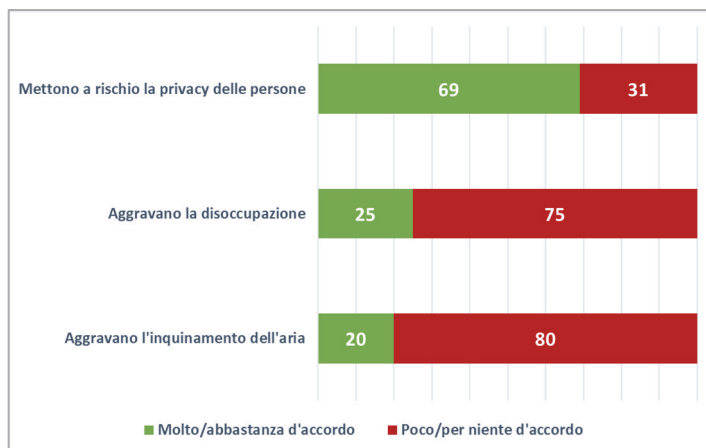
Fonte: Archivio Disarmo – Demetra 2019

La figura 2 mostra come, eccezion fatta per l’uso dei droni in situazioni di gioco e divertimento, il numero di intervistati che si dichiara abbastanza o molto favorevole a questa tecnologia supera generalmente il 50%, sino a raggiungere quote superiori all’80% nella sorveglianza delle frontiere (80%), in agricoltura (84%), nell’ordine pubblico (84%), nel controllo del traffico (89%). Al primo posto si collocano le operazioni di soccorso (95%), un settore in cui i velivoli a pilotaggio remoto già nel primo decennio degli anni 2000 hanno avuto modo di dimostrare pubblicamente la loro utilità. Per quanto riguarda l’utilizzo dei droni in “compiti militari” il consenso si attesta su circa i 2/3 dei rispondenti (72%). Più contenuto (61%) il favore accordato all’utilizzo dei droni nel campo del “trasporto e consegna merci”, probabilmente per il timore che in questa funzione essi possano esercitare una concorrenza dannosa nei confronti del lavoro umano.

Il generale consenso riscontrato dall’utilizzo dei droni in diversi settori d’impiego emerge anche chiedendo al campione di esprimere il proprio grado di accordo/disaccordo nei confronti delle possibili conseguenze, sia positive che negative. Per quanto riguarda gli aspetti potenzialmente negativi, l’unico ambito che suscita prevalentemente preoccupazione (da parte del 69% dei rispondenti) riguarda la possibilità che l’utilizzo dei droni metta a rischio la privacy delle persone, un atteggiamento già presente nelle rilevazioni effettuate da Dronitaly (2015) e quella cross-national del Pew Research Center (2015). Solo il 25% dei rispondenti teme che l’utilizzo dei droni possa

incidere negativamente sull'occupazione e il 20% che possa aggravare l'inquinamento dell'aria (v. figura 3).

Fig. 3 – Droni: grado di accordo con le seguenti affermazioni (%)\*

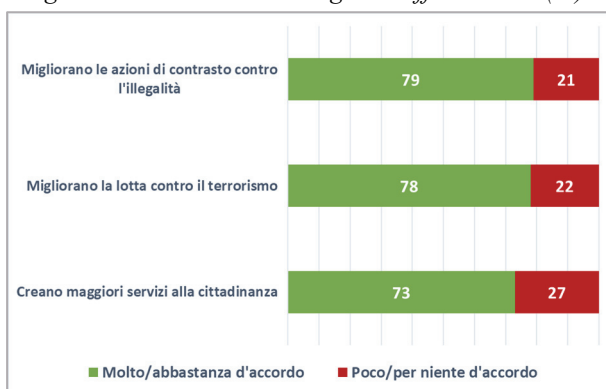


\*La variabile è stata ricodificata depurata dai "Non so"

Fonte: Archivio Disarmo – Demetra 2019

Rispetto alle conseguenze positive dell'utilizzo dei velivoli senza pilota, i rispondenti si trovano in larga maggioranza d'accordo con tutte le affermazioni sottoposte loro. Per il 79% del campione l'impiego dei droni migliora le azioni di contrasto contro l'illegalità, quote di poco inferiori sono quelle di chi crede migliori la lotta al terrorismo (78%) o di chi sostiene che il loro utilizzo produce maggiori servizi alla cittadinanza (73%), (v. fig. 4).

Fig. 4 – Droni: grado di accordo con le seguenti affermazioni (%)\*

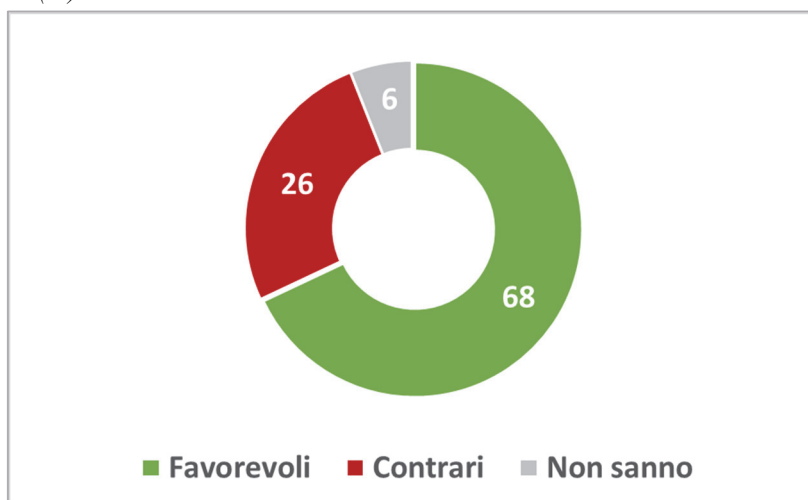


\*La variabile è stata ricodificata depurata dai "Non so"

Fonte: Archivio Disarmo – Demetra 2019

Passiamo ora all'utilizzo dei velivoli a pilotaggio remoto in operazioni militari. Come abbiamo accennato in precedenza, laddove non venga specificato se si tratti di un impiego in operazioni di sorveglianza piuttosto che di attacco, né venga fatto specifico riferimento al loro utilizzo da parte del governo italiano, ciò suscita un favore pari al 68% (v. figura 5).

Fig. 5 – Favorevoli e contrari all'utilizzo dei droni nello svolgimento di compiti militari (%)



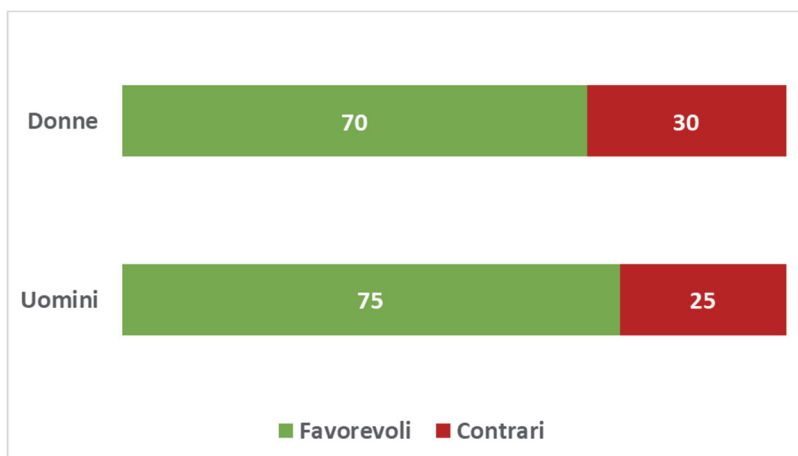
Fonte: Archivio Disarmo – Demetra 2019

Prendendo in considerazione la variabile di genere, vediamo come gli uomini, con un 75% di favorevoli, dichiarino un maggiore favore rispetto alle donne (70%), mostrando all'interno del campione considerato i sintomi di un divario tra generi che vede quello femminile tendenzialmente meno propenso all'uso della forza (v. figura 6).

L'analisi della variabile di genere in relazione al "grado di favore rispetto all'utilizzo dei droni in compiti militari" tramite il test del Chi quadrato di Pearson mostra una relazione non così forte da rappresentare una significatività statistica ( $P=0,167$ ). Dunque, seppur nel nostro campione osserviamo un maggior favore dei maschi rispetto alle femmine (con uno scarto percentuale del 5%), a partire da questo semplice dato non saremmo autorizzati ad estendere tale considerazione all'intera popolazione italiana. Rinviamo quindi l'approfondimento del divario uomini/donne alla successiva analisi dei distinti compiti militari da affidare ai droni<sup>3</sup>.

<sup>3</sup> Vedi oltre p. 122.

Fig. 6 – Favorevoli e contrari all’utilizzo dei droni nello svolgimento di compiti militari per genere (%)\*

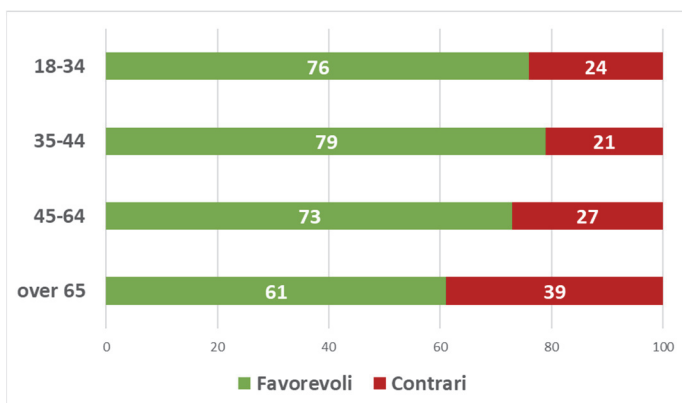


\*La variabile è stata ricodificata depurata dai “Non so”

Fonte: Archivio Disarmo – Demetra 2019

Passando ad analizzare la variabile anagrafica nei favorevoli e contrari all’utilizzo dei droni nei compiti militari, notiamo che, al crescere dell’età, diminuisce il grado di favore, eccezion fatta per la fascia 35-44 che, con un 79% di favorevoli, supera di tre punti percentuali il consenso espresso dai più giovani. La percentuale di favore più bassa è manifestata dagli over 65 (61%) (v. figura 7).

Fig. 7 – Favorevoli e contrari all’utilizzo dei droni nello svolgimento di compiti militari per età (%)\*



\* La variabile è stata ricodificata depurata dai “Non so”

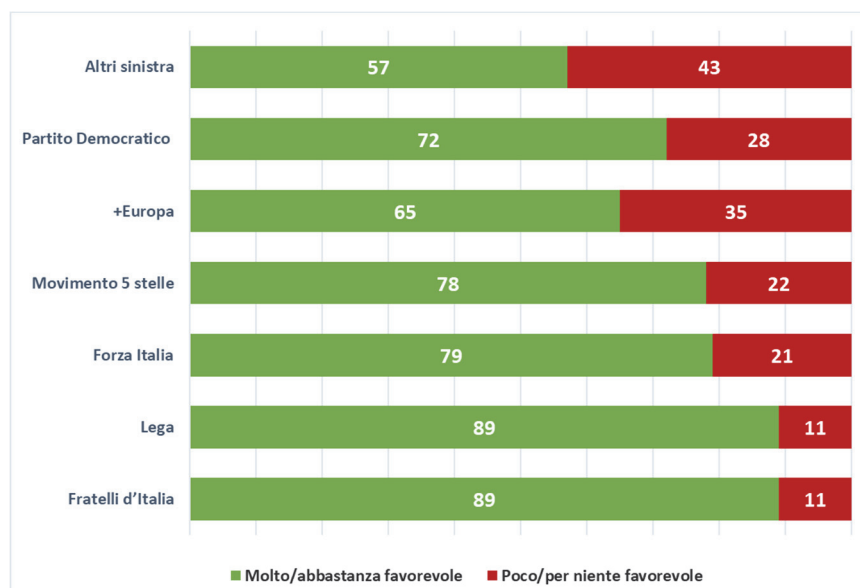
Fonte: Archivio Disarmo – Demetra 2019

Il test del Chi quadrato conferma che la relazione della variabile età con il grado di favore rispetto all'impiego dei droni in compiti militari è statisticamente significativa ( $P=0,001$ ): all'aumentare dell'età aumentano coloro i quali sono contrari all'utilizzo militare dei droni.

Sono in particolare gli over 65, appartenenti alla coorte demografica dei baby boomer, ad esprimere la maggiore contrarietà rispetto all'utilizzo dei droni militari. Essi si confermano così la "generazione della protesta" che ha vissuto l'esperienza storica del '68 e degli anni '70 (Jennings, 1987; Caren *et al.*, 2010).

Passando alla distribuzione del favore in base alla collocazione politica (rilevata sulla base del partito votato alle ultime elezioni politiche), questa mostra il diverso atteggiamento della destra e della sinistra nei confronti dell'utilizzo dei droni militari. Gli elettori di Fratelli d'Italia e della Lega esprimono il loro favore nei confronti di questi sistemi d'arma con l'89% dei rispondenti che si dichiara abbastanza o molto favorevole. Il consenso va tendenzialmente diminuendo quando ci si sposta verso il centro e quindi verso la sinistra: dal 79% di Forza Italia si passa al 78% del Movimento 5 Stelle e al 72% del PD sino a scendere al 57% degli elettori alla sinistra di quest'ultimo partito (v. figura 8).

Fig. 8 – Quanto è favorevole o contrario all'uso dei droni nei compiti militari? (%)\*



\*La variabile è stata ricodificata depurata dai "Non so"

Fonte: Archivio Disarmo – Demetra 2019



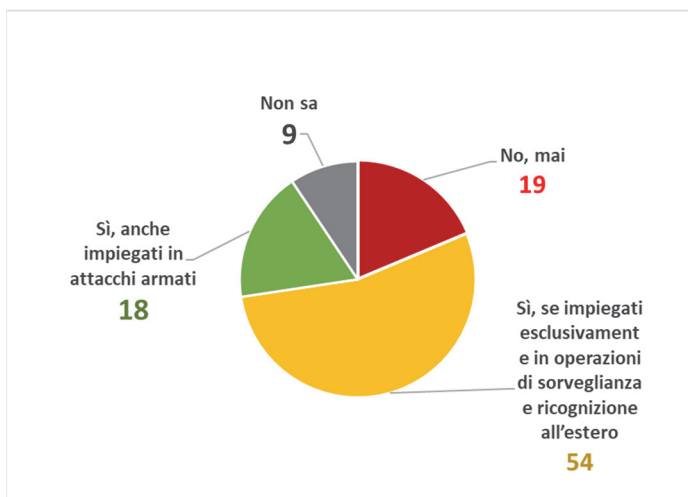
Sottoponendo al test del Chi quadrato la relazione tra variabile indipendente “intenzioni di voto” e il grado di favore rispetto all’impiego di droni in compiti militari, emerge che questa presenta una significatività statistica ( $\text{Sign} < 0,001$ ) tale per cui possiamo affermare che il posizionamento politico appare collegato con l’opinione sull’utilizzo dei velivoli senza pilota in operazioni militari.

Il quadro cambia notevolmente a fronte di due importanti specificazioni, cioè quando, al posto di esprimere un favore o un’opposizione nei confronti dei droni militari in generale, agli intervistati vengono sottoposte due precise circostanze: un impiego dei droni militari da parte del governo italiano, nonché la natura di tale impiego per operazioni di sorveglianza o viceversa per attacchi armati.

Come mostra la figura 9, un po’ più della metà dei rispondenti (54%) si dichiara favorevole all’utilizzo dei droni se impegnati esclusivamente in operazioni di ricognizione e sorveglianza all’estero. Soltanto il 18% sottoscrive l’utilizzo dei velivoli a pilotaggio remoto per attacchi armati mentre, agli antipodi da tale posizione, si situa un quasi simmetrico 19% che è contrario all’uso dei droni militari italiani in qualsiasi circostanza.

Elevato, ma prevedibile in riferimento a una domanda obiettivamente impegnativa anche per gli aspetti “tecnici” che chiama in causa, la quota (9%) di chi non sa/non risponde.

*Fig. 9 – Sarebbe favorevole all’utilizzo di droni per scopi militari da parte del governo italiano (%)?*



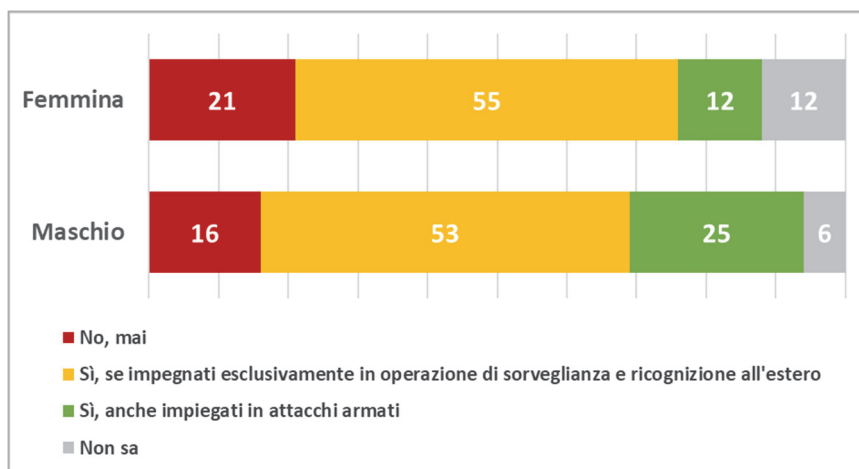
Fonte: Archivio Disarmo – Demetra 2019

Possiamo quindi concludere che il generale favore espresso dal campione nei confronti dei droni militari (già illustrato nella figura 5) si ridimensiona nettamente in precise circostanze: quando, cioè, viene prospettata l'eventualità di un effettivo utilizzo da parte del governo italiano in operazioni di attacco armato.

Tornando sulla variabile di genere, si rileva la maggiore diffidenza delle donne nei confronti dell'uso dei droni in funzioni di attacco (v. figura 10).

Solo il 12% delle donne intervistate (meno della metà rispetto agli uomini), si dichiara favorevole all'utilizzo dei velivoli a pilotaggio remoto in attacchi armati da parte del governo italiano, mentre il 21% afferma la propria contrarietà nei confronti dell'uso dei droni militari in qualsiasi ambito (a fronte del 16% dei maschi). È plausibile che in questa diffidenza pesino due fattori. Il primo può essere individuato nella minore conoscenza dei sistemi d'arma e tecnologica in genere da parte delle donne. Infatti la percentuale di esse che non esprime una propria opinione è doppia rispetto a quella degli uomini (il 12% dichiara che "non sa" contro il 6% degli uomini). Il secondo fattore può essere individuato in quello che è stato definito il *gender gap*, cioè la tendenza, attestata dalla quasi totalità delle inchieste demoscopiche e dagli studi di opinione pubblica, circa la più spiccata ostilità femminile nei confronti di tutte le forme di violenza, anche quelle istituzionalizzate e legittimamente impiegate dallo Stato per la difesa (Ammendola, 1993; Farina, 1995).

Fig. 10 – Favorevoli all'utilizzo di droni per scopi militari da parte del governo italiano per sesso (%)

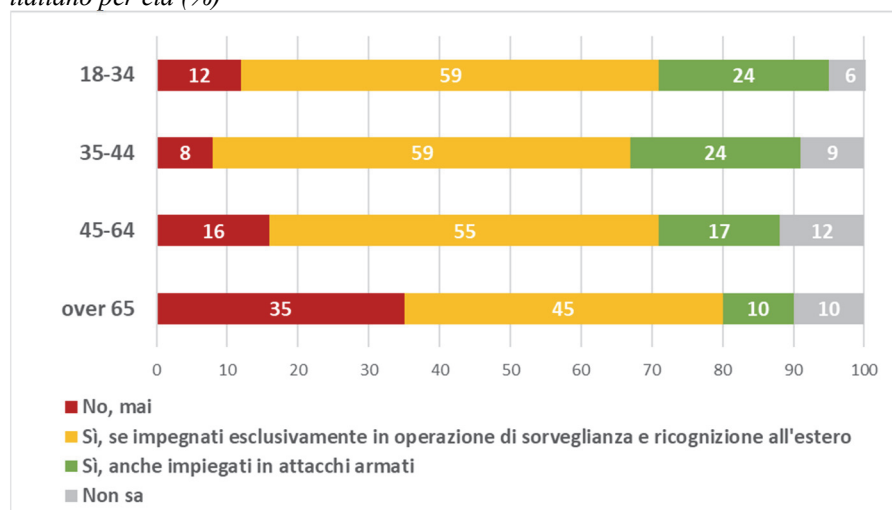


Fonte: Archivio Disarmo – Demetra 2019

La significatività statistica della relazione tra variabile indipendente sesso e il grado di favore rispetto all'utilizzo dei droni militari da parte del governo italiano è confermata dal test del Chi quadrato ( $P < 0,001$ ).

Venendo poi a considerare l'età dei rispondenti, si conferma l'atteggiamento degli over 65 i quali, in una percentuale pari al 35% affermano la loro contrarietà, in qualsiasi circostanza, all'utilizzo dei droni militari, a fronte dell'8% di assolutamente contrari registrati tra gli appartenenti alla classe d'età 33-45. In tutti i gruppi l'opzione maggiormente indicata è quella che prevede l'impiego di droni militari solo in operazioni di sorveglianza e ricognizione (v. figura 11).

Fig. 11 – Favorevoli all'utilizzo di droni per scopi militari da parte del governo italiano per età (%)



Fonte: Archivio Disarmo – Demetra 2019

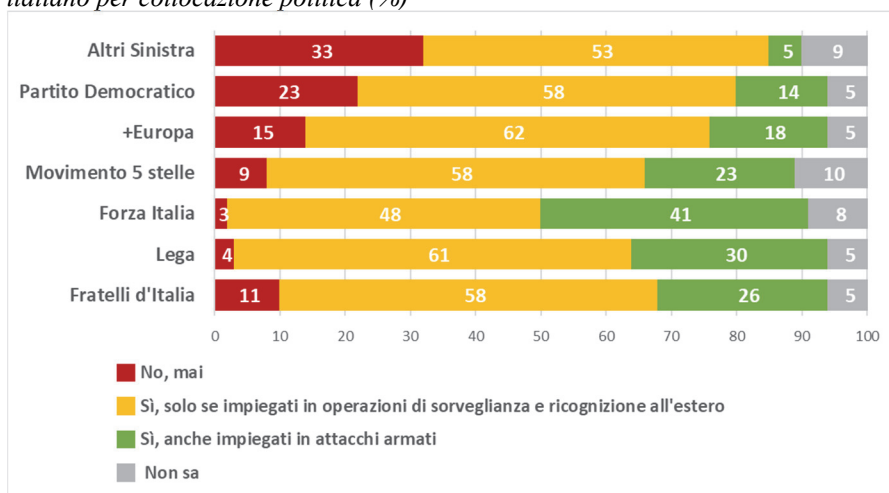
Sottoposta al test del Chi quadrato, la relazione tra la variabile indipendente età e l'opportunità di utilizzo dei droni per scopi militari da parte del governo italiano presenta una significatività statistica ( $P < 0,001$ ).

Considerando infine la variabile della scelta politica, emerge nuovamente una netta diversità di atteggiamento nei confronti dell'uso dei droni deciso dal governo italiano da parte di destra e sinistra (v. figura 12).

La piena contrarietà verso l'utilizzo dei droni militari da parte del governo italiano viene espressa dal 33% degli elettori dei partiti di sinistra radicale, dal 23% dei votanti PD, dal 15% di + Europa e dal 9% del Movimento 5 Stelle. La quota degli oppositori si riduce significativamente tra gli elettori

del centro-destra: Forza Italia (3%) e Lega (4%). Degna di nota è la posizione degli elettori di Fratelli d'Italia tra i quali i contrari superano il 10%, ovvero una percentuale nettamente superiore alle altre del centro-destra. Si tratta di un dato controintuitivo che segnala una riserva circa l'impiego di droni in attacchi armati, presumibilmente in favore di tattiche di combattimento più coerenti con il modello tradizionale di combattente.

Fig. 12 – Favorevoli all'utilizzo di droni per scopi militari da parte del governo italiano per collocazione politica (%)

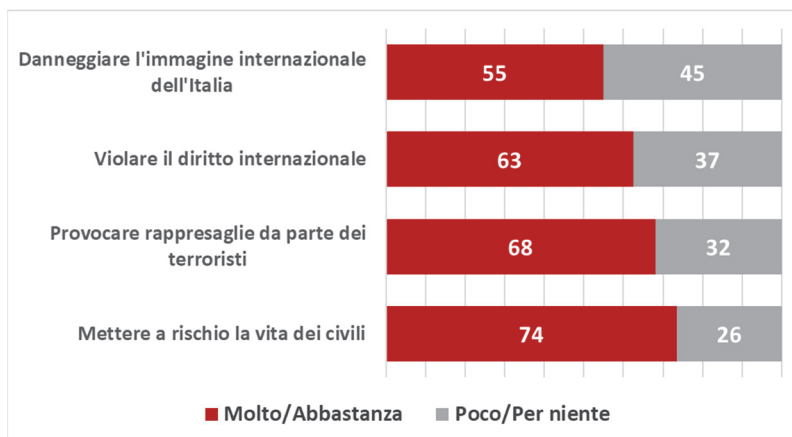


Fonte: Archivio Disarmo – Demetra 2019

Andando infine ad analizzare quali sono le principali preoccupazioni su possibili conseguenze dell'impiego dei droni da parte dell'Italia per compiere attacchi armati, è da notare che, in linea con le principali risultanze a livello internazionale, il timore principale, espresso dal 73,5% dei rispondenti, fa riferimento all'eventualità di mettere a rischio la vita dei civili, seguito dal rischio di provocare rappresaglie. Preoccupano relativamente meno le possibilità di violazione del diritto internazionale (62,5%) e il danneggiamento dell'immagine dell'Italia a livello internazionale (55%) (v. figura 13).

Sono le donne a dimostrarsi più preoccupate delle possibili conseguenze negative dell'utilizzo dei droni per compiere attacchi armati, con uno scarto massimo tra i due sessi del 14,4% riguardo al possibile danneggiamento dell'immagine internazionale dell'Italia. Effettuando il test del Chi quadrato, emerge come la preoccupazione rispetto a tutte e quattro le possibili conseguenze negative dell'uso dei droni in compiti militari in relazione alla variabile di genere sia statisticamente significativa, con un p-value sempre inferiore allo 0,005.

Fig. 13 – Preoccupazioni su possibili conseguenze dell’impiego dei droni per compiere attacchi armati (%)



Fonte: Archivio Disarmo – Demetra 2019

Si tratta di un'ulteriore conferma del *gender gap* che caratterizza l'atteggiamento femminile come a quello maschile in merito all'uso della forza.

## Riferimenti bibliografici

- Ammendola T. (1993), “Opinione pubblica e politica militare in Italia”, *Rivista Trimestrale di Scienza dell'Amministrazione*, 3-4: 277-299.
- Burk J. (1998) (a cura), *La guerra e il militare nel nuovo sistema internazionale*, FrancoAngeli, Milano.
- Caren N., Ghoshal R.A., Ribas V. (2010), “A social movement generation: Cohort and Period Trends in protest attendance and petition signing”, *American Sociological Review*, 20 (10): 1-27
- Farina F. (1995), “Recenti tendenze dell'opinione pubblica sulle questioni militari”, in Gobbicchi (a cura di), *La professione militare oggi. Caratteristiche sociali e nuovo contesto geopolitico*, FrancoAngeli, Milano.
- Isernia P. (1996), *Dove gli angeli non mettono piede. Opinione pubblica e politiche di sicurezza in Italia*, FrancoAngeli, Milano.
- Isernia P. e Everts PH. (2003), “Uniti attorno alla bandiera? Le opinioni pubbliche di Europa e Stati Uniti di fronte alla guerra”, *Italianieuropei*, 2: 49-78.
- Jennings M. K. (1987), “The aging of the American protest generation”, *American Political Science Review*, 81(2): 302-316.
- F. Battistelli (2102), “Atteggiamenti, opinioni, uso della forza. Un'introduzione”, in Battistelli F., Galantino M. G., Lucianetti L., Striuli L. (a cura), *Opinioni sulla guerra*, FrancoAngeli, Milano.

## **Sitografia dei sondaggi**

[http://www.dronitaly.it/wp2015/wpcontent/uploads/2014/12/sumberesi\\_indagine\\_droni\\_risultati.pdf](http://www.dronitaly.it/wp2015/wpcontent/uploads/2014/12/sumberesi_indagine_droni_risultati.pdf)

<http://www.pewresearch.org/fact-tank/2013/05/23/a-majority-ofamericans-still-support-use-of-drones-despite-questions/>

<http://www.pewresearch.org/fact-tank/2013/10/23/report-questionsdrone-use-widely-unpopular-globally-but-not-in-the-u-s/>

## 7. L'opinione pubblica di fronte alle armi autonome

di Francesca Farruggia

### 7.1. L'opinione pubblica mondiale e le armi autonome

L'applicazione dell'intelligenza artificiale all'industria della difesa sta sollevando sempre maggiori preoccupazioni nel dibattito internazionale. In particolare, suscitano contrarietà i cosiddetti “killer robot”, sistemi autonomi d'attacco che, come esposto nei capitoli precedenti, sarebbero in grado di selezionare e attaccare singoli obiettivi senza un controllo umano. In Italia la previsione delle conseguenze critiche che potrebbero derivare dallo sviluppo di tali sistemi d'arma ha portato nel marzo del 2019 centodieci ricercatori di varie discipline (in particolare quelle collegate all'informatica, alla robotica e all'intelligenza artificiale) a presentare al governo e al parlamento italiani un appello per la messa al bando delle armi completamente autonome, ritenendole “moralmente inaccettabili”<sup>1</sup>.

Le principali analisi sul tema, presentate in questo capitolo, ci mostrano come tali preoccupazioni siano condivise dall'opinione pubblica a livello mondiale.

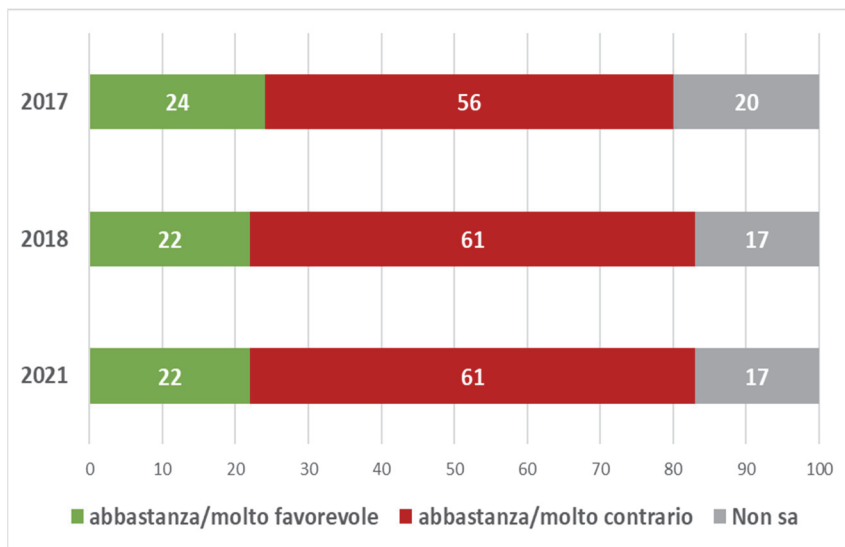
Soltanto la possibile opposizione dei cittadini allo sviluppo delle armi autonome è in grado di portare i Governi ad adottare quadri normativi per contrastare la minaccia proveniente dall'impiego delle Armi Autonome. È così che nel gennaio del 2017 la *Campaign to Stop Killer Robots* ha lanciato un primo sondaggio in 23 Paesi volto a rilevare l'atteggiamento dell'opinione pubblica mondiale nei confronti dei LAWS. La rilevazione è stata reiterata nel 2018, coinvolgendo 26 Paesi, e nel 2021, coinvolgendone 28.

L'analisi dei dati rilevati da IPSOS mostra che nel 2017 il 56% degli intervistati dichiara di opporsi all'utilizzo dei robot killer in guerra. La per-

<sup>1</sup> Vedi oltre, capp. 9 e 10.

centuale di oppositori sale al 61% nella successiva indagine condotta nel dicembre del 2018 e rimane stabile nel 2021 (v. fig. 1)<sup>2</sup>.

Fig. 1 – Favorevoli e contrari alle armi autonome in 23 (2017), 26 (2018) e 28 Paesi (2021)



Fonte: Elaborazione Archivio Disarmo su dati Ipsos (2017, 2018 e 2021)

Consideriamo ora il favore rispetto alle armi autonome nell'ultima rilevazione del 2021 mettendola in relazione con la variabile di genere.

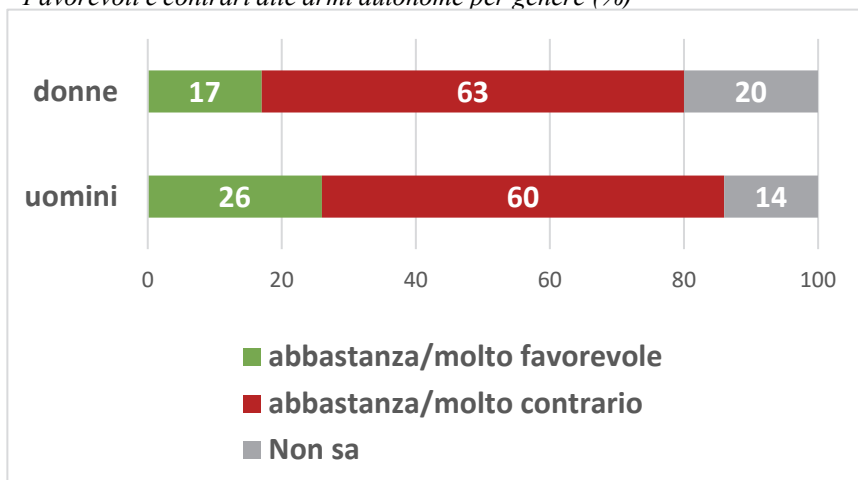
Come emerso anche dall'analisi su opinione pubblica e utilizzo dei droni in ambito militare (vedi cap. 6), le donne si mostrano maggiormente contrarie rispetto agli uomini sull'utilizzo di armi autonome in teatri di guerra (il 63% contro il 60%) (v. fig.2).

Considerando poi la variabile età, anche in questo caso sono i più maturi a mostrarsi maggiormente restii verso l'utilizzo delle nuove tecnologie in campo militare. Il 69% di chi appartiene alla fascia d'età compresa tra i 50 e i 74 anni si dichiara infatti contrario all'utilizzo delle armi autonome, a fronte di un 61% di contrari nella fascia 35-49 e di un 54% di chi ha meno di 35 anni (v. fig. 3).

<sup>2</sup> Il sondaggio Ipsos del 2021 ha coinvolto in totale circa 19.000 intervistati, utilizzando campioni di 500-1000 persone in ognuno dei seguenti 28 Paesi: Argentina, Australia, Belgio, Brasile, Canada, Cina, Colombia, Corea del Sud, Francia, Germania, Giappone, Gran Bretagna, India, Israele, Italia, Messico, Norvegia, Paesi Bassi, Perù, Polonia, Russia, Spagna, Stati Uniti, Sudafrica, Svezia, Svizzera, Turchia e Ungheria.

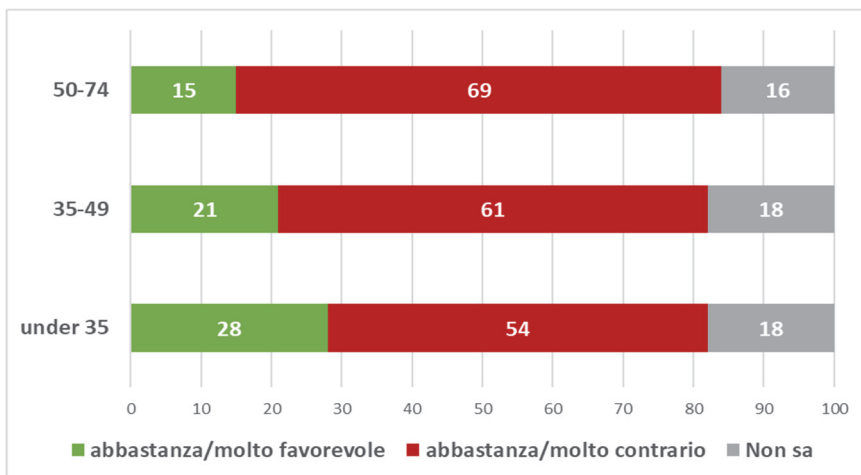


Fig. 2 – Favorevoli e contrari alle armi autonome per genere (%)



Fonte: Elaborazione Archivio Disarmo su dati Ipsos 2021

Fig. 3 – Favorevoli e contrari alle armi autonome per età (%)



Fonte: Elaborazione Archivio Disarmo su dati Ipsos 2021

Da quest'ultima rilevazione emerge che l'opinione pubblica di 27 Paesi su 28 si dichiara contraria all'utilizzo di armi autonome in guerra. L'opposizione è più forte in Svezia (76%), Turchia (73%) e Ungheria (70%). Di contro, confermando quanto emerso dalla precedente indagine, l'opinione pubblica più incline al loro utilizzo è quella indiana con una percentuale del 56% (+6% rispetto al 2018). I Paesi che mostrano la più ampia percentuale di rispondenti che non dichiara una propria opinione sono Francia (30%), Giappone (29%) e Paesi Bassi (26%).

È da notare come nei cinque Paesi più attivi nello sviluppo e nella sperimentazione di questi sistemi con livelli decrescenti di controllo umano la maggioranza sia contraria ai killer robots: Russia (58%), Regno Unito (56%), USA (55%), Cina (53%) e Israele (53%) (v. tab. 1).

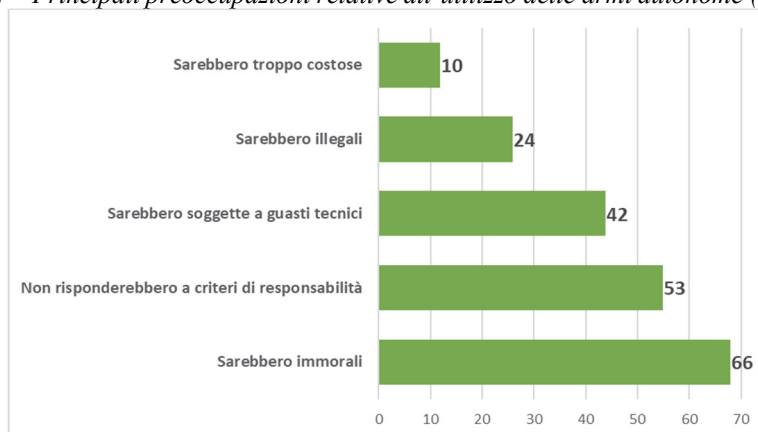
Tab. 1 – Favorevoli e contrari alle armi autonome

	Favorevoli	Contrari	Non sanno
<b>Russia</b>	23%	58%	19%
<b>Regno Unito</b>	20%	56%	24%
<b>USA</b>	22%	55%	23%
<b>Cina</b>	39%	53%	8%
<b>Israele</b>	28%	53%	19%

Fonte: Ipsos per Campaign to Stop Killer Robots, 2021

A quanti si sono dichiarati contrari alle armi autonome è stato poi chiesto quali fossero le principali fonti di preoccupazione legate al loro utilizzo. Una ristretta percentuale (10%) ritiene che la loro produzione sarebbe troppo costosa e poco meno di un quarto del campione (24%) dichiara che il loro utilizzo sarebbe illegale. Rilevante è invece la percentuale di coloro i quali ritengono che le armi autonome andrebbero soggette a guasti tecnici (42%) e di chi sostiene che tali sistemi d'arma non risponderebbero a criteri di responsabilità e di controllo (53%). La maggiore preoccupazione dei rispondenti fa però riferimento a questioni morali. I due terzi degli intervistati (66%) ha infatti risposto che i sistemi di arma autonome “supererebbero una linea morale poiché alle macchine non dovrebbe essere permesso di uccidere” (v. fig. 4).

Fig. 4 – Principali preoccupazioni relative all'utilizzo delle armi autonome (%)



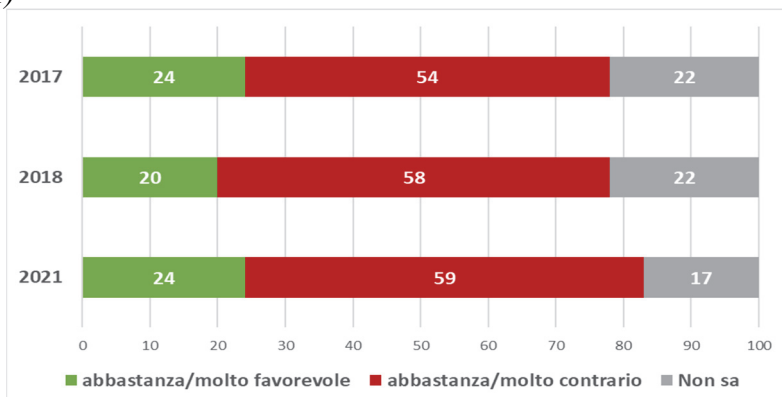
Fonte: Ipsos per Campaign to Stop Killer Robots, 2021

## 7.2. L'opinione pubblica italiana e le armi autonome

### 7.2.1. L'indagine IPSOS

Anche l'opinione pubblica italiana si dichiara in maggioranza contraria all'utilizzo delle armi autonome. Un'opposizione che dal gennaio 2017 al gennaio 2021 cresce dal 54% al 59% (v. fig. 5).

Fig. 5 – Favorevoli e contrari alle armi autonome in Italia (anno 2017, 2018 e 2021)

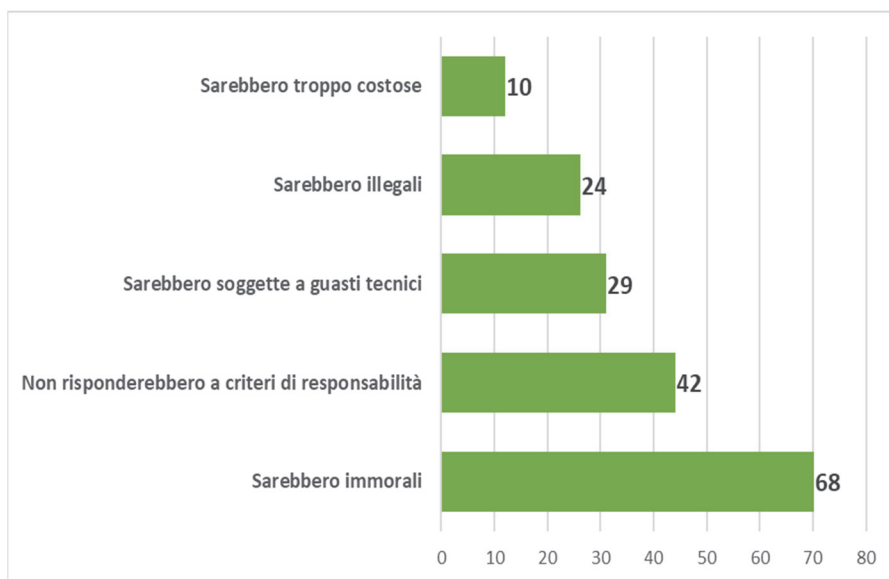


Fonte: Ipsos per Campaign to Stop Killer Robots, 2017, 2018 e 2021

Come emerso anche dal dato a livello mondiale, la maggiore preoccupazione degli italiani rispetto ai sistemi d'arma autonomi è quella relativa al superamento di una barriera morale secondo cui le macchine non dovrebbero poter decidere della vita e della morte di un essere umano. Infatti il 68% degli oppositori a tale sistema d'arma li reputa immorali. L'opinione pubblica italiana, insieme a quella degli altri 28 Paesi coinvolti nella rilevazione, sembra dunque condividere una preoccupazione fortemente espressa da esperti e scienziati a livello internazionale che, oltre ad evidenziare come tali sistemi d'arma potrebbero minacciare le norme legali e diplomatiche consolidate, ritengono che tali macchine non abbiano e non avranno mai la capacità morale di decidere della vita o della morte di un essere umano.

Inoltre, il 42% teme che il loro utilizzo farebbe venire meno i criteri di responsabilità e controllo umano. Il 29% dei rispondenti è preoccupato per i possibili guasti tecnici in cui i robot killer potrebbero incorrere, percentuale relativamente esigua confrontata al dato mondiale che è più alto di 13 punti percentuale. Ancora più contenute le percentuali di chi le ritiene illegali (24%) o troppo costose (10%) (v. fig. 6).

Fig. 6 – Principali preoccupazioni degli italiani relative all'utilizzo delle LAWS (%)



Fonte: Ipsos per Campaign to Stop Killer Robots, anno 2021

## 7.2.2. L'indagine Demetra-Archivio Disarmo

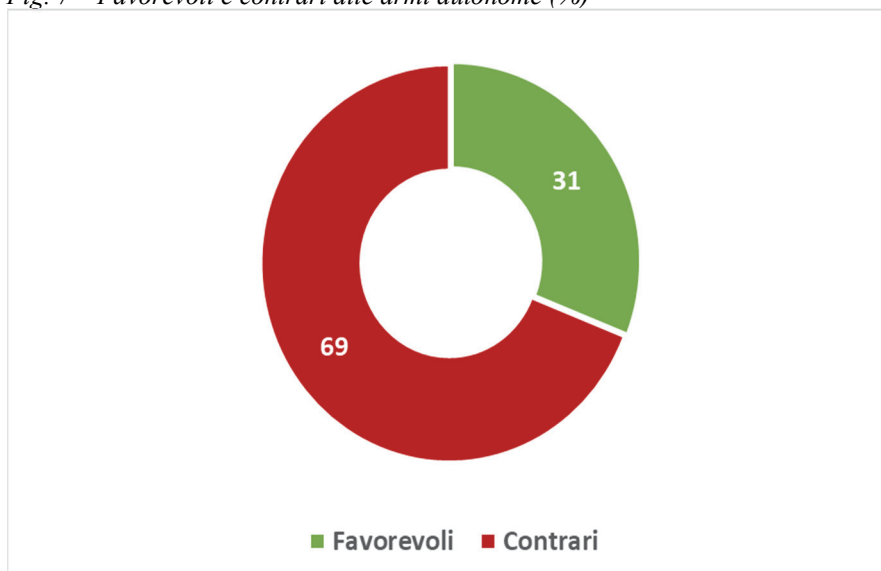
Nell'ambito del sondaggio di opinione effettuato da Archivio Disarmo nel 2019 e presentato nel cap. 6, abbiamo sottoposto una domanda sulle armi autonome all'interno del questionario somministrato a un campione di 1000 intervistati di età superiore ai 18 anni, rappresentativo della popolazione italiana per genere, età e residenza geografica.

Richiesti di esprimersi circa lo sviluppo ad opera di alcuni paesi di armi autonome, cioè in grado di operare da sole sul campo di battaglia, oltre 2/3 degli intervistati (depurati dei “non sa, non risponde”) si dichiara contrario e un po' meno di 1/3 favorevole (v. fig. 7). Tra i primi, ben il 40% si dichiara “molto contrario”.

Ancora una volta, è interessante correlare l'opinione espressa dagli intervistati con alcune caratteristiche strutturali dei medesimi. Iniziando dalla variabile appartenenza sessuale, le donne accentuano significativamente la loro contrarietà a questo tipo di armi, con il 73% di valutazioni negative rispetto al 65% espresso dagli uomini (v. fig. 8), a conferma del più volte richiamato *gender gap*.

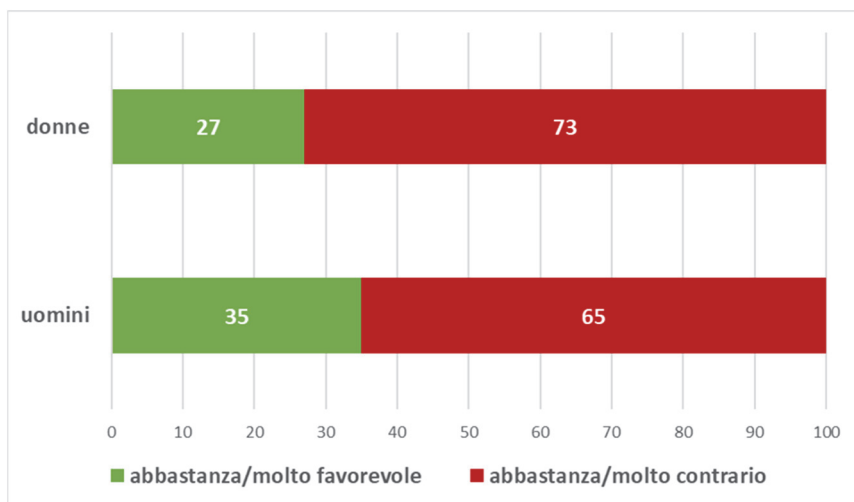
La significatività statistica della relazione tra variabile indipendente sesso e il grado di favore rispetto all'utilizzo di armi autonome sul campo di battaglia è confermata dal test del Chi quadrato ( $P = 0,004$ ).

Fig. 7 – Favorevoli e contrari alle armi autonome (%)



Fonte: Rilevazione Archivio Disarmo – Demetra 2019

Fig. 8 – Armi autonome: favorevoli e contrari alle armi secondo il genere (%)

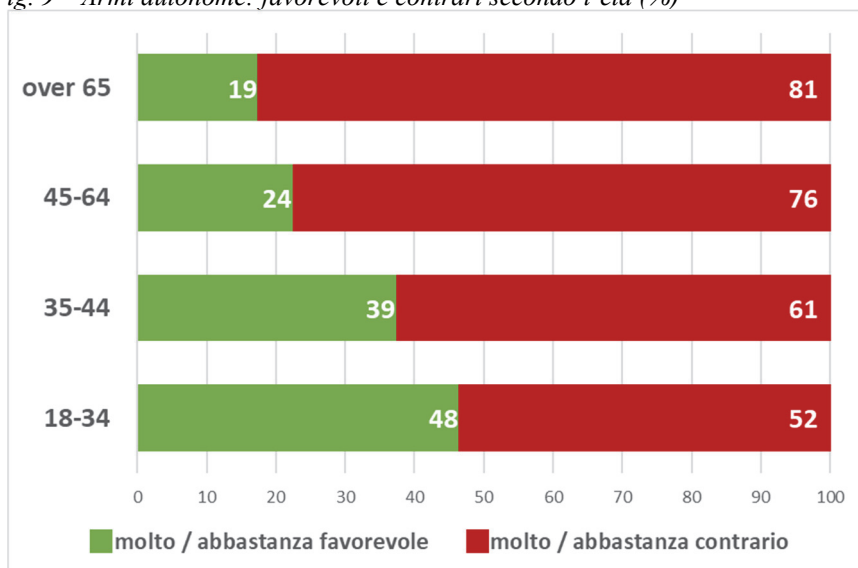


Fonte: Rilevazione Archivio Disarmo – Demetra 2019.

Il grado di favore nei confronti dell'impiego delle LAWS rispetto all'età (articolata in quattro fasce: 18-35, 35-44, 45-64, 65 e oltre) presenta un andamento lineare in cui all'avanzare dell'età corrisponde un atteggiamento via via più contrario nei confronti dello sviluppo delle armi autonome: dal limitato divario tra favorevoli (47,7%) e contrari (52,3%) nella fascia di età 18-34 all'ampia maggioranza di valutazioni negative (oltre 4/5 dei rispondenti) nella fascia di età degli ultra-sessantacinquenni. L'incidenza relativamente elevata di giovani che guardano con favore alle armi autonome appare inversamente proporzionale alla cognizione di ciò che esse potrebbero rappresentare sul campo di battaglia e in genere nella società. Così le evidenti discrepanze tra le varie fasce d'età del nostro campione sono interpretabili con la diffidenza verso l'uso della forza che tende ad aumentare con gli anni degli intervistati e con la presumibile maggiore consapevolezza relativa al ruolo degli armamenti nelle crisi internazionali e nei conflitti. Nel caso dei più giovani, invece, la tecnologia esercita un'indubbia influenza come conquista e come mito. In esso possono confluire fascinazioni di diverso spessore, dall'attrattiva per le applicazioni scientifiche alle correnti pratiche consumistiche quali la diffusione dei videogame (v. fig. 9).

La significatività statistica nella relazione tra età e grado di favore rispetto all'uso delle LAWS è confermata dal test del Chi quadrato ( $P < 0,001$ ).

Fig. 9 – Armi autonome: favorevoli e contrari secondo l'età (%)



Fonte: Rilevazione Archivio Disarmo – Demetra, 2019

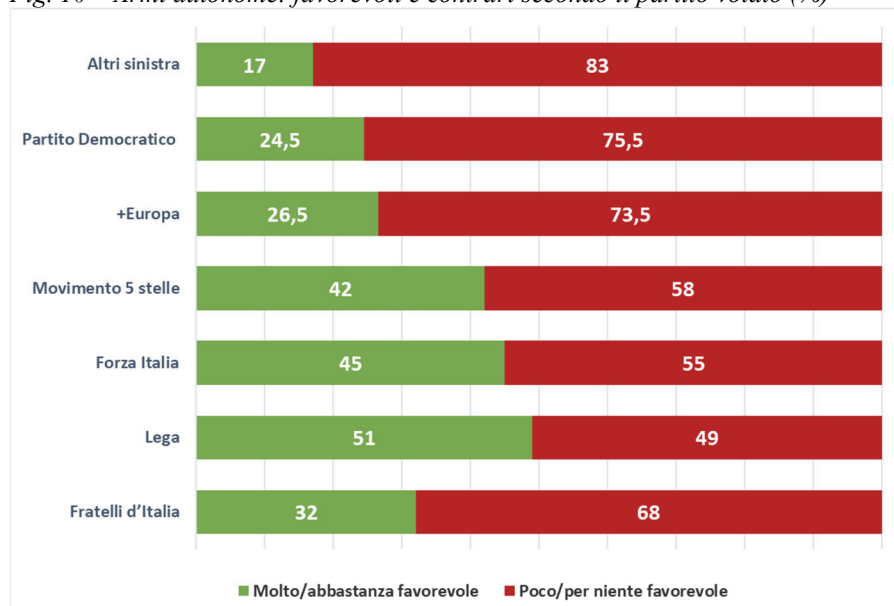
Infine la variabile orientamento politico è esposta nella figura 10 (v.). Rispondendo alla domanda relativa al partito votato alle ultime elezioni, emerge che a condividere sulle armi autonome un giudizio maggioritariamente (sia pur di poco: 50,8%) positivo vi sono gli elettori di un unico partito: la Lega. Tutti gli altri sono prevalentemente contrari, con un crescendo di opzioni che ripercorre puntualmente il *continuum* destra/sinistra: 55% Forza Italia, 58% Movimento 5 Stelle, 73% + Europa Partito democratico 75%, altri sinistra 83%. Un parziale scostamento dalla sequenza in crescita da sinistra a destra è rappresentato da un partito nettamente di destra, Fratelli d'Italia, che con il 68% dei contrari si oppone alle armi autonome in una misura che è a metà strada fra il Movimento 5 Stelle e il Partito Democratico. Come abbiamo ipotizzato in riferimento ai droni, anche rispetto alle armi autonome gli elettori di Fratelli d'Italia sono probabilmente influenzati da una cultura “eroica” che esprime una certa diffidenza nei confronti di strategie e tattiche proprie del modello “utilitaristico”, preferendo ad esso una visione tradizionale del militare che combatte a viso aperto e in prima persona.

La significatività statistica della relazione tra la variabile intenzione di voto e il grado di favore rispetto all'utilizzo di armi autonome sul campo di battaglia è confermata dal Test del Chi quadrato ( $P < 0,001$ ).

L'analisi dei dati sin qui presentata mostra dunque come le variabili considerate (genere, età e orientamento politico) abbiano una relazione stati-

sticamente significativa con il grado di favore rispetto l'utilizzo di armi autonome in teatri di guerra (registrando in tutti i casi un  $p$  value < 0,05).

Fig. 10 – Armi autonome: favorevoli e contrari secondo il partito votato (%)



Fonte: Rilevazione Archivio Disarmo – Demetra 2019

Per analizzare se tra queste vi sia anche una relazione causale, abbiamo effettuato una regressione logistica binaria. Possiamo quindi confermare come all'aumentare dell'età cresce in media la probabilità di essere contrari all'utilizzo delle armi autonome. L'essere maschio aumenta invece la probabilità di essere favorevole. Venendo infine all'orientamento politico, si conferma che chi dichiara di votare per la sinistra e per il centro-sinistra tende ad essere meno favorevole all'utilizzo delle armi autonome rispetto a chi dichiara di votare per il centro-destra e la destra. In termini di variabilità spiegata, l'orientamento politico è la variabile che spiega maggiormente il grado di favore rispetto alle armi autonome, subito dopo la variabile età e infine la variabile di genere<sup>3</sup>.

Vediamo infine come si esprime rispetto all'utilizzo delle armi autonome chi si era già espresso nei confronti dell'utilizzo di quelle semi-autonome (droni).

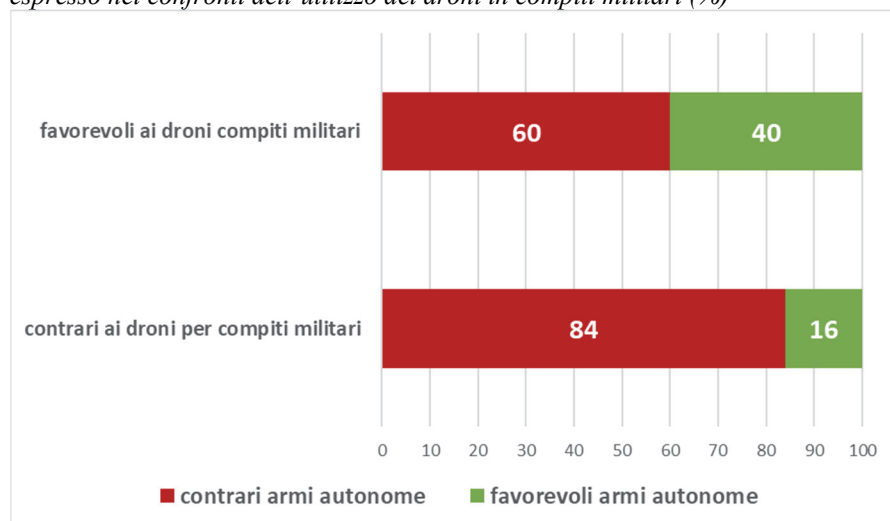
<sup>3</sup> Per verificare quale delle tre variabili indipendenti abbia un impatto maggiore su quella dipendente abbiamo sottoposto ciascuna di esse a un modello di regressione logistica univariata e poi considerato l' $R^2$  di Negelkerke.



Dalla figura 11 si evince che, presumibilmente, chi è contrario all'utilizzo dei droni in ambito militare è anche contrario all'utilizzo delle armi autonome (84%). Controintuitivamente, tuttavia, anche tra coloro che si sono dichiarati favorevoli all'utilizzo dei droni, la maggioranza è contraria all'utilizzo delle armi autonome (60%). Sottoposta al test del Chi quadrato tale relazione mostra di essere statisticamente significativa ( $p < 0,001$ ).

Dunque sostenere l'utilizzo dei droni per compiti militari non costituisce una condizione sufficiente per sostenere i LAWS, il cui impiego sui campi di battaglia incontra maggiori riserve di quelle suscitate dall'impiego dei droni.

*Fig. 11 – Armi autonome: favorevoli e contrari in relazione al grado di favore espresso nei confronti dell'utilizzo dei droni in compiti militari (%)*



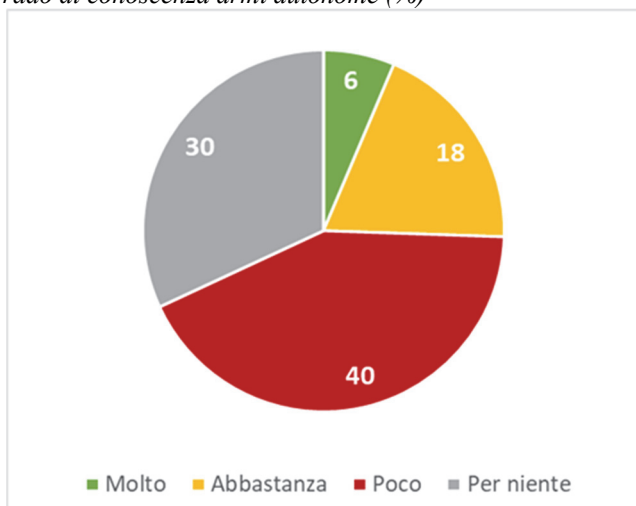
Fonte: Rilevazione Archivio Disarmo – Demetra 2019

### 7.3. Le giovani generazioni e le armi autonome

Allo scopo di individuare le modalità di conoscenza e le tematiche e le visioni correnti presso le nuove generazioni (in sostanza che cosa i giovanissimi conoscono e soprattutto a che cosa pensano quando si parla di armi autonome) abbiamo effettuato uno studio di caso su 106 studenti della scuola secondaria di II grado con età compresa tra gli 11 e 14 anni, 62 maschi e 44 femmine. L'indagine ha coinvolto 6 classi di due istituti comprensivi siti nel Municipio XI di Roma. La rilevazione, realizzata tra l'ottobre e il dicembre del 2019, si è servita di un questionario strutturato a risposta multipla.

Inizialmente è stato chiesto agli intervistati di dichiarare il proprio grado di conoscenza delle armi autonome. Similmente a quanto emerso da un'analoga indagine avente per oggetto i droni militari<sup>4</sup>, circa 3/4 dei rispondenti (70%) dichiara di aver sentito parlare “poco o per niente” delle armi autonome; mentre appena 1/4 ne ha sentito parlare o letto (18% “abbastanza”, 6% “molto”) (v. fig. 12).

Fig. 12 – Grado di conoscenza armi autonome (%)



Fonte: Archivio Disarmo, 2019

Dopo aver brevemente presentato le armi autonome come sistemi di armi che sarebbero in grado di selezionare autonomamente obiettivi e attaccarli senza l'intervento umano, abbiamo chiesto ai ragazzi intervistati quanto sarebbero stati d'accordo sull'impiego in guerra dei “sistemi letali di armi autonome”. Non discostandosi molto dal dato a livello nazionale, il 50% si dichiara per nulla o poco d'accordo, contro un 33% che asserisce di essere abbastanza o molto d'accordo. Non differenziandosi da quanto emerso rispetto al grado di conoscenza dei LAWS da parte degli intervistati, ben il 17% non sa fornire una risposta (v. fig. 13).

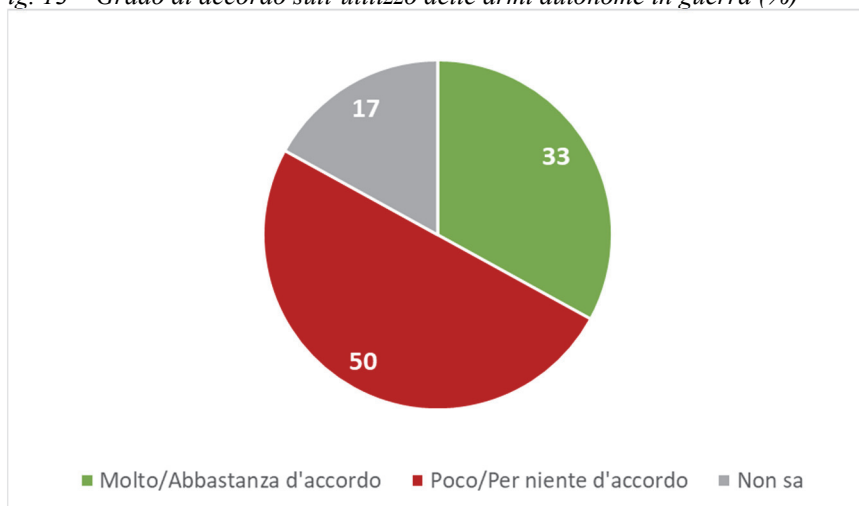
Successivamente è stato chiesto agli intervistati se, a loro parere, l'Italia dovrebbe impegnarsi per un divieto internazionale sui sistemi letali di armi autonome. Poco meno della metà dei rispondenti (49%) ritiene che sì, il nostro Paese dovrebbe impegnarsi maggiormente per una messa al bando delle

<sup>4</sup> Farruggia, F. (2018), Droni e opinione pubblica. L'analisi dei focus group, in *IRIAD Review*, n° 8, pp. 21-29

LAWS, una percentuale formata prevalentemente da coloro i quali si erano dichiarati oppositori rispetto all'utilizzo di tale sistema d'arma; il 17% non ritiene opportuno un particolare impegno da parte dell'Italia; mentre sale al 34% la percentuale di chi non sa esprimere una propria opinione (v. fig. 14).

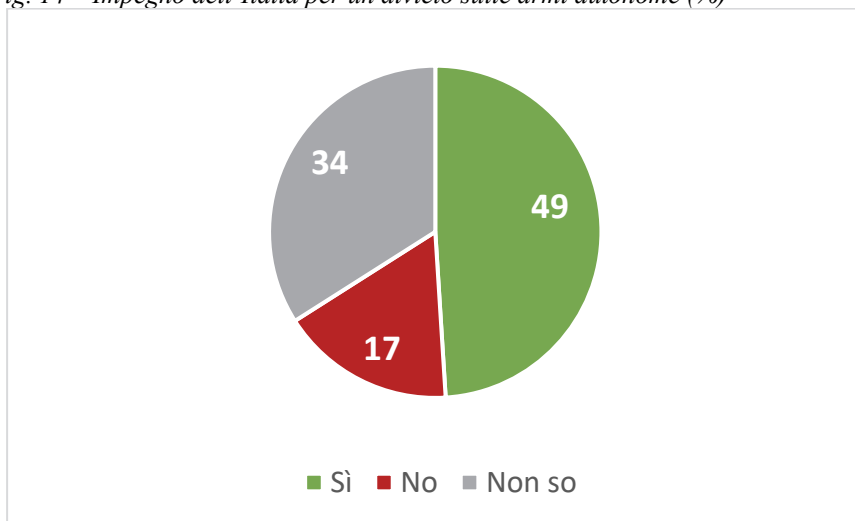
Infine, in riferimento a quanti si sono dichiarati contrari all'utilizzo in guerra delle armi autonome, accenniamo a quali sono le principali preoccupazioni legate a tale evenienza. La possibilità di malfunzionamenti tecnici risulta essere il principale timore dei giovani intervistati (35,8%), i quali si dimostrano meno preoccupati dal fatto che l'impiego di armi autonome può essere illegale (per il 25,5%) o troppo costoso (per il 22,6%). È interessante notare come la questione morale, risultata la prima preoccupazione a livello sia mondiale sia nazionale, non assuma altrettanta rilevanza per i giovanissimi. L'eventualità che una macchina possa decidere della vita o della morte di un essere umano sembra impensierire "solo" il 17,9% degli intervistati.

Fig. 13 – Grado di accordo sull'utilizzo delle armi autonome in guerra (%)



Fonte: Archivio Disarmo, 2019

Fig. 14 – Impegno dell'Italia per un divieto sulle armi autonome (%)



Fonte: Archivio Disarmo, 2019

#### 7.4. Osservazioni conclusive

Almeno in principio l'opzione armi autonome sembra avere pochi sostenitori tra i cittadini italiani. Ciò costituisce una condizione necessaria per l'assunzione di una posizione critica in materia da parte del nostro Paese. A sua volta essa potrà divenire sufficiente unicamente se crescerà da semplice espressione di una posizione sollecitata ed espressa individualmente a presa di coscienza diffusa circa una minaccia che incombe sullo scenario internazionale di qui al prossimo decennio. In tal caso l'opinione pubblica sarà in grado di esercitare una pressione sui media tradizionali e sui social, che a sua volta si trasmetterà a parlamento e governo. Questi organi, infine, potranno decidere di portare nelle istanze internazionali (quali i colloqui ONU per la *Convention on Certain Conventional Weapons*) un punto di vista proattivo e competente a nome dell'Italia.

Resterà da verificare se e in che modo a livello mondiale i governi prenderanno atto di questa opposizione pubblica allo sviluppo di sistemi d'arma che sfidano tanto il buon senso quanto il senso comune, sottraendo sia ai decisori (politici) sia agli esecutori (militari) l'esclusiva circa decisioni che chiamano in causa responsabilità tra le più gravi e complesse.

## **Riferimenti bibliografici**

Farruggia, F. (2018), “Droni e opinione pubblica. L’analisi dei focus group”, in *IRIAD Review*, n. 8, Istituto di Ricerche Internazionali Archivio Disarmo IRIAD.

## **Sitografia dei sondaggi**

<https://www.ipsos.com/sites/default/files/2017-03/AWS%207555.pdf>

[https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/human-rights-watch-autonomous-weapons-pr-01-22-2019\\_0.pdf](https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/human-rights-watch-autonomous-weapons-pr-01-22-2019_0.pdf)

[https://www.ipsos.com/sites/default/files/ct/news/documents/2021-01/ipsos\\_global\\_advisor\\_-\\_lethal\\_autonomous\\_weapons\\_survey\\_-\\_nov\\_2020-jan\\_2021.pdf](https://www.ipsos.com/sites/default/files/ct/news/documents/2021-01/ipsos_global_advisor_-_lethal_autonomous_weapons_survey_-_nov_2020-jan_2021.pdf)

## 8. *Il diritto internazionale umanitario e la sfida delle armi autonome all'intus-legere*

di Sofia Bertieri, Adriano Iaria

### 8.1. Introduzione

Dal punto di vista giuridico, l'impiego di sistemi d'arma autonomi non solleva necessariamente obiezioni: sono molteplici già oggi quelli utilizzati perlopiù con scopi difensivi. I LAWS – di contraerea e antimissilistici – hanno la caratteristica di essere difensivi, reagiscono a seguito di un'intrusione nello spazio aereo con una risposta immediata e limitata e con un alto grado di prevedibilità nell'esito della loro azione (Iaria, 2018). L'*Iron Dome* sviluppato da Israele, il *Goalkeeper Close-In Weapon System* dei Paesi Bassi o il *Nächstbereichschutz system* (NBS) MANTIS utilizzato dalla Germania sono esempi di sistemi di arma autonomi sviluppati con scopi difensivi e già impiegati che non sollevano alcun dubbio di natura etica o giuridica proprio per la loro caratteristica di essere difensivi e per la loro prevedibilità nel comportamento.

Per molti esperti il cambiamento chiave avvenuto negli ultimi anni – una sfida fondamentale nella prevedibilità del sistema – è l'ulteriore sviluppo della IA e in particolare degli algoritmi che incorporano l'apprendimento automatico. «L'etimologia della parola intelligenza si fa risalire all'avverbio latino *intus* (dentro) e al verbo latino *legere* (leggere), inteso come comprendere, raccogliere idee e informazioni riguardo a qualcuno o a qualcosa. Quindi, l'intelligenza è la facoltà di comprendere la realtà non in maniera superficiale ma, andando oltre, in profondità, per coglierne gli aspetti nascosti e non immediatamente evidenti» (Etimo Italiano). Nel campo della cibernetica, per il Dizionario Treccani la IA è “la riproduzione parziale dell'attività intellettuale propria dell'uomo – con particolare riguardo ai processi di apprendimento, di riconoscimento, di scelta – realizzata o attraverso l'elaborazione di modelli ideali, o, concretamente, con la messa a punto di macchine che utilizzano per lo più a tale fine elaboratori elettronici”. Il *comportamento* dell'algoritmo di apprendimento è determinato non solo dalla

programmazione iniziale (eseguita da un essere umano) ma anche dal processo in cui l'algoritmo stesso *impara* e si sviluppa per *esperienza*. Si individuano dunque due fasi: la prima è data dall'apprendimento tramite la formazione prima dell'utilizzo, mentre la seconda fase è data dall'apprendimento per esperienza, durante lo svolgimento di un'attività (ICRC, 2018).

Armi autonome che integrano la IA, permettendo alla macchina di poter imparare (DL) e quindi di modificare il proprio comportamento, potrebbero dunque non consentire a chi ne sceglie l'utilizzo di prevederne il comportamento e, in ultima istanza, di essere responsabile della condotta posta in essere.

## 8.2. Mezzi e metodi di combattimento

Nel corso degli anni la comunità internazionale ha limitato, o in certi casi vietato, alcuni mezzi e metodi di combattimento. Vi è ad esempio il divieto di ordinare che non vi siano sopravvissuti o il divieto alla perfidia, considerate norme di diritto consuetudinario. Allo stesso modo, per quanto riguarda i mezzi di combattimento, gli Stati hanno via via regolamentato e messo al bando l'utilizzo di certe armi. In alcuni casi con dei trattati *ad hoc* – Convenzione sulle armi biologiche (1972), Convenzione sulle armi chimiche (1993), Convenzione sulle mine antiuomo (1997), Convenzione sulle armi a grappolo (2006), Convenzione per la proibizione delle armi nucleari (2017) – in altri casi invece approvando dei protocolli addizionali, come i cinque protocolli alla Convenzione su certe armi convenzionali del 1980.

L'articolo 35 del Protocollo addizionale (I) alle Convenzioni di Ginevra stabilisce al primo paragrafo che: «In ogni conflitto armato, il diritto delle parti in conflitto di scegliere metodi e mezzi di guerra non è illimitato». Limitare la potenza distruttiva e le conseguenze delle armi utilizzate sono concetti che trovavano dei sostenitori già nel IV secolo a.C.

Già Sun Tzu (544 a.C. – 496 a.C.) nei suoi scritti sanciva come la possibile neutralizzazione del nemico non dovesse per forza coincidere con l'uccisione del nemico. Sant'Agostino (354-430) affermava che «se il nemico che combatte deve perire, che questo avvenga per necessità non per tua volontà [...] il vinto e il prigioniero hanno diritto alla compassione» (Messineo, 1971), o ancora Francisco de Vitoria (1496-1546), nel suo *De iure belli* scriveva che «non è mai lecito uccidere l'innocente in quanto tale e intenzionalmente, tuttavia incidentalmente, anche se consapevolmente, è lecito in certi casi uccidere innocenti. Si deve evitare che dalla guerra derivino mali superiori a quelli a cui la guerra pone rimedio» (de Vitoria, 1539). Ancora, il giurista Alberico Gentili (1552-1608) affermava che la necessità militare

può rendere legale qualunque cosa, ma l'abuso dei mezzi militari potrebbe indebolire la causa della giustizia e dare all'avversario ragione per muovere a sua volta una guerra giusta. Quindi, non violare le donne del nemico né provocare offese contro la giustizia naturale. Grozio nel 1625 nel suo *De iure belli ac pacis* sosteneva la necessità di imporre delle limitazioni al potere distruttivo delle armi utilizzate in quello che lui definiva come *temperamentum belli*. Un'ulteriore formulazione di tale principio si ha nell'articolo 22 del Regolamento dell'Aja del 1907 che stabilisce come il diritto dei belligeranti di adottare mezzi per ferire il nemico non sia illimitato.

E infine Rousseau nel *Contratto Sociale* del 1762, stabiliva come

la guerra è una relazione [...] tra Stato e Stato e gli uomini sono nemici solo accidentalmente [...] come soldati [...] Lo scopo della guerra essendo la distruzione dello Stato nemico, si ha il diritto di ucciderne i difensori finché sono armati, ma appena questi posano le armi e si arrendono, cessano di essere nemici o strumenti del nemico e ritornano ad essere semplicemente uomini, la cui vita nessuno ha il diritto di prendere (Rousseau, 1762).

Il già citato articolo 36 del Protocollo addizionale (I) pone un obbligo nei confronti degli Stati di verificare già durante lo sviluppo di nuovi mezzi e metodi di combattimento se questi siano contrari al diritto internazionale umanitario esistente. Come sottolineato nel commentario del 1987 ad opera del Comitato Internazionale della Croce Rossa, sulla base di questo articolo, le Alte Parti contraenti si impegnano a determinare la natura eventualmente illecita di una nuova arma, sia per quanto riguarda le disposizioni del Protocollo, sia per quanto riguarda qualsiasi altra norma applicabile del diritto internazionale. La determinazione deve essere effettuata sulla base del normale utilizzo dell'arma come previsto al momento della valutazione. Se queste misure non vengono prese, lo Stato sarà in ogni caso responsabile per eventuali danni illeciti che ne conseguono.

È sulla base di questo criterio che venne approvato il quarto protocollo addizionale alla CCW, relativo al divieto d'utilizzo dei laser accecanti, prima ancora che questi venissero impiegati. Il divieto di utilizzo di una nuova arma in anticipo rispetto al suo utilizzo venne definito dal Comitato Internazionale della Croce Rossa come «un passo storico per l'umanità. Per la prima volta dal 1868, quando l'uso di proiettili esplosivi fu bandito prima ancora del loro impiego, un'arma di interesse militare è stata bandita prima del suo uso sul campo di battaglia e prima che un flusso di vittime desse prova visibile dei suoi effetti tragici» (ICRC, 1995, p. 3).

L'obbligo imposto dall'articolo 36 del Protocollo addizionale (I) agli Stati contraenti si applica anche per i sistemi d'arma completamente autonomi. L'organizzazione non governativa *Article 36* si batte affinché i sistemi



d'arma autonomi implementino un «significativo controllo umano negli attacchi individuali»<sup>1</sup>. Questa nozione è stata ripresa da diversi esperti e sembra rappresentare il requisito sostanziale per far avanzare il dibattito intorno ai LAWS tenendo conto della necessità di prevedibilità dell'arma e di responsabilità della condotta per garantire la protezione dei civili, accertando l'eventuale violazione del diritto internazionale umanitario.

Il punto è dunque comprendere quali attività svolte autonomamente dai LAWS debbano essere oggetto della nostra attenzione e dove risulta centrale la prevedibilità della condotta. Un approccio interessante per analizzare il fenomeno è farlo attraverso il c.d. ciclo OODA (Osservare, Orientare, Decidere e Agire) ponendosi l'obiettivo di comprendere, in un'operazione militare, quale di queste quattro azioni possano essere delegate a sistemi autonomi. Nelle attività di osservazione, orientamento e decisione non si riscontrano profili direttamente correlati al diritto internazionale umanitario, ma per quel che riguarda l'azione risulta cruciale l'elemento della prevedibilità dell'esito tra la decisione e l'azione intrapresa. Se è ragionevolmente possibile prevedere la conformità al diritto internazionale umanitario, si può considerare efficace il controllo umano sull'attività, a prescindere dal livello e tipo di interazione con la macchina al momento dell'azione letale. Se, d'altra parte, non si potrà ragionevolmente prevedere se la macchina rispetterà il diritto internazionale umanitario, l'azione autonoma sarà da ritenersi potenzialmente illecita (Schuller, 2016).

Tale approccio spinge a considerare i sistemi d'arma autonomi, per quanto complessi, ancora come macchine piuttosto che agenti e ancor di più, come agenti legali. Diplomatici ed esperti sollevano dei dubbi sul fatto che i sistemi d'arma autonomi saranno in grado di applicare le norme del diritto internazionale umanitario. Tuttavia se continuiamo a considerare i LAWS come delle macchine, non possiamo che constatare come queste non applichino norme di diritto; possono svolgere funzioni e azioni conformi a quanto previsto dal diritto, ma così facendo non stanno applicando la legge. Il professore Marco Sassoli, nella sua presentazione alla riunione di esperti del CICR del 2014 sulle armi autonome, ha affermato, in modo condivisibile, che «solo gli esseri umani sono destinatari del diritto internazionale umanitario» (Moyes, 2016, pp. 46-52).

<sup>1</sup> La definizione utilizzata in inglese è «*Meaningful human control over individual attacks*».

### 8.3. La protezione dei civili

La protezione dei civili rappresenta uno dei due cardini su cui si impernia il diritto internazionale umanitario. Se da una parte infatti questa branca del diritto regola i mezzi e i metodi di combattimento tra le parti in conflitto, dall'altra si adopera affinché le persone che non ne prendono parte, o non ne prendono più parte, siano tutelate e non siano oggetto di violenza bellica.

Gli Stati assolvono l'obbligo di proteggere i civili attraverso il rispetto, *inter alia*, dei principi di distinzione, proporzionalità e precauzione nell'attacco. Tali principi sono considerati norme di diritto consuetudinario e il loro rispetto è obbligatorio per tutte le parti in conflitto.

Il principio di distinzione obbliga le parti a distinguere sempre tra civili e combattenti: gli attacchi possono essere diretti soltanto contro i combattenti e non contro i civili. Sebbene già la Dichiarazione di San Pietroburgo del 1868 stabilisca che l'unico obiettivo legittimo che gli Stati hanno durante un conflitto è quello di indebolire le forze armate nemiche, è il Regolamento dell'Aja del 1907 che, nel proibire l'attacco con qualsiasi mezzo a città, villaggi, abitazioni o edifici indifesi, formula una prima base nel riconoscere il principio di distinzione. Dall'obbligo di distinzione tra civili e combattenti, discende il divieto di attacchi indiscriminati.

La formulazione giuridica del principio di proporzionalità nell'attacco è contenuto nell'articolo 51 paragrafo 5 lettera b del I Protocollo addizionale alle Convenzioni di Ginevra del 1977. Gli Stati sono obbligati a scegliere mezzi e metodi di combattimento che nel perseguire un vantaggio militare concreto e diretto non risultino eccessivi in relazione ai danni collaterali provocati a beni civili o alle o alla popolazione civile. Il principio di proporzionalità nell'attacco, dunque, non consiste in un rapporto tra i mezzi utilizzati e i fini raggiunti, quanto piuttosto tra i mezzi utilizzati e il fine ultimo di non causare danni collaterali eccessivi rispetto al vantaggio militare diretto e concreto conseguito. Infine, il principio di precauzione nell'attacco impone agli Stati che nella condotta di operazioni militari si tenga sempre conto della popolazione civile e dei beni civili che potrebbero essere coinvolti durante l'operazione e di prendere tutte le precauzioni possibili per minimizzare il rischio che beni e popolazione civile possano rimanere coinvolti.

La tutela che gli Stati hanno riconosciuto alla popolazione civile, attraverso il rispetto di questi principi da parte degli Stati, impone che l'eventuale utilizzo di sistemi d'arma autonomi sia conforme ai principi di distinzione, proporzionalità e precauzione nell'attacco. Rimane tuttavia da sciogliere il nodo legato alla responsabilità della condotta.

Secondo il diritto esistente, uno Stato sarebbe responsabile per la condotta e le eventuali violazioni del diritto internazionale umanitario commes-

se da sistemi d'arma autonomi; infatti, l'utilizzo di questo tipo di armi ricade nella scelta e, in ultima istanza, nella responsabilità da parte dello Stato. Inoltre, gli Stati parte al Protocollo addizionale (I) alle Convenzioni di Ginevra del 1977, ai sensi dell'articolo 36, sono obbligati nello studio, sviluppo, acquisizione o adozione di nuove armi, a determinare se il loro impiego possa essere proibito dal diritto internazionale a essi applicabile.

La proporzionalità richiede una ponderazione contestuale di due fattori: la possibilità di uccidere o ferire civili e danneggiare beni civili, da un lato, e il potenziale vantaggio militare diretto e concreto dell'attacco, dall'altro. La determinazione del danno potenziale per i civili e i loro beni è determinabile con un certo livello di accuratezza, di conseguenza, i comandanti utilizzano già simulatori di danni collaterali per garantire che gli attacchi siano proporzionali rispettando, inoltre, il principio di precauzione (Schmitt, 2013). La questione se un sistema autonomo possa effettuare un'analisi di proporzionalità può essere ancora più gravosa di quella relativa alla capacità dei LAWS di rispettare il principio di distinzione. L'analisi di proporzionalità risulta particolarmente condizionata da fattori specifici e spesso in rapido mutamento per consentire di ridurla, ad esempio, a una regola secondo cui è possibile uccidere una vittima civile per ogni combattente; o due vittime civili per comandante di unità; o tre vittime civili per un carro armato distrutto. Inoltre, è fondamentale valutare se esistano mezzi e metodi di combattimento diversi in grado di ottenere il medesimo vantaggio militare ma limitando i danni a civili e beni civili. Poiché la valutazione della proporzionalità richiede un peso relativo da attribuire agli interessi concorrenti, questi sistemi d'arma dovrebbero essere in grado di anticipare l'effetto di tutte le potenziali decisioni e il numero risultante di vittime civili. Dovrebbero inoltre reagire alle mutevoli circostanze, essendo in grado di calcolare il vantaggio militare e determinare se il danno collaterale è accettabile.

Più complesso risulta invece il quadro dal punto di vista del diritto penale internazionale. Secondo lo Statuto della Corte Penale Internazionale (CPI), lanciare intenzionalmente un attacco, consapevoli che i danni a beni civili e ai civili siano eccessivi rispetto al vantaggio militare concreto e diretto conseguito, rappresenta un crimine di guerra perseguibile dalla Corte (art. 8 c. 2). L'elemento centrale nel perseguire una persona è rappresentato dal *mens rea* o elemento psicologico. Infatti, secondo quanto disposto dall'articolo 30 dello Statuto della CPI, una persona è penalmente responsabile solo se oltre l'elemento materiale – la condotta contraria allo Statuto – vi sia anche intenzione e consapevolezza. Se, almeno fino a oggi, risulta impensabile perseguire una macchina per una condotta criminale da essa presa autonomamente, è pur vero che la mancanza di un adeguato controllo e la potenziale imprevedibilità dei sistemi d'arma completamente autonomi rende difficile

perseguire gli individui responsabili della programmazione e del dispiegamento dell'arma. Infatti, la capacità di elaborazione e apprendimento della macchina potrebbe superare le previsioni stesse di coloro i quali hanno programmato e dispiegato tali armi non rendendoli di fatto responsabili della condotta a causa dell'imprevedibilità del comportamento del sistema d'arma (Iaria, 2018).

#### **8.4. Il ruolo dei consulenti giuridici e politici**

Gli Stati, ratificando le Convenzioni di Ginevra e i suoi Protocolli, si impegnano a rispettare e garantire il rispetto del diritto internazionale umanitario. La conoscenza del diritto applicabile durante le operazioni militari diventa dunque cruciale per rispettare e far rispettare gli obblighi esistenti. Nel rispetto di questi obblighi, l'articolo 82 del Protocollo addizionale (I) stabilisce che «le Alte Parti contraenti in ogni tempo e le Parti in conflitto in periodo di conflitto armato garantiranno che dei consiglieri giuridici siano disponibili, quando occorra, per consigliare i comandanti militari di livello appropriato circa l'applicazione delle Convenzioni e del presente Protocollo, e circa l'insegnamento appropriato da impartire in materia alle forze armate». In tempo di guerra il compito del consigliere giuridico è dunque quello di dare un parere sulle operazioni militari pianificate e in corso, verificare l'osservanza del diritto esistente nonché sulle implicazioni giuridiche legate alla condotta intrapresa dal comandante delle operazioni. In questo flusso di informazioni inviate e ricevute risultano fondamentali i canali di trasmissione delle informazioni e la capacità dell'agente di adeguare la propria condotta al mutare del contesto operativo analizzato dal consigliere giuridico e dall'ordine impartito dal comandante delle operazioni.

Nell'arco degli anni, accanto alla figura del consigliere giuridico, le Forze Armate hanno usufruito di consulenti specializzati in affari politici, culturali, religiosi e di genere. Tali figure, pur non espressamente previste dal punto di vista giuridico nelle condotte delle operazioni, risultano fondamentali. Per esempio, la figura del consulente politico è cruciale per il rispetto delle norme previste dal diritto internazionale umanitario. Nell'applicazione del principio di proporzionalità nell'attacco, per esempio, la valutazione relativa al vantaggio militare concreto e diretto è prerogativa del comandante in capo all'operazione supportato dai consulenti legali e politici incaricati di illustrare il piano giuridico nonché gli aspetti politici, economici e sociali che completano il quadro in cui l'azione militare viene svolta.

È chiaro dunque che il ruolo di queste due figure è fondamentale nella valutazione giuridica e politica che il comandante delle operazioni compie

e, conseguentemente, sugli ordini impartiti a tutti i livelli della catena di comando. Nel caso di sistemi d'arma autonomi, così come nel caso di esseri umani dispiegati in operazioni militari, vi è la necessità di garantire la responsabilità del comandante delle operazioni rispetto all'ordine dato. Se volessimo anche considerare i LAWS come agenti di diritto, ipotesi rigettata in precedenza, essi sarebbero posti alla fine di una catena di comando in cui il comandante delle operazioni è posto al vertice ed è coadiuvato nelle sue scelte dai consiglieri giuridici e politici. Pertanto, una diversa valutazione del contesto e del mutato quadro operativo deve essere prima valutata da chi è responsabile dell'operazione e, se ne fa richiesta, dai consiglieri giuridici e politici. L'analisi della catena di comando e le valutazioni sulla responsabilità dell'operazione che ne conseguono, sembrano ancora una volta propendere verso la necessità che i sistemi d'arma autonomi siano subordinati ad un significativo controllo da parte degli esseri umani (Iaria, 2018).

Nel 2021, il Ministero della Difesa francese ha istituito un Comitato etico che ha espresso un'articolata opinione sull'integrazione di sistemi autonomi a sistemi d'arma autonomi letali. Il Comitato ha evidenziato il timore da parte dei militari di perdere il controllo sul piano operativo, evidenziando la necessità, tra le altre cose, di una valutazione sistematica delle conseguenze delle azioni letali compiute da un sistema d'arma da parte del comando. In particolare, solo la catena di comando ha l'autorità di modificare gli obiettivi a missione in corso o di annullare la missione stessa. Inoltre, le linee guida proposte dal Comitato etico stabiliscono che il comando definisca un quadro di trasposizione della dottrina, ovvero gli obiettivi da raggiungere, i limiti di spazio e tempo, i vincoli e regole di ingaggio per ogni missione svolta da un sistema d'arma autonomo, che non dovrebbe mai avere la capacità di discostarsi dal quadro operativo senza l'intervento della catena di comando. Infine, in qualsiasi situazione operativa urgente, la catena di comando deve essere allertata e deve convalidare esplicitamente qualsiasi nuovo quadro operativo del sistema d'arma.

La centralità umana è stata ribadita anche dalle Forze Armate italiane, ed in particolare dell'Esercito, in una pubblicazione del 2019 relativa al *Future Operating Environment post 2035 – Implicazioni per lo strumento militare e terrestre*. Il documento, riconoscendo la centralità e la necessità di sfruttare le *disruptive technologies*, conferma quella percezione, da parte di chi gestisce il piano operativo, di mantenere il pieno controllo del quadro operativo: “Per quanto affiancata da sistemi intelligenti e autonomi, infatti, lo strumento militare del futuro attribuirà alla componente umana una funzione imprescindibile e assolutamente insostituibile nella gestione del campo di battaglia”.

## 8.5. L'umanità e la pubblica coscienza

La definizione della parola «umanità» rappresenta un esercizio piuttosto complesso. Dal punto di vista etimologico deriva dal latino *humanitas-atris*, derivato di *humanus*, «umano», nel significato di «genere umano» (Dizionario Treccani). Ancor più difficile è definire l'umanità su un piano giuridico, probabilmente perché le implicazioni di natura etica nel definire cosa rientri nel genere umano mutano al mutare del contesto storico, sociale e culturale. Forse più che di definizioni abbiamo bisogno di esempi per comprendere cosa possa significare applicare il principio di umanità in guerra (Iaria, 2018).

Così il giornalista e scrittore G. H. Perris descrisse la tregua di Natale del 1914 che interessò il fronte delle Fiandre dove si confrontavano soldati britannici e tedeschi durante la Prima guerra mondiale:

L'oscurità calò verso le 7 della Vigilia di Natale, e con essa una calma improvvisa. I cecchini tedeschi sembravano essere scomparsi. Poi il suono del canto dei caroselli salì dalle trincee; e, a quel punto, i cecchini britannici smisero di puntare i loro fucili contro il nemico. Il coro magico affondò nelle tenebre e nuovamente riprese verso il cielo nero. Alcuni soldati britannici abbozzarono un applauso. Urla dai tedeschi: 'Tu inglese, perché non vieni fuori?' – così scrisse un ufficiale della R.F.A. – e i nostri fieri fanti risposero, urlando, di 'Aspettare'. Alla fine uscirono; e, molto presto, fuochi e candele ardevano lungo i parapetti fino a quel momento vigilati incessantemente, mentre gli uomini fraternizzavano in mezzo a una folla, scambiandosi doni e concordando che la tregua durasse fino alla mezzanotte del giorno di Natale.

Tutto venne organizzato privatamente e avviato da uno dei nostri compagni. Difficile immaginarlo. L'unica cosa proibita era di apportare migliorie alle trincee.

Se per un qualsiasi inconveniente fosse stato sparato un solo colpo, non sarebbe stato preso come un atto di guerra, e le scuse sarebbero state accettate; inoltre, la ripresa delle ostilità non sarebbe avvenuta senza il dovuto preavviso da entrambe le parti (Perris, 1915, p. 391).

In quell'occasione i soldati decisero spontaneamente di stabilire delle tregue sul fronte durante il periodo natalizio.

Se la notte di Natale del 1914 su quel fronte fossero stati schierati sistemi d'arma autonomi non vi sarebbe stata alcuna tregua, sarebbe venuto meno quel principio di umanità tra militari che, condividendo una fede religiosa, decisero in modo spontaneo di sospendere momentaneamente le ostilità. D'altra parte l'umanità è costellata da esempi di umanità, dove l'utilizzo ripetuto della stessa parola non è un refuso quanto piuttosto un'occasione per evidenziare il legame indissolubile tra l'uomo e la sua natura umana (Iaria,

2018). Va inoltre aggiunto che le prime regole morali tra combattenti nascono da quel sentimento di cavalleria e di rispetto tra nemici a cui si concedeva l'onore delle armi riconoscendo nell'avversario un *justus hostis*, nell'accezione che ne dà il grande teorico giuridico Carl Schmitt. Questo approccio quasi romantico al tema non deve in alcun modo farci distogliere l'attenzione dai rischi di un'escalation di tensioni e violenza data proprio dalla capacità di reazione immediata di sistemi d'arma autonomi che sono in grado di *prendere* decisioni e agire con una capacità di risposta misurabile in millisecondi.

Nel diritto internazionale umanitario le nozioni di umanità e pubblica coscienza sono state introdotte da quella che è nota come Clausola Martens. Durante la conferenza diplomatica in cui si discusse il Regolamento dell'Aja del 1899, il diplomatico prussiano Martens, chiese che venisse introdotto nel preambolo un paragrafo secondo cui: «i civili e i combattenti rimangono sotto la protezione e l'imperio dei principi del diritto delle genti quali risultano dalle consuetudini stabilite, dai principi di umanità e dai dettami della pubblica coscienza». La Clausola Martens è considerata una norma di diritto consuetudinario ed è stata inclusa anche nel Protocollo addizionale (I) alle Convenzioni di Ginevra all'articolo 1.2 e nel preambolo del Protocollo addizionale relativo ai conflitti armati non internazionali. La *ratio* della clausola nasce dalla volontà di prevenire un'errata interpretazione secondo cui ciò che non è esplicitamente proibito dai trattati sia considerato lecito. La Clausola Martens va dunque vista con questo spirito, utilizzando il linguaggio della Corte Internazionale di Giustizia (CIG), come una rete di sicurezza per l'umanità (ICJ, *Legality of the threat or use of nuclear weapons, Advisory Opinion of 8 July 1996*). È parere di chi scrive che l'impossibilità di implementare il principio di umanità a sistemi d'arma completamente autonomi impedisca il rispetto della cornice giuridica esistente a queste tipologie di armi. Oltre alle questioni di natura giuridica, restano le preoccupazioni etiche e morali nel delegare la scelta di vita o di morte di esseri umani a sensori e *softwares*.

L'avanzare del diritto internazionale umanitario si è sempre caratterizzato dal ruolo svolto dalla società civile, dagli accademici, dai leader politici, dagli Stati e dal Comitato Internazionale di Croce Rossa nel definire la coscienza pubblica. È un lavoro instancabile che ha trovato riconoscimento nel preambolo di diverse convenzioni approvate grazie alla competenza, e spesso intransigenza, della società civile, affinché la coscienza pubblica prendesse la forma di obbligo internazionale. Nella recente approvazione del Trattato per la Proibizione delle Armi Nucleari, avvenuta nel 2017, l'ultimo paragrafo del preambolo sottolinea:

il ruolo della coscienza pubblica nell'avanzamento dei principi dell'umanità come dimostrato dalla richiesta di eliminazione totale delle armi nucleari e riconoscendo gli sforzi a tal fine intrapresi dalle Nazioni Unite, dal Movimento internazionale della Croce Rossa e dal Mezzaluna Rossa, da altre organizzazioni internazionali e regionali, da organizzazioni non governative, leader religiosi, parlamentari, accademici e dagli hibakusha.

Le obiezioni in merito ai LAWS, sollevate da diversi Stati e leader politici, da molte Ong a livello internazionale, da accademici, scienziati ed esperti, nonché da membri della società civile, lasciano intendere come anche l'attenzione verso lo sviluppo e l'utilizzo di sistemi d'arma completamente autonomi sia alta e starà proprio a questi attori definire la coscienza pubblica su un tema così controverso.

## **8.6. La posizione UE e italiana**

In ambito UE, solo il Parlamento Europeo si è espresso nettamente contro le armi autonome. Nella risoluzione del 27 febbraio 2014 dedicata ai droni, è stato inserito un punto relativo alle armi autonome, dove si chiede all'Alto Rappresentante dell'Unione per la politica estera e di sicurezza comune, agli Stati Membri e al Consiglio di "vietare lo sviluppo, la produzione e l'impiego di armi completamente autonome che consentono di sferrare attacchi senza alcun intervento umano".

In ambito UE è tuttavia il Consiglio, operante nel quadro della politica estera e di sicurezza comune, ad essere competente ad esprimere la posizione dell'Unione in relazione al dibattito internazionale per lo sviluppo di una normativa inerente i LAWS.

Alla vigilia della quinta conferenza di riesame della Convenzione sulle CCW tenutasi nel dicembre 2016, il Consiglio dei ministri degli Affari esteri ha apprezzato il lavoro del gruppo di esperti governativi in materia dei LAWS, evidenziando come allo sviluppo dei sistemi di armi autonome si debba applicare il corpus di norme e principi del diritto internazionale umanitario e le altre regole rilevanti del diritto internazionale. Preme comunque sottolineare come il Consiglio, a differenza del Parlamento, non si sia espresso a favore di un divieto assoluto, quanto per una regolamentazione delle armi autonome (Ronzitti, 2018), consolidando e irrobustendo le norme di diritto umanitario già applicabili attraverso la definizione di principi operativi e linee guida di dettaglio.

L'ex Alto Rappresentante dell'UE Federica Mogherini, nel discorso al Parlamento Europeo dell'11 settembre 2018, ha conseguentemente messo in rilievo che



Il diritto internazionale, compreso il diritto internazionale umanitario e il diritto dei diritti umani, si applica a tutti i sistemi di armi; gli esseri umani devono prendere decisioni in merito all'uso della forza letale, esercitare il controllo sui sistemi di armi letali che usano e rimanere responsabili delle decisioni sulla vita e sulla morte; la Convenzione delle Nazioni Unite su alcune armi convenzionali è il quadro adeguato per discutere di regolamentare questo tipo di armi; e, dato il duplice uso delle tecnologie emergenti, le misure politiche non dovrebbero ostacolare la ricerca civile, compresa l'intelligenza artificiale (EEAS, 2018).

Nel quadro dei lavori del gruppo di esperti governativi della CCW, l'Italia ha contribuito al dibattito normativo, negoziando con gli altri partner europei i contenuti degli interventi UE ed intervenendo a titolo nazionale. Ad esempio, nell'aprile del 2018, il rappresentante permanente italiano alla Conferenza sul Disarmo, Amb. Gianfranco Incarnato, ha ribadito che il corpus normativo esistente di diritto internazionale umanitario si applica pienamente a tutti i sistemi d'arma, inclusi quelli relativi ai potenziali LAWS ed ha pertanto messo in rilievo la necessità di un controllo umano rilevante su sistemi d'arma letali, anche ai fini della responsabilità in caso di violazioni. In linea con la posizione europea, l'Italia ha enfatizzato la rilevanza di una piena applicazione dell'art. 36 del Protocollo addizionale alle Convenzioni di Ginevra del 1949. Come già descritto, l'art. 36 impegna gli Stati ad una verifica *ex ante* dei sistemi d'arma nella fase iniziale del *procurement*, potendosi *ab origine* verificare la compatibilità con il diritto internazionale umanitario di un sistema d'arma in progettazione. In Italia, la verifica che ogni sistema d'arma nella fase di studio, sviluppo, acquisizione o adozione rispetti il diritto internazionale umanitario è contemplata dal Codice dell'Ordinamento Militare del 2010. Allo stadio attuale il processo di verifica si declina principalmente in un controllo di carattere parlamentare, condotto dal Ministero della Difesa in cooperazione con le Commissioni Difesa della Camera e del Senato, che hanno il compito di vagliare e deliberare qualsiasi spesa relativa allo studio, sviluppo, acquisizione e adozione di nuovi sistemi d'arma. In sede di CCW si è pertanto potuto positivamente mettere in luce come in Italia vi sia già un robusto meccanismo di controllo parlamentare sulla fase di *procurement* dei sistemi d'arma. Tale meccanismo potrebbe tuttavia essere ulteriormente rafforzato sulla base delle raccomandazioni e migliori pratiche che emergeranno dai lavori del gruppo di esperti governativi della Convenzione in tema di concreta attuazione dell'art. 36.

Inoltre, nel dibattito sulla caratterizzazione dei LAWS, l'Italia ha ribadito come il lavoro del GGE dovesse focalizzarsi su quei sistemi d'arma letali pienamente autonomi, ribadendo che tali sistemi ancora non esistono, ma che potranno essere sviluppati in futuro ponendo un problema di compa-

tibilità con le regole del diritto internazionale umanitario (GGE, Characterization of LAWS, 2018).

In un recente intervento alla Giornata di studio su *Intelligenza artificiale, sicurezza, responsabilità, etica*, promossa dal Segretariato generale della Difesa e Direzione nazionale degli armamenti in collaborazione con il Pontificio consiglio della Cultura della Santa Sede, il Ministro della Difesa Guerini, parlando della IA, ha affermato che è di vitale importanza «definire in modo chiaro e condiviso i limiti e le condizioni di autonomia di tali macchine». Il Ministro ha affermato che «sappiamo benissimo che sistemi di armamento autonomi già esistono [...], ma è evidente che in campo militare esistono significative implicazioni etiche e legali», pertanto esiste la concreta necessità di «individuare un adeguato sistema giuridico entro il quale poter collocare la robotica autonoma» (Analisi Difesa, 2019), in accordo con quanto già sancito dalla Commissione Giuridica del Parlamento Europeo.

Nel corso del meeting del Gruppo di Esperti Governativi sui LAWS, tenutosi tra il 20 e il 21 agosto 2019, dopo una lunga fase di negoziazione, si è finalmente trovato il consenso su un rapporto finale, che include la definizione di 11 principi guida nel campo dello sviluppo delle LAWS condivisi da tutti gli Stati partecipanti. Tali principi stabiliscono che:

- a) il diritto internazionale umanitario continua ad applicarsi pienamente a tutti i sistemi di armamento, compreso il potenziale sviluppo e utilizzo di sistemi letali di armi autonome.
- b) La responsabilità umana per le decisioni sull'uso dei sistemi d'arma deve essere mantenuta e che la responsabilità non può essere trasferita alle macchine. Questo dovrebbe essere considerato durante l'intero ciclo di vita dei sistemi d'armi.
- c) L'interazione uomo-macchina, che può assumere varie forme ed essere implementata in varie fasi del ciclo di vita di un'arma, dovrebbe garantire che il potenziale utilizzo di sistemi d'arma basati su tecnologie in grado di produrre sistemi di armi autonome letali siano conformi alle norme internazionali applicabili, e in particolare al diritto internazionale umanitario. Nel determinare la qualità e l'estensione dell'interazione uomo-macchina, una serie di fattori dovrebbe essere considerata includendo il contesto operativo e le caratteristiche e le capacità delle armi nel loro complesso.
- d) La responsabilità per lo sviluppo, il dispiegamento e l'utilizzo di qualsiasi sistema di armi emergenti nel quadro della CCW deve essere garantito in conformità al diritto internazionale applicabile, anche attraverso l'utilizzo di tali sistemi all'interno di una catena responsabile di comando e controlli umani.
- e) In conformità con gli obblighi degli Stati e in base al diritto internazio-

nale, nello studio, nello sviluppo, acquisizione o adozione di una nuova arma, mezzi o metodi di combattimento, è necessario stabilire se il suo impiego, in alcune o in tutte le circostanze, sia vietata dal diritto internazionale.

- f) Quando si sviluppano o acquisiscono nuovi sistemi di armi basati su tecnologie emergenti nell'area dei LAWS, dovrebbero essere considerati dei sistemi di sicurezza fisica, adeguate garanzie non fisiche (compresa la sicurezza informatica contro l'*hacking* o lo *spoofing* dei dati), il rischio di acquisizione da parte di gruppi terroristici e il rischio di proliferazione di tali sistemi.
- g) Le valutazioni dei rischi e le misure di mitigazione dovrebbero far parte della progettazione, dello sviluppo, delle prove e ciclo di spiegamento delle tecnologie emergenti in tutti i sistemi d'arma.
- h) Dovrebbe essere preso in considerazione l'uso di tecnologie emergenti nell'area dei LAWS nel rispetto e in conformità del diritto internazionale umanitario e delle altre leggi internazionali applicabili.
- i) Nell'elaborare potenziali misure politiche, tecnologie emergenti nell'area dei LAWS, queste non dovrebbero essere antropomorfizzate.
- j) Le discussioni e le eventuali misure politiche prese nel contesto della CCW non dovrebbero ostacolare il progresso o l'accesso a usi pacifici di tecnologie autonome intelligenti.
- k) La CCW offre un quadro adeguato ad affrontare il problema delle tecnologie emergenti nel quadro dei LAWS nel rispetto degli obiettivi e delle finalità del Convenzione, che cerca di trovare un equilibrio tra necessità militare e considerazioni umanitarie.

È interessante rilevare come lungo tutto il corso dei lavori del Gruppo di Esperti Governativi della CCW, i partner europei e l'Italia abbiano lavorato intensamente per promuovere un approccio costruttivo e condiviso nell'analisi delle implicazioni di diritto umanitario poste dai LAWS, portando avanti una linea di pensiero incentrata sullo sviluppo di strumenti normativi non legalmente vincolanti, come la definizione dei sopramenzionati principi guida. Tale approccio, frutto di un proficuo dialogo avviato da alcuni Stati dell'Unione Europea e su cui poi si è allineata l'intera Unione, risulta particolarmente interessante e a tratti innovativo nel contesto della CCW. Infatti, la scelta di principi guida non giuridicamente vincolanti, ma comunque efficaci per costruire un iniziale *consensus* intorno a un tema così delicato e ricco di sviluppi tecnologici nel breve periodo sul crinale civile-militare (*dual use*), offre un indubbio beneficio nel muoversi con gradualità laddove le attuali condizioni politiche rischiano di far arenare ogni processo normativo.

D'altra parte, il diritto internazionale umanitario, a oltre settanta anni dalla firma delle Convenzioni di Ginevra, vede oggi una certa resistenza da

parte di alcuni Stati nel giungere a nuovi strumenti giuridicamente vincolanti o comunque rafforzare e implementare le misure già esistenti. Ne è un esempio l'impossibilità di trovare un *consensus* tra gli Stati per trasmettere un report sul rafforzamento del rispetto del diritto internazionale umanitario alla 33<sup>a</sup> Conferenza Internazionale di Croce Rossa e Mezzaluna Rossa dopo il meeting del 3-5 dicembre 2018. Per questo, la scelta di procedere attraverso dichiarazioni politiche sta mostrando tutta la sua efficacia.

Nel contesto del GGE sui LAWS, la linea di pensiero adottata dall'Unione Europea ha portato dunque ad un risultato più che lusinghiero con la definizione degli undici principi guida che offrono un primo quadro (*framework*) condiviso su cui lavorare e confermano la centralità della CCW nel processo normativo inerente i LAWS.

Originariamente promossi da un *Food for Thought Paper* presentato da Belgio, Irlanda e Lussemburgo, i principi guida andrebbero ulteriormente posti in rilievo attraverso una dichiarazione politica ampiamente condivisa da adottare ad esempio in occasione della prossima Conferenza degli Stati parte, come auspicato da molti partner dell'Unione Europea e dall'Italia.

Altri Stati invece auspicano che dai principi guida si possa aprire fin da subito un percorso per giungere a *framework* giuridicamente vincolanti.

L'Italia ha fornito i suoi commenti a questi 11 principi nell'agosto del 2020 ribadendo che lo sviluppo, l'impiego e l'utilizzo di qualsiasi sistema d'arma, incluso i LAWS, debbano rispettare le norme e i principi del diritto internazionale umanitario. Ha inoltre sottolineato l'obbligo di effettuare controlli legali su armi, mezzi e metodi di guerra, ai sensi dell'art. 36 del I Protocollo aggiuntivo alle Convenzioni di Ginevra e ha riaffermato la necessità che la decisione di usare la forza letale rimanga nelle mani degli esseri umani. Su quest'ultimo punto ha ribadito che

gli operatori umani devono essere responsabili della validazione della selezione degli obiettivi (*targeting* e, in alcuni casi, *re-targeting*) e/o dell'attivazione/disattivazione della modalità autonoma del relativo sistema. A tale scopo, è essenziale che, ai fini dell'operationalizzazione degli undici principi guida a livello nazionale, le Alte Parti contraenti forniscano ai LAWS una serie specifica di limiti di tempo, spazio e obiettivi determinati, rendendo così più significativo il controllo umano.

## 8.7. Osservazioni conclusive

Il CEO di Apple, Tim Cook, durante la cerimonia in onore dei laureati nel 2017 del MIT di Boston, ha ben spiegato il ruolo della tecnologia di fronte alle sfide poste dalla IA:

La tecnologia può fare grandi cose. Ma non vuole fare grandi cose. Non vuole fare niente. Questo ruolo spetta a noi. Spetta ai nostri valori e al nostro impegno verso i nostri familiari, ai nostri amici, le nostre comunità, spetta al nostro amore per la bellezza e alla convinzione che le nostre vite sono interconnesse, al nostro senso civico e alla nostra gentilezza. Non sono preoccupato della IA che dà ai computer la capacità di pensare come gli umani. Sono più preoccupato per le persone che pensano come computer senza valori o compassione, senza preoccuparsi delle conseguenze. Questo è ciò di cui abbiamo bisogno per proteggerci. Perché se la scienza è una ricerca nell'oscurità, allora le scienze umane sono una candela che ci mostra dove siamo stati e il pericolo che ci aspetta.

Lo sviluppo di nuove tecnologie apre spesso dibattiti di natura etica e giuridica sulle implicazioni delle stesse. IA, *deep learning* e algoritmi complessi sono temi che fino ad oggi hanno visto coinvolti i colossi della tecnologia – Google, Facebook, Apple – pionieri in questo settore. Non si è tenuto conto di cosa significhi applicare queste tecnologie al campo militare e si è sottovalutato, in ultima istanza, il rischio concreto di delegare alla “coscienza” di una macchina il diritto di una persona di vivere o morire. Sarà dunque necessaria una maggior sinergia tra aziende dell'industria tecnologica, Stati e aziende militari per valutare attentamente sia le opportunità che i rischi insiti nello sviluppare sistemi di IA sempre più complessi.

Se è vero che il progresso della scienza è inevitabile, è pur vero che applicare i progressi scientifici al campo militare non è inevitabile, piuttosto è una scelta. E allora questa scelta non può non tenere conto delle esigenze di umanità dei conflitti armati e del progredire del diritto internazionale, che ha previsto la repressione dei crimini internazionali attraverso la Corte Penale Internazionale. La responsabilità nella condotta militare rappresenta un punto centrale al fine di rispettare e garantire il rispetto del diritto dei conflitti armati. Questo principio non può essere oggetto di ripensamenti a causa di sistemi d'arma che, per il loro elevato livello di autonomia e quindi di imprevedibilità, non permetterebbero di accertare l'eventuale responsabilità penale della condotta. Il fattore psicologico, il *mens rea*, non può che essere un elemento tipico dell'essere umano ed è dunque giusto relegare i LAWS all'alveo delle macchine piuttosto che degli agenti, condividendo quanto sostenuto da Marco Sassoli che solo gli esseri umani sono destinatari del diritto internazionale umanitario (Iaria, 2018).

## Riferimenti bibliografici

Analisi Difesa (2019), “Guerini: perplessità sull'utilizzo spinto dell'intelligenza artificiale”, *Analisi Difesa*, 25 settembre.

- CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems Geneva (2018a), *Statement by Ambassador Gianfranco Incarnato, Permanent Representative of Italy to the Conference on Disarmament, Characterization of LAWS*.
- CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems Geneva (2018b), *Statement by Ambassador Gianfranco Incarnato, Permanent Representative of Italy to the Conference on Disarmament, General exchange of views*.
- De Vitoria F. (2005), *De jure belli*, tr. it. Laterza, Roma [1539].
- European External Action Service (2018), *Speech by High Representative/Vice-President Federica Mogherini at the plenary session of the European Parliament on Autonomous Weapons Systems*, Strasbourg, 11 September.
- Gentili A. (2008), *Il diritto di guerra (De jure belli libri cap. VI del libro I, 1598)*. Giuffrè, Roma.
- Grotius H. (2011), *De jure belli ac pacis*, trad. it. Nabu Press, Firenze [1625].
- Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2019), *Draft Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (Annex 4)*. 21 August, 2019.
- Iaria A. (2018), “Da autonomi a completamente autonomi: l’applicazione dell’intelligenza artificiale nei sistemi d’arma autonomi (LAWS)”, *Rassegna della Giustizia Militare*, 6: 24-32.
- ICJ (1996), *Legality of the threat or use of nuclear weapons*, Advisory Opinion of 8 July.
- ICRC (1987), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff Publishers.
- ICRC (1995), *Vienna Diplomatic Conference Achieves New Prohibition on Blinding Laser Weapons and Deadlock on Landmines*.
- ICRC (2018), *Ethics and autonomous weapon systems: An ethical basis for human control?*
- Messineo A. (1971), “Il diritto umanitario”, *La civiltà cattolica*, 2896: 319-331.
- Ministère Des Armées, Defence Ethics Committee (2021), *Opinion on the Integration of Autonomy into Lethal Weapons Systems*.
- Moyes R. (2016), “Meaningful human control over individual attacks”. in ICRC, *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, Versoix, Switzerland: 46-52.
- ONU (2019), *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems Geneva, 25–29 March 2019 and 20-21 August 2019 Agenda Item 5, Focus of work of the Group of Governmental Experts in 2019, *Food for Thought Paper submitted by Belgium, Ireland and Luxembourg*.

- Perris G.H. (1915), *The campaign of 1914 in France and Belgium*. Henry Holt and Company.
- Repubblica Italiana (2020), *National commentaries on the 11 guiding principles – Comments by Italy*.
- Ronzitti N. (2018), “Uso e sviluppo delle armi autonome. Prospettive per un controllo alivello internazionale”, *Studi per il Parlamento*, Camera, Roma: 12.
- Rousseau J.J. (1762), *Il contratto sociale*, tr. it. Istituto Editoriale Moderno, Milano: 19.
- Schmitt M. (2013), *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, Harvard National Security Journal Feature.
- Schuller A. (2016), “Focusing the debate on autonomous weapon systems: A new approach to linking technology and IHL”, in ICRC, *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, Switzerland: Versoix.
- Stato Maggiore dell’Esercito (2019), *Future operating environment post 2035 – Implicazioni per lo strumento militare terrestre*.
- Tzu S. (2013). *L’arte della guerra*, tr. it. Feltrinelli, Milano (ed. or. VI sec. a.C).

## 9. *Il dibattito internazionale sulle armi autonome*

di *Guglielmo Tamburrini*

Questo capitolo riassume alcune delle principali iniziative che la comunità scientifica ha intrapreso per la regolamentazione delle armi autonome ed evidenzia i punti salienti del dibattito, in ambito politico e diplomatico, sul controllo umano significativo da esercitare su tutti i sistemi d'arma. Illustra inoltre una proposta di regolamentazione delle armi autonome che è insieme prudentiale e differenziata, poiché tiene conto della diversità tra armi autonome e tra contesti bellici nei quali esse possono essere dispiegate.

### **9.1. La comunità scientifica e l'etica delle armi autonome**

La comunità dei ricercatori della IA e della robotica ha contribuito con numerose iniziative a sensibilizzare il mondo politico e l'opinione pubblica intorno ai problemi etici posti dallo sviluppo delle armi autonome (vedi capp. 1, 3 e 5). Ricordiamo qui alcune iniziative tra le più salienti.

Vari membri della comunità dei ricercatori nel settore della robotica, in particolare Ronald C. Arkin e Noel Sharkey, sono stati protagonisti nel primo decennio di questo secolo delle prime discussioni sull'accettabilità etica e giuridica delle armi autonome. Arkin sottolineò le possibili implicazioni positive derivanti dall'impiego di armi autonome sui campi di battaglia (si veda cap. 5, par. 5.4), partendo dalla constatazione che gli esseri umani hanno ripetutamente violato lo *jus in bello* e i principi di distinzione e di proporzionalità del DIU. Secondo Arkin questo stato di cose dipende largamente da fattori che sono ininfluenti per il comportamento di una macchina ma che pesano notevolmente sulla condotta dei combattenti sul campo di battaglia, come il desiderio di autoconservazione e le reazioni emotive incontrollabili. La sua ricerca sulle applicazioni militari della robotica è stata ispirata dall'obiettivo di arrivare a progettare armi autonome che siano capaci di rispettare il DIU meglio dei normali soldati. Questa visione, con le soggiacenti



motivazioni etiche, fu presentata da Arkin al *First International Symposium on Roboethics*, organizzato nel 2004 da Gianmarco Veruggio e Fiorella Operto, della Scuola di Robotica di Genova, presso la Villa Alfred Nobel di Sanremo. Lo stesso Arkin descrisse più tardi questo simposio come «un evento spartiacque per la roboetica» (Arkin, 2009, pp. 29-30).

In contrasto con la posizione di Arkin, Sharkey mise subito in luce aspetti moralmente e giuridicamente problematici dell'autonomia dei sistemi d'arma. Come è stato già ricordato nel capitolo 5 (paragrafi 5.3 e 5.4), egli sottolineò che gli sviluppi prevedibili della robotica e della IA non consentono di sottoscrivere l'idea che armi autonome con prestazioni migliori degli esseri umani nel rispetto delle norme del DIU siano a portata di mano. Inoltre, dalla prospettiva dell'etica delle conseguenze, egli mise in evidenza la difficoltà di prevedere gli esiti di interazioni veloci tra sistemi d'arma autonomi con la conseguente difficoltà di controllarne il comportamento e gli incentivi che le armi autonome offrono all'avvio di nuovi conflitti (Sharkey 2007, 2008, 2012).

Sharkey fondò nel 2009, insieme a un piccolo gruppo di altri ricercatori, l'International Committee for Robot Arms Control (ICRAC). Nel 2012, quasi trecento ricercatori in informatica e robotica, provenienti da 37 paesi, sottoscrissero un appello pubblico con la richiesta di proibire le armi autonome (<https://www.icrac.net/the-scientists-call/>). L'appello, promosso dall'ICRAC e pubblicato sul suo sito, pone l'accento sulle questioni di responsabilità morale e giuridica sollevate dalle armi autonome. Tale documento sottolinea il vuoto di responsabilità che potrebbe emergere allorché si sposta dall'essere umano alla macchina la decisione di impiegare la forza in un'azione bellica. In quest'ottica non vi sarebbe più un *qualcuno* al quale chiedere conto di eventuali esiti illegali o moralmente inaccettabili di una tale decisione automatica, poiché essa è stata operativamente presa da un *qualcosa* che non ha i titoli per essere biasimato, punito o in ogni caso considerato responsabile dell'accaduto. In altri termini, l'appello degli scienziati fonda la richiesta di proibire le armi autonome principalmente sull'obbligo morale di collegare ogni atto di forza compiuto nel corso di un conflitto bellico alle decisioni di uno o più esseri umani e alla loro assunzione di responsabilità.

Sharkey giocò un ruolo di primo piano anche nelle iniziative che portarono a lanciare il 23 aprile del 2013 la *Campaign to Stop Killer Robots* (SKR). La campagna, promossa da un nutrito gruppo di organizzazioni non governative, nacque con l'obiettivo principale di promuovere l'adozione di un trattato internazionale per proibire lo sviluppo, la produzione, il possesso e l'uso delle armi autonome (<https://www.stopkillerrobots.org/>). Tra i promotori della campagna SKR figurano associazioni e gruppi di ricercatori che operano in vari settori scientifici, come *Pugwash Conferences on Science &*

*World Affairs*, organizzazione insignita del Premio Nobel per la pace nel 1995 e il già ricordato ICRAC. In Italia hanno successivamente aderito alla campagna SKR anche Archivio Disarmo, la Rete Italiana Pace e Disarmo e l'Unione degli Scienziati per il Disarmo (USPID).

Nel 2015, all'avvio dei lavori del principale congresso mondiale nel settore della IA (l'IJCAI – *International Joint Conference on Artificial Intelligence*) fu presentata una lettera aperta per la messa al bando delle armi autonome. Migliaia di ricercatori della IA e della robotica firmarono questa lettera aperta (<http://futureoflife.org/open-letter-autonomous-weapons/>), chiedendo di proibire definitivamente lo sviluppo, la produzione, la vendita e l'uso delle armi autonome.

La lettera esorta i ricercatori della IA e della robotica a seguire le orme delle comunità dei biologi e dei chimici, i quali contribuirono attivamente alle iniziative che sfociarono nella messa al bando delle armi biologiche e chimiche; e a seguire inoltre le orme della comunità dei fisici, i quali furono determinanti nell'organizzazione di iniziative che sfociarono nella messa al bando dei laser accecanti. La lettera aperta si concentra sugli effetti negativi che lo sviluppo e l'uso delle armi autonome potrebbero avere per la sicurezza dei popoli, la pace e la stabilità internazionale:

Una questione centrale che l'umanità deve affrontare oggi riguarda l'avvio oppure la prevenzione di una corsa globale alle armi dell'IA. Se una delle maggiori potenze militari imbroccherà la strada dello sviluppo delle armi autonome, una nuova corsa globale alle armi sarà praticamente inevitabile. E il punto di arrivo di una tale traiettoria tecnologica è del tutto evidente: le armi autonome diventeranno i kalashnikov del domani. A differenza delle armi nucleari, le armi autonome non richiedono materie prime costose o difficili da acquisire; si diffonderanno ovunque; saranno prodotte in grandi quantità e a costi molto bassi; faranno la loro comparsa sul mercato nero delle armi, nelle mani dei terroristi, nelle mani di dittatori interessati al controllo della popolazione e di signori della guerra intenti a progettare operazioni di pulizia etnica. Le armi autonome sono uno strumento ideale per compiere esecuzioni politiche mirate, per destabilizzare nazioni intere, soggiogare popolazioni e sterminare selettivamente un gruppo etnico.

Le ragioni morali per la messa al bando delle armi autonome presentate nel testo della lettera sono principalmente riconducibili all'etica delle conseguenze. Appelli dello stesso tenore sono stati in seguito sottoscritti da imprenditori operanti nei settori dell'informatica, della robotica e dell'Intelligenza Artificiale (95<https://futureoflife.org/2017/08/20/killer-robots-worlds-top-ai-robotics-companies-urge-united-nations-ban-lethal-autonomous-weapons/>), da gruppi di loro dipendenti, da ricercatori di altri settori scientifici e tecnologici.

## 9.2. Le armi autonome alla *Convention on Certain Conventional Weapons*

Stimolato dalle iniziative di ampi settori della società civile, il confronto diplomatico e politico sulle armi autonome ebbe inizio soprattutto grazie alla pubblicazione, nel 2013, quasi in contemporanea con il lancio della campagna SKR, di un rapporto a firma di Christof Heyns per lo *Human Rights Council* delle Nazioni Unite (Heyns, 2013). Heyns, che ricopriva allora il ruolo di Relatore speciale delle Nazioni Unite per le esecuzioni extragiudiziali, sommarie o arbitrarie, sollecitò una moratoria sulle armi autonome e la costituzione di un organismo internazionale per discutere di una loro regolamentazione. Nel settembre dello stesso anno la Francia, in collaborazione con l'*Office for Disarmament Affairs* delle Nazioni Unite, organizzò un seminario sulle armi autonome al *Palais des Nations* di Ginevra. In tale occasione avanzò la proposta di esaminare le questioni evidenziate nel rapporto di Heyns nel quadro istituzionale fornito dalla “Convenzione delle Nazioni Unite sulla proibizione o la limitazione dell’uso di alcune armi convenzionali che possono essere considerate eccessivamente dannose o aventi effetti indiscriminati” del 1980 (più sinteticamente Convenzione sulle armi convenzionali o CCW, abbreviazione di *Convention on Certain Conventional Weapons*). La proposta fu approvata poche settimane dopo dal CCW, dando avvio a una serie di incontri informali di esperti sulle armi autonome, che si tennero in seno al CCW, presso la sede ginevrina delle Nazioni Unite e con cadenza annuale dal 2014 al 2016.

Le discussioni del CCW dedicate alle armi autonome hanno inizialmente avuto scopi conoscitivi riguardo alle tecnologie robotiche e di IA che abilitano l’autonomia dei sistemi d’arma, nonché di approfondimento delle relative questioni etiche e giuridiche (Amoroso, 2021, pp. 11-15). Nel 2017 è stato costituito un *Group of Governmental Experts* (GGE) in seno al CCW, con il mandato di vagliare la compatibilità delle armi autonome con le norme del DIU, e di avanzare su questa base delle raccomandazioni da sottoporre alla valutazione e alle decisioni degli Stati membri del CCW. Nello stesso anno la Camera dei deputati impegnò il Governo italiano “a continuare a partecipare attivamente al dibattito internazionale in corso in particolare nell’ambito della Convenzione sulle armi convenzionali, di concerto con i principali *partner* dell’Italia [...] con l’obiettivo di arrivare a una [...] regolamentazione internazionale dei sistemi d’arma di tipo *Lethal Autonomous Weapons System* (Laws) [...]” (mozione 1-01776 approvata nella seduta del 6 dicembre 2017).

Inizialmente il CCW ha dovuto delimitare il suo oggetto di indagine e chiarire i termini delle questioni sul tappeto. Punto di partenza obbligato è

stato un esame delle proprietà salienti delle armi autonome in riferimento alla direttiva sull'autonomia dei sistemi d'arma pubblicata nel 2012 dal DoD. Secondo tale direttiva un'arma autonoma deve essere in grado, dopo la sua attivazione, «di selezionare e di attaccare gli obiettivi senza ulteriori interventi da parte di un operatore umano» (DoD, 2012). Ulteriori riferimenti sono state le analoghe descrizioni fornite sia dal Comitato Internazionale della Croce Rossa (CICR, 2014), sia da Human Rights Watch (HRW 2012).

Le caratteristiche salienti delle armi autonome forniscono un buon punto di partenza per la discussione politica, diplomatica e normativa su di esse, ma in tutta evidenza non bastano a delimitare con precisione sufficiente il campo. Si potrebbe infatti ragionevolmente sostenere che anche una mina antiuomo soddisfa la condizione per l'autonomia posta dal DoD, poiché essa è capace, sia pure in modo piuttosto primitivo, di selezionare, in funzione del peso rilevato dai suoi sensori, un obiettivo dopo essere stata attivata e di attaccarlo senza richiedere ulteriori interventi da parte di un operatore umano. In definitiva, l'impostazione al problema dell'autonomia adottata dal DoD e dal CICR non permette di distinguere adeguatamente l'autonomia operativa di armi costruite in base alle tecnologie più avanzate della robotica e della IA, le quali sollevano problemi etici nuovi e urgenti. Altri sistemi, come le mine antiuomo, pongono questioni etiche già adeguatamente riconosciute e affrontate nella Convenzione per la proibizione dell'uso, stoccaggio, produzione, vendita di mine antiuomo e relativa distruzione (nota anche come Trattato di Ottawa del 1997).

Per superare la difficoltà insita nell'impostazione al problema di cogliere le specificità dell'autonomia operativa dei sistemi d'arma, è utile considerare la proposta della ONG britannica *Article 36*. In un rapporto pubblicato nel 2013, *Article 36* pone l'accento sulla necessità di assicurare che gli attacchi sferrati da *tutti* i sistemi d'arma siano soggetti a un «controllo umano significativo» (*Article 36*, 2013). Questa proposta ha avuto il merito di individuare per prima nell'elemento umano la questione chiave da affrontare nella riflessione sull'autonomia dei sistemi d'arma. La preoccupazione di un'interruzione della catena di responsabilità nelle azioni belliche ha motivato l'introduzione dell'attributo “significativo” a proposito del controllo umano. Usando questo attributo, si intende escludere ogni forma di controllo puramente *nominale* di un sistema d'arma. Ciò potrebbe accadere se il controllore umano non ha a sua disposizione tempo sufficiente o informazioni adeguate per intervenire con cognizione di causa sul sistema d'arma, allo scopo di interromperne o di modificarne l'azione.

La formula del controllo umano significativo è stata accolta con interesse da molti attori del dibattito al CCW. Kerstin Vignard, vicedirettrice dell'UNIDIR (United Nations Institute for Disarmament Research), ha osser-

vato: «In definitiva, la questione dell'autonomia riguarda il tipo di controllo/vigilanza che riteniamo debba essere appannaggio degli esseri umani nell'impiego di strumenti per l'esercizio della violenza» (UNIDIR, 2016). Con una mozione presentata nel 2018 al CCW, Austria, Cile e Brasile hanno richiesto che il GGE proceda i suoi lavori con il mandato di negoziare uno strumento giuridico che sia vincolante per tutti gli Stati, finalizzato ad «assicurare un controllo umano significativo sulle funzioni critiche dei sistemi d'arma autonomi con effetti letali» (Austria *et al.*, 2018). Un interesse convergente da parte della comunità internazionale per la formula del Controllo Umano Significativo (CUS) è emerso con la pubblicazione nel 2018 di un documento del GGE nel quale si afferma che «è necessario preservare la responsabilità umana per le decisioni che riguardano gli usi letali della forza» (GGE, 2018).

Varie caratteristiche della formula CUS spiegano perché essa sia stata accolta con tanto favore. L'idea di imporre un controllo umano significativo su qualsiasi sistema d'arma può essere afferrata facilmente, anche in assenza di conoscenze specifiche sulle tecnologie militari più avanzate. La formula CUS si avvantaggia della sua «ambiguità costruttiva» (Crotoft, 2016, pp. 58-60). Essa è ambigua poiché non esplicita in che cosa debba consistere un controllo veramente significativo sui sistemi d'arma, ma è costruttiva perché esprime un'esigenza condivisa all'intersezione di posizioni diplomatiche e politiche che differiscono tra loro per altri aspetti. Inoltre, la formula CUS consente di mettere da parte la questione definitoria «Che cos'è un'arma autonoma?», ponendo al centro della discussione una questione normativa: «Quale controllo umano si deve esercitare su *ogni* sistema d'arma?». Poiché la questione normativa riguarda ogni sistema d'arma, essa riguarda in particolare le armi che meritano di essere chiamate autonome, comunque sia definita la loro autonomia.

Lo spostamento di attenzione sulla questione normativa consente di accantonare inconcludenti diatribe preliminari su cosa sia un'arma *veramente* autonoma, discussioni vaghe e concettualmente malferme sulla distinzione tra sistema automatico e sistema autonomo, concezioni inadeguate – perché troppo inclusive o troppo restrittive – dell'autonomia operativa di un sistema tecnologico (Amoroso e Tamburrini, 2019).

### 9.3. Il controllo umano significativo e i suoi contenuti

Se la formula CUS offre un punto di partenza promettente per affrontare le questioni normative sollevate dalle armi autonome, una soluzione adeguata a tali questioni deve dare una risposta alla domanda: «Che cosa rende

il controllo umano su un sistema d'arma veramente 'significativo'?» Per affrontare questa domanda, è utile richiamare i principi dell'etica dei doveri elencati e discussi nel capitolo 1:

- (i) Rispetto delle norme morali nella condotta delle azioni belliche introdotte dalla teoria della guerra giusta e dal DIU (con particolare riferimento ai principi di distinzione e proporzionalità).
- (ii) Mantenimento della catena delle responsabilità nelle azioni belliche.
- (iii) Rispetto della dignità degli esseri umani che possono subire l'uso della forza nelle azioni belliche.

Per garantire il rispetto di questi vincoli, è necessario assegnare all'essere umano alcuni ruoli fondamentali nel controllo dei sistemi d'arma (Amoroso e Tamburrini, 2019; 2021):

1. il controllo umano deve intervenire come sistema ausiliario di salvaguardia (*fail-safe*), per contribuire a impedire che il malfunzionamento o un comportamento imprevisto del sistema d'arma sfoci in un attacco diretto contro la popolazione civile e i suoi beni, in un danno collaterale eccessivo o in altre violazioni del DIU.
2. Il controllo umano deve funzionare come catalizzatore di responsabilità, assicurando la sussistenza delle condizioni per attribuire delle responsabilità personali nel caso di violazioni del DIU.
3. Il controllo umano deve garantire il rispetto della dignità degli esseri umani sottoposti a decisioni di vita o di morte in un conflitto armato, consentendo di ricondurre a un *agente morale* – piuttosto che a una macchina priva di tale attributo – le decisioni che hanno un impatto sulla loro vita, sulla loro integrità fisica e sui beni dei quali dispongono.

Sono state ampiamente discusse nel capitolo 5 le motivazioni etiche e giuridiche a sostegno delle funzioni e dei ruoli degli operatori umani (elencate ai punti 2 e 3). A proposito del punto 1, è importante sottolineare anche qui il contributo che un essere umano può dare per prevenire i cosiddetti «disastri della IA» nelle azioni belliche. Un sistema della IA può indurre violazioni del DIU a causa di errori percettivi o di valutazione nei quali gli esseri umani non incorrono normalmente o che possono individuare utilizzando indizi contestuali difficilmente accessibili alla macchina (vedi la discussione di questo punto e le illustrazioni variamente fornite nei capitoli 2, 3, e 5). L'importanza di questa funzione per l'esercizio di un controllo umano che sia davvero significativo può essere evidenziata ricordando il noto caso del falso allarme nucleare nel quale fu protagonista il colonnello dell'aviazione sovietica Stanislav Yevgrafovich Petrov.

La mattina del 26 settembre 1983, il sistema sovietico OKO di *early warning* per gli attacchi nucleari registrò il lancio in rapida sequenza di cinque missili balistici, partiti dal territorio degli Stati Uniti e diretti verso l'Unione

Sovietica. Petrov, ufficiale responsabile di turno, arrivò a concludere che si trattava di un falso allarme dovuto a un malfunzionamento del sistema. In base a tale convincimento, Petrov contravvenne alla consegna di trasmettere ai superiori la notizia dell'allarme segnalato dal sistema, notificando invece un episodio di malfunzionamento. La diagnosi di Petrov si rivelò giusta. Ricevendo la segnalazione di lancio generata da OKO, il comando sovietico avrebbe potuto decidere di rispondere a sua volta con un lancio di missili balistici, scatenando così una guerra nucleare devastante.

Un altro fattore da ricordare in relazione al punto 1 riguarda gli attuali limiti dei sistemi di IA, analizzati nel capitolo 4 e, soprattutto, la loro limitata capacità di fornire spiegazioni comprensibili agli esseri umani per le loro decisioni e azioni. Per intervenire come sistema ausiliario di salvaguardia, un operatore umano deve avere le informazioni necessarie sulle decisioni e sulle azioni che l'arma autonoma sta per intraprendere. In particolare, l'operatore deve essere messo in grado di comprendere il perché di una decisione assunta dall'arma autonoma. Il campo di ricerca della XAI (*Explainable AI*) si occupa proprio del problema di dotare i sistemi della IA di una tale capacità di spiegazione. Ma i risultati finora conseguiti in questo ambito di ricerca non sono ancora sufficientemente adeguati a fornire agli operatori umani le spiegazioni necessarie a svolgere il loro ruolo di sistemi ausiliari di salvaguardia.

È importante a questo punto chiedersi se la richiesta di imporre un controllo umano significativo su ogni sistema d'arma implichi in modo necessario e uniforme l'eliminazione dell'autonomia operativa dei sistemi d'arma, per quanto riguarda specificamente le funzioni critiche di selezione e attacco di un obiettivo militare evidenziate dal DoD e dal CICR. Esistono infatti molti sistemi d'arma che sono da tempo utilizzati dalle Forze armate di vari Stati e soddisfano le funzioni critiche individuate dal DoD e dal CICR, senza aver tuttavia suscitato obiezioni di incompatibilità con il DIU o altre obiezioni di tipo etico o giuridico. Uno di questi sistemi d'arma è il sistema mobile antimissile *Iron Dome*, utilizzato in Israele per monitorare e neutralizzare con il lancio di missili intercettori i razzi e altri proiettili balistici diretti verso il territorio israeliano (<https://www.army-technology.com/projects/iron-dome-air-defence-mi/>). Gli operatori militari si limitano a posizionare sul terreno *Iron Dome* e a circoscrivere l'area che esso deve monitorare e proteggere. Dopo aver compiuto queste operazioni preliminari, gli operatori abilitano *Iron Dome* ad operare in piena autonomia. Dotato di analoghe capacità di intercettazione, anche il sistema anti-materiali NBS (*Nächstbereichschutzsystem*) *MANTIS*. Esso è utilizzato dalle forze armate tedesche per proteggere i soldati e le installazioni militari da proiettili balistici in arrivo (<https://www.army-technology.com/projects/mantis/>). I tempi di reazione di *Iron Dome* e *MANTIS* – come pure del *Phalanx* e del *Centurion C-Ram* in

dotazione alle Forze armate statunitensi – sono molto più rapidi dei tempi di reazione di un operatore umano e consentono perciò di proteggere persone e cose con efficacia decisamente maggiore di un sistema che sia asservito a un operatore umano per la decisione ultima di attacco (vedi capitolo 4, e inoltre Rossi, 2019, p. 10). I ritardi insiti nel ciclo percezione-decisione-azione di un operatore umano sono generalmente troppo estesi per proteggersi efficacemente da proiettili balistici in arrivo.

L'uso di *Iron Dome*, *Mantis*, *Phalanx* e di altri sistemi autonomi anti-materiali che funzionano come scudi protettivi di difesa da proiettili in arrivo non è stato mai messo in discussione da una prospettiva etica o giuridica. E tuttavia tali sistemi soddisfano le proprietà salienti di un'arma autonoma, e cioè di selezione e di attacco indipendente di un obiettivo dopo la loro attivazione. Per esercitare il CUS non sembra necessario privare questi sistemi della loro autonomia nelle funzioni critiche di selezione e attacco di un obiettivo costituito. È infatti generalmente sufficiente, nelle loro normali condizioni d'uso, che un operatore umano si accerti periodicamente che non vi siano oggetti o persone da proteggere nel campo di azione dell'arma. Questo tipo di controllo non è invece sufficiente per garantire il CUS su altre armi autonome esistenti, che non sono state progettate o abitualmente impiegate come sistemi autonomi difensivi contro i proiettili balistici in arrivo, bensì come armi autonome a prevalente uso offensivo (Boulain e Verbruggen, 2017, p. VII).

Armi autonome offensive già esistenti sono le cosiddette munizioni *loitering*, velivoli senza equipaggio armati di una testata esplosiva, i quali possono girovagare per un certo periodo di tempo alla ricerca di un obiettivo sul quale impattare all'interno di un perimetro prefissato (vedi capitolo 2). L'operatore umano, prima di procedere alla loro attivazione, stabilisce l'area geografica in cui intervenire e le categorie di obiettivi che l'arma è abilitata ad attaccare, nonché la durata massima dell'operazione (Boulain e Verbruggen, 2017, p. VII). Il missile israeliano *Harpy* è di tipo *loitering*. Esso può volare per ore in cerca di segnali emessi dalle postazioni radar del nemico, piombando su di esse per distruggerle al momento dell'impatto (vedi capitolo 4, e inoltre Rossi, 2019, p. 8). Le situazioni nelle quali opera *Harpy* possono evolvere rapidamente e in maniera imprevedibile nella fase di pianificazione dell'azione. Mentre *Harpy* sorvola l'area stabilita, un veicolo adibito al trasporto di civili potrebbe avvicinarsi a una postazione radar nemica da attaccare, oppure la postazione radar potrebbe essere montata su un veicolo spostatosi in prossimità di un ospedale. In entrambi i casi, un attacco di *Harpy* alla postazione radar potrebbe avere conseguenze incompatibili con i principi di distinzione e proporzionalità codificati nel DIU. I danni provocati sarebbero difficilmente riconducibili alle responsabilità degli operatori umani, poiché il contesto operativo è cambiato in modo imprevedibile dopo l'attivazione del sistema.



Pertanto, al fine di esercitare il CUS su un tale sistema è necessario che un operatore umano possa monitorare costantemente se vi siano oggetti o persone da proteggere nel campo di azione dell'arma e abbia il potere effettivo di autorizzarne l'attacco o di impedirne l'esecuzione.

#### **9.4. Verso un trattato internazionale sul controllo umano significativo delle armi autonome?**

Gli esempi elementari presi in considerazione nel paragrafo precedente suggeriscono che le armi autonome esistenti richiedono diverse forme di CUS, in quanto differiscono tra loro per tipologia, impiego e contesto d'uso. Alla luce di osservazioni di questo tenore, si è fatta strada nel dibattito accademico, diplomatico e politico l'idea che armi autonome diverse possano richiedere livelli diversi di controllo umano per garantire il rispetto dei vincoli etici e giuridici esaminati nel capitolo 5 e richiamati più sopra (Amoroso e Tamburrini, 2019; IPRAW, 2019). Un tale approccio *differenziato* al problema del CUS implica che si debba distinguere tra vari livelli di controllo condiviso tra uomo e macchina nello svolgimento dei compiti critici di selezione e ingaggio di un obiettivo e che si assegni a ciascuna arma il livello di controllo adeguato dalla prospettiva normativa etica e giuridica.

La seguente lista di livelli di controllo condiviso dell'azione tra uomo e macchina, per quanto schematica, ci permette di dare un'idea generale di quale sia il problema che una soluzione differenziata al problema del CUS deve affrontare (Sharkey, 2016; Amoroso e Tamburrini, 2019 e 2021). I cinque livelli considerati sono ordinati in base a privilegi di controllo che a mano a mano si spostano dall'essere umano (che esercita un controllo totale a L1 sulle funzioni critiche di selezione e ingaggio di un obiettivo) alla macchina (che invece ha un controllo totale a L5):

- L1: la selezione dell'obiettivo da attaccare è integralmente effettuata dall'operatore umano;
- L2: la selezione dell'obiettivo da attaccare è effettuata dall'operatore umano in base a un ventaglio di opzioni suggerite dal sistema d'arma;
- L3: l'operatore umano si limita ad approvare o a rifiutare la scelta del sistema d'arma in merito all'obiettivo da attaccare;
- L4: l'operatore umano supervisiona la selezione dell'obiettivo effettuata dal sistema, mantenendo la possibilità di riprendere il controllo e annullare l'attacco;
- L5: l'operatore umano si limita ad attivare il sistema d'arma, definendone la missione nella fase preliminare di pianificazione, senza avere la possibilità di intervenire nella fase operativa.

Abbiamo già visto che L5 è un livello troppo sbilanciato a favore della macchina, almeno per quanto riguarda la ricerca dinamica di obiettivi (come illustrato dal caso di *Harpy* e di altre munizioni di tipo *loitering*). D'altra parte, L1 e L2, se proposti come i livelli sempre e comunque più appropriati per l'esercizio del CUS, risultano essere troppo sbilanciati a favore dell'uomo, almeno per quanto riguarda l'utilizzazione di sistemi difensivi come *Iron Dome* e *MANTIS*. Una soluzione al problema del CUS che tenga conto di tali differenze deve modulare opportunamente il controllo umano lungo i livelli L1-L5, in base alle caratteristiche dei sistemi d'arma e dei loro contesti d'uso. Da un lato, per garantire che gli operatori umani esercitino sempre il CUS, non è necessario escludere in ogni circostanza l'autonomia dei sistemi d'arma nelle funzioni critiche di selezione e attacco di un obiettivo, come pretenderebbe una soluzione uniforme ad autonomia zero per qualsiasi sistema d'arma. Ma da un altro lato, per mantenere il CUS non è sempre sufficiente circoscrivere l'esercizio del controllo umano alla fase di pianificazione dell'azione militare.

Tra le varie tipologie di soluzione differenziata al problema del CUS che si possono escogitare e sottoporre al dibattito diplomatico e politico, ci limitiamo ad abbozzare qui uno schema di proposta che è differenziata sui livelli L1-L5, ma *prudenziale* per quanto riguarda le condizioni per il mantenimento del CUS (Amoroso e Tamburrini, 2019 e 2021; Amoroso, 2021).

Consideriamo innanzitutto la sentinella robotica SGR-A1 (Rossi, 2019), ideata in Corea del Sud per selezionare ed eventualmente aprire il fuoco autonomamente sugli intrusi nella zona demilitarizzata tra le due Coree. Un CUS adeguato su SGR-A1 potrebbe essere esercitato a livello L2, che prevede l'approvazione o il rifiuto di un operatore umano delle proposte del sistema in merito agli obiettivi da attaccare. Un controllo a livello L2 potrebbe essere sufficiente anche per il cosiddetto *deliberate targeting* – la selezione pianificata di obiettivi – purché l'operatore umano abbia informazioni adeguate a decidere se vi siano stati cambiamenti nello scenario operativo tali da richiedere una nuova pianificazione o l'interruzione della missione. Nel caso di *Iron Dome* e di altri sistemi difensivi simili, il CUS potrebbe essere adeguatamente mantenuto anche al livello L3, che prevede la supervisione di un operatore umano con diritto di veto nelle fasi operative, seppure l'esercizio effettivo del diritto di veto sarà, per forza di cose, limitato dai tempi rapidi di risposta del sistema.

Più in generale, una soluzione differenziata ma prudenziale al problema del CUS potrebbe articolarsi in due punti principali. Per prima cosa, in assenza di informazioni specifiche al contrario, si potrebbero imporre per default i livelli L1 o L2 di controllo umano (aspetto *prudenziale* della soluzione). Potrebbero però essere ammesse eccezioni alla regola default,

opportunamente argomentate e sottoscritte dalla comunità internazionale degli Stati, consentendo di andare oltre L2 nel caso di specifici sistemi d'arma e modalità d'uso, a patto che il rispetto dei vincoli etici e giuridici sulla condotta delle azioni belliche non sia minacciato spostando in questo modo i privilegi di controllo verso la macchina (aspetto *differenziato* della soluzione).

Con quali motivazioni si può sostenere la scelta di dare priorità a una regola default che indica il livello L2 di controllo condiviso come quello da adottare in assenza di informazioni al contrario? Le principali motivazioni per questa scelta derivano dai limiti – illustrati in vari modi nei capitoli 2, 3, e 5 – alla possibilità di prevedere e di controllare il comportamento dei sistemi d'arma che sono basati sulle tecnologie della IA e della robotica. Questi limiti dipendono dalle capacità stesse della macchina e dalle sue interazioni con l'ambiente operativo:

- la capacità di apprendere, fondamentale per sviluppare un sistema avanzato della IA e della robotica;
- la capacità di vagare (*loitering*) per un periodo esteso di tempo alla ricerca di un obiettivo da attaccare su un territorio che è soggetto a cambiamenti, anche repentini, delle condizioni osservate al momento di pianificare l'azione dell'arma autonoma;
- la capacità di coordinarsi con altri sistemi in assenza di un sistema centralizzato di controllo che l'operatore umano possa supervisionare (*swarming* o intelligenza da sciame);
- le interazioni e le conseguenti perturbazioni del comportamento atteso che derivano dai tentativi di jamming, hackeraggio e altri attacchi cibernetic;
- le complesse e veloci interazioni, di carattere competitivo o cooperativo, con altri sistemi artificiali, che avvengono su un campo di battaglia destinato a divenire sempre più informatizzato e robotizzato.

In definitiva, in assenza di prove convincenti che specifiche armi autonome non sollevano problemi previsionali e di controllo dovute a questi vari fattori, l'imposizione della regola default offre una protezione prudenziale dalle violazioni dei vincoli etici e giuridici che modellano i contenuti del CUS.

## 9.5. Osservazioni conclusive

Per tradurre la proposta di soluzione differenziata e prudenziale al problema del CUS in un effettivo strumento multilaterale di regolamentazione delle armi autonome, le sfide più importanti per la comunità politica e di-

plomatica internazionale riguarderanno l'individuazione di procedure operative per applicare i livelli più elevati di controllo umano in tutte quelle circostanze nelle quali non vi sono informazioni tali da giustificare l'introduzione di specifiche eccezioni. Tali procedure dovranno essere sottoposte all'esame e all'approvazione della comunità internazionale degli Stati nel consesso del CCW o in altre sedi internazionali opportune. Bisogna però evidenziare che i lavori del CCW non hanno sinora registrato progressi significativi né in questa direzione specifica, né nella direzione più generale di un qualsiasi strumento multilaterale in merito al problema del CUS. Anche la sesta Conferenza di revisione degli Stati parte della CCW, tenutasi dal 13 al 17 dicembre 2021 a Ginevra, è stata un'occasione mancata per intraprendere un percorso fruttuoso verso la regolamentazione dei sistemi di armi autonome. Smentendo aspettative diffuse, gli Stati parte della CCW si sono limitati ad aggiornare i lavori del GGE, senza fornire né un chiaro mandato al GGE per negoziare uno strumento multilaterale in merito, né la minima indicazione sui suoi possibili contenuti, come si può constatare leggendo la Decisione I contenuta nel testo della Dichiarazione finale (CCW 2022). Questa mancanza di ambizione è deludente, soprattutto alla luce di inviti recenti a conseguire risultati più tangibili, che sono stati espressi da vari attori internazionali indipendenti e autorevoli, come il Segretario Generale delle Nazioni Unite, Il CICR e la maggioranza di Stati parte del CCW.

Gli osservatori concordano sul fatto che il fallimento della sesta Conferenza di revisione, così come le persistenti difficoltà nei lavori del GGE, testimoniate dall'assenza di progressi tangibili nelle due sessioni tenutesi nel 2022 (<https://meetings.unoda.org/meeting/ccw-gge-2022/> ) derivano in ultima analisi dall'azione di un gruppo ristretto di potenze militari (si veda per esempio <https://www.hrw.org/news/2021/12/19/killer-robots-military-powers-stymie-ban>). Guidate da Stati Uniti e Russia, queste potenze fanno leva sul metodo del *consensus*, che caratterizza il processo decisionale della CCW, per bloccare qualsiasi progresso della discussione.

L'opposizione alla regolamentazione multilaterale è spiegabile verosimilmente in base al timore che una richiesta troppo restrittiva di controllo umano porti a una proibizione indiscriminata di tutte le armi autonome, nonostante alcuni benefici militari attesi. Un tale timore può essere in parte stemperato dallo schema di proposta di soluzione al problema del CUS avanzata nel paragrafo precedente. In quanto differenziata, tale proposta respinge soluzioni uniformi alla questione del controllo umano, astenendosi altresì dal proibire *tutti* i sistemi di armi autonome. Vi sono livelli di autonomia normativamente accettabili (ad esempio, autonomia supervisionata) per alcuni sistemi d'arma (ad esempio, armi autonome anti-materiali con funzioni esclusivamente difensive). Tuttavia, rigorosi vincoli operativi devono essere invariabilmente

rispettati (ad esempio per quanto riguarda restrizioni sulle finestre temporali di utilizzo o sulle caratteristiche del campo di battaglia), per garantire che l'autonomia di un'arma non ostacoli mai l'esercizio del CUS e il rispetto dei principi etici e giuridici soggiacenti. In quanto prudenziale, tale proposta impone i livelli più stringenti di controllo umano sull'ingaggio di un obiettivo, ma consente l'introduzione di disposizioni meno restrittive, purché esse siano state concordate a livello internazionale.

Una proposta differenziata è stata avanzata nel maggio 2021 anche dal CICR. Essa prevede due divieti ad ampio spettro riguardanti (1) le armi autonome antiuomo e (2) le armi autonome che hanno comportamenti imprevedibili. L'autonomia nei sistemi d'arma è altrimenti permessa, anche se soggetta a severe restrizioni, per quanto riguarda i tipi di obiettivi, i limiti sulla durata, la portata geografica e la scala di utilizzo, i limiti sulle situazioni di utilizzo (come l'assenza di civili), nonché la supervisione umana garantita e il potere di veto. Questa proposta, che si sviluppa in due direzioni (divieto o regolamentazione) è stata sposata dal presidente del GGE nel 2021, l'ambasciatore belga Marc Pecsteen de Buytsverve, nel suo tentativo di incoraggiare il consenso sulla necessità di negoziare uno strumento multilaterale sui sistemi di armi autonome. La sua adesione, tuttavia, non ha sortito l'effetto sperato, come testimonia il risultato deludente delle già ricordate sessioni del GGE nel 2022 e, parallelamente, della sesta Conferenza di revisione della CCW. Di conseguenza, alcuni Stati interessati e le Ong coinvolte nella campagna SKR stanno valutando l'opzione di esplorare sedi alternative al CCW per negoziare un accordo internazionale che sancisca il requisito del CUS, sulla scia di ciò che è già avvenuto sia per la Convenzione sulla messa al bando delle mine antiuomo sia per la Convenzione sulle munizioni a grappolo.

## Riferimenti bibliografici

- Amoroso D. (2021), *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*. Edizioni Scientifiche Italiane e Nomos Verlag, Napoli.
- Amoroso D., Sauer F., Sharkey N., Suchman L., Tamburrini G. (2018), *Autonomy in Weapon Systems. The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy*, Heinrich Böll Stiftung, Berlino.
- Amoroso D., Tamburrini G. (2017), "The Ethical and Legal Case Against Autonomy in Weapons Systems". *Global Jurist*, 17, 3: 1-20.
- Amoroso D., Tamburrini G. (2019), *What makes human control over weapon systems "meaningful"?*, Working paper #4, International Committee for Robot Arms Control, testo disponibile al sito: <https://www.icrac.net/research/>.

- Amoroso D., Tamburrini G. (2021), Toward a normative model of meaningful human control over weapon systems, *Ethics & International Affairs*, 35, 2: 245-272.
- Arkin R. C. (2009), *Governing Lethal Behavior in Autonomous Robots*, CRC Press, Boca Raton.
- Article 36 (2013), *Killer Robots: UK Government Policy on Fully Autonomous Weapons*, Londra, 19 aprile 2013, testo disponibile al sito: <http://www.article36.org/weapons-review/killer-robots-uk-government-policy-on-fully-autonomous-weapons-2/>.
- Austria, Brasile, Chile (2018), *Proposal for a Mandate to Negotiate a Legally Binding Instrument that addresses the Legal, Humanitarian and Ethical Concerns posed by Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (LAWS), submitted to the Group of Governmental Experts on lethal autonomous weapons of the CCW*. Ginevra: ONU, testo disponibile al sito: <https://undocs.org/CCW/GGE.2/2018/WP.7>.
- Boulanin V. and Verbruggen M. (2017), *Mapping the development of autonomy in weapons systems*, SIPRI – Stockholm International Peace Research Institute, Stoccoloma, testo disponibile al sito: <https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems>).
- CICR (2014). *Autonomous weapon systems: Technical, military, legal and humanitarian aspects. CCW Expert meeting*, International Committee of the Red Cross, Ginevra, testo disponibile al sito: <https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014>
- CICR (2016), *Views of the International Committee of the Red Cross on autonomous weapon system*, paper submitted to the Informal meeting of experts on lethal autonomous weapons systems of the Convention on Certain Conventional Weapons (CCW), Geneva (11 April 2016).
- CICR (2021), ICRC Position on Autonomous Weapons Systems, Geneva: ICRC, 12 May.
- Crootof R. (2016), “A Meaningful Floor for ‘Meaningful Human Control’”, *Temple Journal of International & Comparative Law*, 30: 53-62.
- CCW (2022), *Final Document of the Sixth Review Conference*, CCW/CONF/VI/II, Convention on Certain Conventional Weapons, Geneva, 12 January.
- DoD (2012), *Autonomy in Weapons Systems*, Directive 3000.09. Washington DC:US Department of Defense, testo disponibile al sito: [www.dtic.mil/whs/directives/corres/pdf/300009p.pdf](http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf).
- Heyns Ch. (2013), *Report of the Special rapporteur on extrajudicial, summary or arbitrary executions*, 9 April 2013, UN Doc. A/HRC/23/47.
- HRW (2012), *Losing Humanity. The Case against Killer Robots*, Human Rights Watch, New York, 19 November 2012.
- HRW (2015), *Mind the Gap: The Lack of Accountability for Killer Robots*. Rapporto pubblicato il 9 aprile 2015. New York, Human Rights Watch, testo disponibile al sito: <https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots>.
- IPRAW (2019), *Focus on human control*. Report n. 5, Berlin, Agosto 2019, testo disponibile al sito: <https://www.ipraw.org/human-control/>).

- Rossi J. C. (2019), “Un’opera dell’uomo: le macchine autonome letali”. *IRIAD Review*, n. 5, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Sharkey N. E. (2007), “Automated Killers and the Computing Profession”, *Computer*, 40, 11: 122-123
- Sharkey N. E. (2008), “Cassandra or False Prophet of Doom: AI Robots and War”, *IEEE Intelligent Systems*, 23, 4: 14-17.
- Sharkey N. E. (2012), “The inevitability of autonomous robot warfare”, *International Review of the Red Cross*, 94: 787-789.
- UNIDIR (2016). *Statement of the UN Institute for Disarmament Research at the CCW Informal Meeting of Experts on Lethal Autonomous Weapon Systems*, 12 Aprile, testo disponibile al sito: <http://www.unidir.org/files/medias/pdfs/unidir-s-statement-to-the-ccw-informal-meeting-of-experts-on-lethal-autonomous-weapon-systems-eng-0-648.pdf>

## *10. Le armi autonome tra sviluppo economico e controllo politico: istituzioni internazionali, comunità scientifiche, società civile*

di Barbara Gallo, Maurizio Simoncelli

### **10.1. Spese militari e investimenti nelle armi semiautonome e autonome**

Non c'è stato bisogno del drammatico conflitto che l'invasione russa ha innescato in Ucraina per assistere a un'inversione nella tendenza al contenimento delle spese militari a livello mondiale. Conclusasi la breve stagione di speranze sui possibili dividendi della pace, apertasi con la fine della guerra fredda, già dalla fine degli anni '90 del secolo scorso, i dati del SIPRI mostrano un incremento in cifre assolute: dai 1.075 miliardi di dollari del 1998, ai 1.644 del 2008, ai 2.113 del 2021.

Come noto, di gran lunga al primo posto nella percentuale della spesa militare mondiale si collocano gli Stati Uniti con il 38%. Segue al secondo posto la Cina con il 14%. Al terzo posto si collocano i 4 maggiori paesi europei – Francia, Germania, Gran Bretagna, Italia – che insieme sfiorano il 10% del totale mondiale.

Come abbiamo visto nelle pagine precedenti, Stati Uniti, Russia, Israele, Cina, India, Gran Bretagna, Francia, Corea del Sud ed altri stanno investendo rilevanti risorse nelle armi semiautonome, al punto che già dispongono di sistemi con un elevato grado di autonomia come i velivoli e veicoli senza pilota e le munizioni circuitanti (*loitering*) dette anche droni-kamikaze. Dalla semi-autonomia, la marcia degli armamenti *man-off-the-loop* ovviamente non è un *unicum*, prerogativa di un settore tecnologico da sempre all'avanguardia, ma si inserisce nel generale contesto dei grandi investimenti che le principali nazioni del mondo stanno dedicando all'automazione del campo di battaglia, processo destinato a toccare l'apice con l'ingresso della IA.

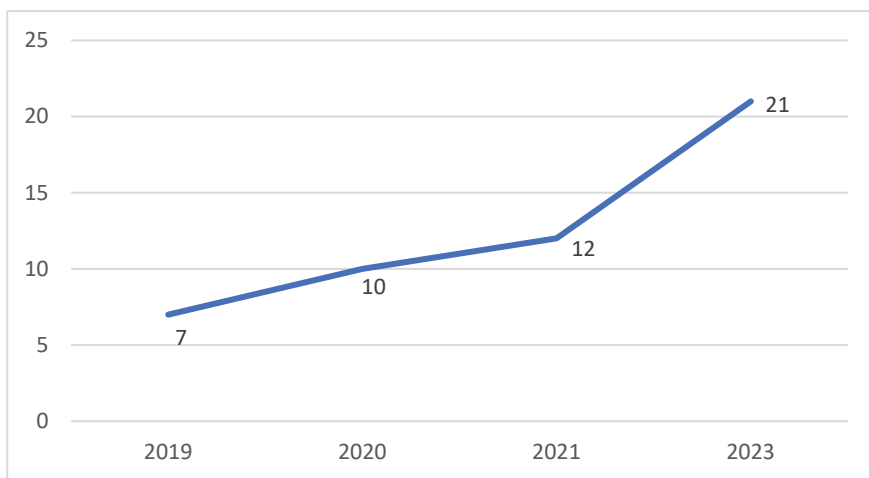
Secondo un report di International Data Corporation (IDC, 2022), si stima che i ricavi globali per il comparto della IA, compresi software, hardware e



servizi, si stiano incrementando del 19,6% su base annua, raggiungendo nel 2022 la cifra di 432,8 miliardi di dollari, destinati nel 2023 a superare la soglia dei 500 miliardi.

Quanto all'Europa, secondo i dati elaborati da *Statista.com*, le spese per la IA sono state di oltre 7 miliardi di dollari nel 2019 mentre si prevede la loro triplicazione nel 2023 (v. fig. 1).

Fig. 1 – Spesa prevista per l'IA in Europa 2019-2023 (mld \$)



Fonte: *Statista.com* 2022

Nel marzo 2022 Matt Asay su *Techrepublic.com*, analizzando il Rapporto *Stanford AI Index*, rilevava che gli investimenti privati nella IA sono arrivati a 93,5 miliardi di dollari nel 2021, più che raddoppiando la cifra del 2020. Nel settore della R&S, il numero di brevetti IA depositati nel 2021 risulta superiore di 30 volte rispetto a quello del 2015, con un tasso di crescita annuale composto del 76,9%. Questa mole di brevetti comporta un significativo incremento dei finanziamenti di *venture capital* delle startup, soprattutto negli USA (52,9 miliardi di dollari nel 2021), cioè il triplo della Cina (17,2 miliardi di dollari) e più del decuplo della Gran Bretagna (4,6 miliardi di dollari).

La crescita degli investimenti nella ricerca nello specifico settore delle armi autonome è in proporzione. Nel periodo 2015-2020 gli USA hanno investito 18 miliardi di dollari. La costituzione di appositi centri di ricerca (come lo statunitense Joint Artificial Intelligence Center – JAIC o il britannico Defence Science and Technology Laboratory – DSTL) rappresentano chiaramente la volontà dei rispettivi governi di potenziarle sempre di più la R&S in questo comparto, per poi dotare delle nuove armi le proprie forze armate.

## 10.2. La IA in guerra e in combattimento: problemi strategici e tattici

Negli ultimi tempi le tecnologie della IA applicate in vari ambiti (riconoscimento di immagini e della voce, traduzione linguistica simultanea, aggregazione e analisi di immense quantità di dati – *data analytics* e *data science*, controllo di sistemi autonomi ecc.) hanno registrato notevoli successi. L'applicazione della IA ai sistemi d'arma ha suscitato interesse in ambito militare, sia nell'ambito dei sistemi C3IR, sia in quello del supporto alle decisioni, sia infine in quello della realizzazione vera e propria di armi autonome. L'interesse suscitato dalla IA, però, non oscura alcune criticità né impedisce alcune riflessioni.

Come si è visto nel capitolo 1, l'imperativo comune ai sistemi politico-militari occidentali è quello di evitare sempre più, per le proprie forze armate, il rischio delle perdite umane, pur intrinseco al concetto di guerra. Questo è evidente anche nella massiccia diffusione delle armi semiautonome (droni). Tuttavia il passaggio ulteriore all'adozione di armi autonome (robot killer) apre pericolosi spiragli verso un campo di battaglia dove si scontrano sempre più le macchine da guerra e sempre meno gli uomini e dove a prevalere sono la capacità tecnologica e la potenza industriale di un paese. Non a caso Vladimir Putin già nel settembre del 2017 aveva affermato che «chi svilupperà la migliore intelligenza artificiale, diventerà il padrone del mondo» (Pax for Peace, 2019).

La fascinazione della IA nasconde il fatto che un vero controllo umano su questi sistemi è nella realtà assai difficile e complesso. È forte la preoccupazione di fronte al tentativo di realizzare sistemi in grado di operare, nei confronti del controllo umano, con un'autonomia che aumenti progressivamente sino alla totale emancipazione della macchina dall'uomo.

È stato osservato che la drastica restrizione del tempo del ciclo osservazione-decisione-azione (caratteristico delle operazioni militari) comporta regole di ingaggio inevitabilmente più rapide ed operazioni molto più veloci di quanto non potrebbe eseguire l'essere umano. Il discorso è ancora più calzante se facciamo riferimento allo *swarm*, alle decisioni assunte collettivamente e operate dallo sciame. In generale, le vulnerabilità informatiche, di cui si è ampiamente parlato nel cap. 4, sono assai numerose e particolarmente insidiose: si va dalla contaminazione (*poisoning*) dei dati o delle procedure di training all'inserzione di eventuali *backdoor* attivate da dati opportunamente manipolati, sino all'inserimento nascosto di un codice malevolo di attacco (*payload*) all'interno delle reti neurali. Il risultato del lavoro degli algoritmi a volte appare inatteso agli stessi programmatori. A loro volta, i malfunzionamenti o le manipolazioni possono avere effetti a cascata sui sistemi

complessi che dipendono dagli algoritmi stessi, con danni molto più vasti di quanto si possa immaginare.

Fondamentali e necessarie sono non solo una grande disponibilità di dati da utilizzare, ma anche la capacità di apprendere da parte della IA attraverso la procedura di ML (programmazione, addestramento, testing e uso) partendo appunto dai dati e dall'esperienza. Questo presuppone che la IA deve operare ripetutamente accumulando una serie di informazioni sui risultati positivi e negativi della sua azione, ciò che in caso di decisioni letali errate solleva evidentemente gravi dubbi. Considerati i limiti e le problematicità del ML, l'utilizzo della IA come unica fonte per decisioni importanti appare assai rischioso. Per di più sappiamo che esiste una vulnerabilità dei sistemi della IA da parte di attacchi cibernetici, analogamente a quanto si è visto nel corso del 2022, con gli attacchi hacker contro siti istituzionali o di grandi imprese.

Un particolare rilievo assume pertanto l'esperienza dei tecnici di ML e le loro specifiche competenze: se gli "addestratori" della IA non sono al livello professionale richiesto, si avranno conseguenze negative di analogo livello. Come è stato ricordato nel capitolo 5, piccole perturbazioni dei valori dei pixel che formano l'immagine di input, che al nostro occhio sfuggono, possono portare la macchina a clamorosi errori, scambiando uno scuolabus per uno struzzo. Se questi errori avvengono in una situazione di stress da combattimento (dove gli imprevisti possono essere infiniti), è facile prevedere che cosa possa succedere.

Poi, la presenza occulta di *bias*, cioè di pregiudizi presenti nella programmazione degli algoritmi, può comportare ulteriori problemi di affidabilità, ovviabili solo attraverso una grossa quantità di dati di alta qualità e di un adeguato addestramento, elementi non sempre disponibili sul campo di battaglia. La cosiddetta *fog of war* quindi può interferire sul funzionamento della IA. Oltretutto essa è esposta anche ad una serie di possibili attacchi avversari, quali i cosiddetti *adversarial attacks*, che comprendono i *causative attacks* (creazione di debolezze nel sistema da sfruttare in un secondo tempo) e gli *exploratory attacks* (individuazione di punti deboli degli specifici programmi di ML).

Se si considerano tutte queste problematiche, ad esempio estendendole anche in relazione alla questione del nucleare militare, le preoccupazioni aumentano a dismisura. Affidare a sistemi autonomi un'eventuale azione nucleare militare a fronte di un ipotetico attacco appare assai rischioso, anche alla luce delle esperienze passate (v. sopra cap. 9).

Analogamente, in assenza della supervisione umana, un eventuale errore della IA potrebbe scatenare una guerra nucleare globale. Invece di aumentare la sicurezza si avrebbe una crescente incertezza, nonché una pericolosa

confusione: pensiamo all'utilizzo della IA nel caso dell'individuazione di missili ipersonici, che per le loro caratteristiche provocano un'ambiguità relativamente sia all'obiettivo (forze nucleari o convenzionali?), sia alla destinazione (contro quale paese?), sia all'origine (da dove provengono?) (Pascolini, 2020).

Data poi la duplice capacità nucleare/convenzionale dei missili ipersonici, l'urgenza di comprendere la tipologia della testata può portare ad affidarne l'analisi e la decisione finale alla IA, in grado di assumere decisioni in tempi brevissimi elaborando una grande mole di dati. Non a caso è stata sottolineata la necessità di affrontare «non solo i potenziali vantaggi della militarizzazione della IA, ma anche e soprattutto i possibili rischi e la relativa governance» (Pascolini, 2020).

Di fronte a questo quadro complesso, con alcune luci e molte ombre, l'attuale corsa agli armamenti basata sulla IA appare ulteriormente preoccupante in un quadro di relazioni internazionali fortemente compromesse, i cui nodi insoluti sarebbero da affrontare non con un dilagante riarmo, ma con un costruttivo approccio negoziale e con auspicabili soluzioni multilaterali. La crisi della biosfera che sta minacciando la vita sul nostro pianeta – dal deterioramento del clima alle pandemie – ha bisogno di risposte condivise, non di armamenti sempre più sofisticati, realizzati per tentare un dominio egemonico del mondo comunque impossibile.

### **10.3. Dibattiti e proposte nelle istituzioni internazionali**

È evidente che l'adozione di sistemi d'arma autonomi comporterebbe una trasformazione radicale nella gestione dei conflitti, con un inevitabile sovvertimento del quadro in ambito etico, giuridico, comportamentale e operativo. D'altronde la società civile ha avvertito i rischi e i pericoli di una applicazione incontrollata della IA ai sistemi d'arma, come è emerso sia dalla rilevazione IPSOS del 2021 su 28 Paesi, sia da quella dell'Archivio Disarmo del febbraio 2019, entrambe discusse nel cap. 7. Per quanto riguarda gli italiani, essi hanno espresso un'ampia contrarietà nei confronti dell'autonomizzazione (59% nel caso comparato, 68% nel caso italiano). Almeno altrettanto rilevanti le prese di posizione della comunità scientifica a partire dal 2012, in particolare in occasione della lettera aperta del 2015 firmata da migliaia di ricercatori della IA e della robotica. Né sono da trascurare i successivi appelli formulati da imprenditori dei settori dell'informatica, della robotica e della IA, da gruppi di loro dipendenti, da ricercatori operanti in settori affini (v. cap. 9).

Dal punto di vista giuridico, i LAWS devono comunque ottemperare alle norme del diritto internazionale umanitario, in riferimento sia al manteni-

mento della catena delle responsabilità nelle azioni belliche, sia al rispetto della dignità degli esseri umani coinvolti nelle medesime. Come è stato messo in evidenza nei capitoli 2 e 8, non solo è difficile distinguere un nemico fuori combattimento ai sensi di quanto prevede il Protocollo del 1977, art. 41, aggiuntivo alle Convenzioni di Ginevra del 1949 (principio di distinzione), ma anche applicare il principio di proporzionalità (Protocollo I del 1977, art. 51.5.b). Va considerato anche che il diritto internazionale è progredito nel tempo e ha previsto la repressione dei crimini internazionali attraverso la Corte Penale Internazionale, mettendo sempre più in evidenza la responsabilità della condotta militare, un aspetto affrontato per la prima volta nel 1945 dal processo di Norimberga. Questo principio non può essere ignorato nell'attivazione di nuove armi, cioè di macchine, ovviamente non responsabili a differenza dell'uomo. La responsabilità di un errore letale di un LAWS (ad esempio l'abbattimento di un aereo civile o la distruzione di uno scuolabus) non potrebbe essere addossata giuridicamente alla macchina. I seguenti interrogativi, sollevati dalla IA, sono in attesa di una risposta: in caso di errore la responsabilità dell'impiego delle armi autonome a chi dovrebbe essere indirizzata? Al programmatore dell'algoritmo, alla ditta costruttrice, all'azienda dell'indotto subfornitrice, agli addetti all'installazione, al personale incaricato della manutenzione, a chi ne ha deciso l'acquisto e la dislocazione, a chi ha approvato politicamente l'adozione, a un'azione avversaria di disturbo, a eventi imprevisi, a chi/che cos'altro? La catena delle responsabilità diviene talmente vaga ed indeterminata da lasciare inevasi gli interrogativi sull'adozione indiscriminata di tali armi.

Dando corpo a dubbi diffusi tra gli stessi militari del proprio e di altri paesi, nel 2021 il ministero della Difesa francese ha deciso di istituire un Comitato etico. Esso ha rimarcato la preoccupazione già espressa da singoli esponenti delle forze armate circa una loro eventuale perdita di controllo sul piano operativo e ha sottolineato come invece il comando debba continuare a rivestire un ruolo essenziale rispetto alla valutazione delle conseguenze causate dalle azioni letali messe in atto da un sistema di armi autonome. Anche nel documento intitolato *Future Operating Environment post 2035*, pubblicato dallo Stato maggiore dell'Esercito italiano, ricordato nel capitolo 8, viene riaffermato il principio secondo il quale deve essere mantenuto, sul piano operativo, il pieno controllo umano.

Come anticipato nel capitolo 9, le sfide poste dai LAWS sul piano della sicurezza internazionale hanno suscitato nella società civile e nella comunità scientifica un diffuso sentimento di preoccupazione, che si è tradotto in decise prese di posizione, spingendo anche i governi a confrontarsi in ambito multilaterale. Nei colloqui di Ginevra in materia di CCW, il dibattito tra le varie posizioni (chi assolutamente contrario, chi decisamente favorevole, chi

teso a cercare uno strumento operativo concreto) ha portato ad una serie di passi non trascurabili. Dal dibattito è emerso il concetto di «controllo umano significativo» (formula “CUS”), che ha suscitato un certo consenso presso le delegazioni governative, anche perché evita di disperdersi nella controversia su che cosa sia un LAWS, concentrandosi invece sul suo controllo e sui suoi diversi livelli. Come prospettato da Sharkey (2016) e da Amoroso e Tamburini (2019), lo schema indicato sarebbe il seguente: 1) la selezione dell’obiettivo da attaccare è integralmente effettuata dall’operatore umano; 2) la selezione dell’obiettivo da attaccare è effettuata dall’operatore umano in base a un ventaglio di opzioni suggerite dal sistema d’arma; 3) l’operatore umano si limita ad approvare o a rifiutare la scelta del sistema d’arma in merito all’obiettivo da attaccare; 4) l’operatore umano supervisiona la selezione dell’obiettivo effettuata dal sistema, mantenendo la possibilità di riprendere il controllo ed annullare l’attacco; 5) l’operatore umano si limita ad attivare il sistema d’arma, definendone la missione nella fase preliminare di pianificazione, senza avere la possibilità di intervenire nella fase operativa.

In sede di CCW la proposta di alcuni paesi per un mandato al GGE di negoziare uno strumento giuridico vincolante per tutti gli Stati, volto ad “assicurare un controllo umano significativo sulle funzioni critiche dei sistemi d’arma autonomi con effetti letali” appare oggi in una situazione di stallo. Durante la Sesta Conferenza di Revisione degli Stati parte della CCW, svoltasi a dicembre 2021, vi è stata opposizione ad una regolamentazione multilaterale soprattutto da parte di alcune grandi potenze (USA e Russia). Ciononostante, le ripetute sollecitazioni da parte di soggetti internazionali quali il Segretario generale delle Nazioni Unite, il Comitato della Croce Rossa Internazionale e la maggioranza degli Stati parte del CCW, di arrivare al conseguimento di obiettivi e risultati concreti.

#### **10.4. L’impegno della comunità scientifica e della società civile**

Già da prima, e prevedibilmente con maggiore convinzione in seguito alla guerra in Ucraina, la questione della IA applicata agli armamenti ha suscitato e susciterà l’attenzione e l’impegno della società civile. Ciò a partire dalla constatazione che, sebbene le armi completamente autonome ad oggi ancora non esistano, circolano tuttavia sistemi che vantano un notevole grado di autonomia nelle funzioni operative, logistiche e di combattimento.

Protagonisti dell’impegno della società civile sono state le comunità scientifiche, le associazioni e le organizzazioni non governative, alcune imprese e le istituzioni religiose. Nell’ultimo decennio hanno preso corpo numerose iniziative di sensibilizzazione in cui si sono ritrovati esperti, operatori

dei media e semplici cittadini. Esse hanno avuto il merito di coinvolgere governi a livello nazionale ed opinione pubblica sulla necessità di risposte alle sfide etiche, legali, tecniche e sociali sollevate da tecnologie belliche sempre più avanzate.

Come abbiamo visto nel cap. 9, già nel 2012 Human Rights Watch (HRW) aveva pubblicato un Rapporto intitolato *Loosing Humanity; the Case Against Killer Robots* in collaborazione con l'*International Human Rights Clinic* (IHRC) dell'Università di Harvard. Il Rapporto metteva in luce le possibili conseguenze di un futuro uso di armi completamente autonome, sottolineandone l'assoluta inadeguatezza a conformarsi ai principi e alle leggi del diritto internazionale umanitario. Secondo alcuni esperti come ad esempio Ron Arkin, professore di robotica presso il Georgia Institute of Technology, l'idea di progettare robot in grado di distinguere tra un target militare (legittimo) ed uno civile (illegittimo) comporterebbe enormi sfide tecnologiche. Basti considerare le difficoltà che incontrerebbe un robot nel riconoscere e differenziare un essere umano dall'ambiente circostante, un militare in divisa da un civile, e cosa più importante, un combattente da un non-combattente. Secondo il Rapporto di Human Rights Watch, l'introduzione di armi completamente autonome in un conflitto condurrebbe a difficili interpretazioni dei principi stabiliti dallo *jus in bello* come quello secondo il quale i combattenti durante le operazioni militari, oltre a dover risparmiare la vita dei civili, devono adottare misure atte ad evitare vittime tra gli stessi militari nemici non combattenti.

Nell'aprile 2013, venne lanciata la *Campaign to Stop Killer Robots*, costituita da una coalizione di circa centoquaranta Organizzazioni Non Governative a livello internazionale con il fine di mettere al bando le armi totalmente autonome. La Campagna chiede ai governi di tutto il mondo e alle Nazioni Unite di ratificare un Trattato internazionale che ne vieti l'utilizzo e soprattutto che venga tassativamente mantenuto il controllo umano nel ciclo decisionale (individuazione del bersaglio ed attacco). Grazie alla pressione della società civile, nello stesso 2013 si è svolto un primo incontro informale presso le Nazioni Unite di Ginevra. Nel 2016 molti Stati che facevano già parte della CCW, entrata in vigore nel 1983 con l'obiettivo di limitare l'utilizzo di "certe armi" durante i conflitti armati, hanno affermato l'intenzione di includere in agenda anche le armi totalmente autonome.

Anche tra le imprese si sono manifestati segni di interesse. Nel 2017 la Clearpath Robotics e Google, insieme ad oltre duecento aziende tecnologiche, hanno deciso di non supportare le ricerche della IA in ambito militare, chiedendo inoltre alle Nazioni Unite di vietare la produzione di simili armi. Nel giugno 2018 quattromila dipendenti di Google hanno aderito ad una petizione che chiedeva all'azienda di interrompere il Progetto Maven, controverso programma di ricerca in collaborazione con il Pentagono, che im-

plicava l'uso della IA in campo militare. Nella lettera veniva esplicitamente richiesto di cancellare il progetto e di provvedere a formulare una policy che impegnasse Google a non collaborare più allo sviluppo di tecnologie legate al mondo della difesa (*Campaign to Stop Killer Robots*, 2018).

Altresì chiara la posizione delle Nazioni Unite. In un discorso tenuto nella sede dell'ONU di Parigi nel 2019, il Segretario generale delle Nazioni Unite, Antonio Guterres, si è espresso a favore della realizzazione di un Trattato internazionale che vieti l'uso dei killer robot. Secondo Guterres, quelle macchine che hanno potere di decidere sulle vite degli esseri umani «sono politicamente inaccettabili e moralmente ripugnanti e dovrebbero essere vietate da una legge internazionale» (*Pax for Peace*, 2019).

In ogni caso, come ha evidenziato il cap. 9, il ruolo decisivo è rappresentato dalla comunità scientifica, spina dorsale delle analisi, della interpretazione e divulgazione dei dati e, non a caso, primo soggetto della società civile a raccogliere l'allarme della Campagna per fermare i robot killer. Nel 2015, circa 4.500 scienziati (tra cui Stephen Hawking, Yoshua Bengio e molti esperti della IA) hanno sottoscritto una lettera contro i sistemi d'arma letali autonomi. Il testo richiama l'attenzione sul fatto che, grazie alla tecnologia della IA, lo spiegamento di tali sistemi potrebbe avvenire nell'arco di pochi anni e non di decenni, con conseguenze del tutto imprevedibili e con il rischio di una corsa globale agli armamenti. Nella lettera vengono anche evidenziati i numerosi aspetti positivi, come ad esempio in campo medico, della IA. Nello stesso tempo, il suo impiego in campo militare può costituire una seria minaccia, rendendo urgente il divieto di mettere in campo armi prive di un significativo controllo umano.

Queste le criticità evidenziate nell'ambito etico, legale, operativo, della proliferazione e della sicurezza a livello globale, provocate dall'utilizzo in guerra di armi autonome:

1. una macchina non dovrebbe mai prendere decisioni totalmente autonome circa la vita e la morte di un essere umano.
2. Le armi autonome non sarebbero in grado di rispettare i principi di proporzionalità, distinzione e necessità militare, che sono alla base del diritto umanitario internazionale e che solo la coscienza umana è in grado di soddisfare.
3. Tali armi sono relativamente economiche e facili da copiare. Esiste un rischio molto elevato che, una volta prodotte, esse potrebbero facilmente essere utilizzate anche da attori non-statali (come ad esempio le milizie del c.d. Stato Islamico – IS)<sup>1</sup>.

<sup>1</sup> Nel 2016 l'I.S. ha portato a termine nel nord dell'Iraq il suo primo attacco realizzato con



4. Molti governi speculano poi sulla convinzione che tali armi porterebbero ad un numero minore di vittime. Al contrario, la conseguente sensazione di una attenuazione del rischio potrebbe rendere preferibile una soluzione militare rispetto ad una diplomatica, stravolgendo quindi il millenario concetto di guerra teorizzato da Sun Tzu (2010) secondo cui «il governante accorto è solo colui che risulta vittorioso non combattendo alcuna guerra».
5. Le armi totalmente autonome rischiano di creare un pericoloso vuoto riguardo alle responsabilità nel caso, ad esempio, dell'uccisione di un civile. Nel 2016 il progetto di ricerca *Moral Machine* del Massachusetts Institute of Technology (MIT) ha coinvolto due milioni e trecentomila persone in 233 paesi. Esso ha mostrato come i principi morali cambino da paese a paese, così come le preferenze soggettive che risultano condizionate dalle variabili sociali, culturali, economiche e religiose; in Giappone e in Finlandia, ad esempio, si è più propensi a sacrificare un pedone che non attraversa sulle strisce, mentre in Nigeria oppure in Pakistan lo stesso pedone avrebbe molte più possibilità di sopravvivenza (Santagata, Melegari, 2018). La situazione si complicherebbe ulteriormente in un ipotetico scenario di guerra, nel caso in cui un sistema d'arma autonoma in avaria, del valore di milioni di dollari, si trovasse nella situazione di dover scegliere di schiantarsi su una montagna oppure di atterrare nel centro di una cittadina mettendo a repentaglio la vita di molti civili.
6. L'impiego sempre più preponderante della tecnologia nei conflitti armati rischia di determinare una corsa agli armamenti con effetti significativi sulla pace e sulla sicurezza mondiali. Inoltre esso permetterebbe ai ministeri della Difesa ed alle aziende produttrici di questi sistemi d'arma di accedere a milioni di dati personali, con il rischio di violare il diritto alla privacy di milioni di persone e con il pericolo di subire attacchi cyber di natura criminale in grado di generare una catastrofica guerra planetaria. Nel giugno del 1997 venticinque funzionari della NSA (National Security Agency) avevano “bucato” le reti informatiche del Dipartimento della Difesa statunitense, permettendo al Read Team (nome in codice dei venticinque funzionari) di penetrare il sistema di sicurezza americana in soli quattro giorni (Accoto, 2019).

Anche nel nostro Paese gli scienziati si sono posti alla testa del movimento di opinione. Nel marzo 2019 centodieci ricercatori italiani hanno lanciato un appello al Governo e al Parlamento italiani affinché assumano un'iniziativa in ambito internazionale per il divieto di sistemi d'arma letali

un drone, uccidendo, due combattenti Peshmerga (Warrick, 2017). Nel 2017 il gruppo terroristico annunciava la formazione del primo “Unmanned Aircraft of the Mujahedden”.

autonomi. Il testo dell'appello elaborato, con il contributo degli esperti dell'Unione Scienziati Italiani per il Disarmo-USPID, evidenzia il fatto che, se da una parte l'uso della IA apporta significativi benefici sociali ed economici in molti settori, dall'altra, qualora applicata agli armamenti, costituirebbe una potenziale minaccia dal punto di vista sia del diritto umanitario, sia della sicurezza globale.

In occasione dell'Appello, in sintonia con l'azione della Rete Italiana Pace e Disarmo di cui è parte, Archivio Disarmo ha dato vita a una serie di iniziative di ricerca e sensibilizzazione in accordo e con il sostegno della *International Campaign to Stop Killer Robots*. Attraverso rilevazioni sociologiche (sondaggio di opinione, focus group), conferenze, dibattiti, seminari universitari e lezioni nelle scuole è stato espresso un significativo sforzo di coinvolgimento dell'opinione pubblica soprattutto giovanile. L'obiettivo è di accrescere la consapevolezza sulle implicazioni morali, legali e politiche dei LAWS, promuovendo azioni di advocacy affinché una discussione approfondita sull'argomento entri al più presto nell'agenda politica italiana.

Un altro soggetto importante nel movimento di opposizione delle armi autonome è costituito dalle istituzioni religiose. Per quanto riguarda la Chiesa cattolica<sup>2</sup> è da segnalare il manifesto *Rome Call for AI Ethics*,<sup>3</sup> firmato a Roma nel febbraio 2020 dal presidente della Pontificia Accademia per la Vita, monsignor Vincenzo Paglia, dal vicepresidente dell'Ibm John Kelly III, dal presidente di Microsoft Brad Smith, dal direttore generale della Fao Dongyu Qu e dalla ministra dell'Innovazione tecnologica e della digitalizzazione, Paola Pisano. Il documento è nato per supportare un approccio etico alla IA promuovendo un senso di responsabilità condivisa tra organizzazioni, governi e istituzioni. L'obiettivo è garantire un futuro in cui il progresso tecnologico in generale e la IA in particolare, frutto dell'ingegno e della creatività umana, siano al servizio del benessere della persona e del miglioramento della convivenza sociale, senza per questo sostituirsi al discernimento umano.

Nel gennaio 2021, l'iniziativa della Pontificia Accademia per la Vita ha ricevuto un riconoscimento internazionale nel prestigioso *AI Index Report*, la pubblicazione annuale dell'Institute for Human-Centered-HAI dell'Università di Stanford. Che ha sottolineato come l'uso etico delle tecnologie della IA sia stato uno dei temi di attualità più trattati e discussi del 2020.

<sup>2</sup> È del 2018 la prima condanna da parte del Vaticano del possibile uso di armi letali autonome, che renderebbero la guerra "ancora più inumana" sul presupposto che qualsiasi nuova tecnologia deve essere compatibile con la giusta concezione dell'essere umano, primo fondamento della legge e dell'etica (<https://www.vaticannews.va/it/vaticano/news/2018-04/santa-sede-onu-armi-jurkovic0.html>).

<sup>3</sup> <https://www.romecall.org/>

Sempre nel 2020 l'organizzazione ecumenica Pax, scaturita dalla cattolica Pax Christi Olanda, ha pubblicato il Rapporto *Save your university from killer robots* (Pax, 2020). In esso viene evidenziato il fondamentale ruolo delle università nei generosi approfondimenti e discussioni all'interno delle classi sull'impatto delle nuove tecnologie nonché l'invito ad organizzare eventi sul tema dei killer robot.

Il profondo impatto della tecnologia sull'ambiente, sulla società e sulla vita di milioni di persone negli ultimi anni ha generato, all'interno della società civile, una riflessione critica sul concetto di *disumanizzazione*, un fenomeno che si verifica nel momento in cui le nostre identità vengono prima analizzate attraverso lo sviluppo di complessi algoritmi e successivamente abbinate ad un modello pre-programmato in base alle nostre caratteristiche fisiche e scelte personali. L'introduzione di forme sempre più pervasive della IA nella realtà che ci circonda rischia di consolidare disuguaglianze sociali già radicate nella società. Gli sviluppi nel campo dell'automazione riguardano anche i sistemi di arma moderni, i quali sono sempre più sofisticati, costosi e distruttivi. Nel novembre 2021, Amnesty International e la Campagna Stop Killer Robots hanno lanciato un filtro per Instagram e Facebook chiamato «Escape the scan» che utilizza la tecnologia della realtà aumentata (AR) al fine di mostrare che esistono armi in corso di sviluppo in grado di usare la tecnologia del riconoscimento facciale, i sensori di movimento e una capacità di colpire bersagli senza che vi sia un controllo umano significativo<sup>4</sup>. Quanto alla tecnologia del riconoscimento facciale – che ad oggi non è in grado di riconoscere donne, persone di colore e quelle con disabilità – se fosse impiegata in un campo di battaglia, oppure dalle forze dell'ordine o per il controllo delle frontiere, esporrebbe a palesi violazioni dei principi del diritto internazionale umanitario, sia alla possibilità di dare vita a sistemi di oppressione e repressione difficilmente controllabili.

Nell'aprile 2022, la Campagna Stop Killer Robots ha presentato il documentario intitolato *Immoral Code*, che affronta il tema della pervasività della tecnologia nella vita di ogni essere umano. Esso pone una serie di domande “scomode”, che hanno il merito di mostrare come la complessità dell'esistenza umana non possa essere risolta semplicemente con una serie di algoritmi e che ridurre le decisioni umane a processi automatizzati solleva molti dubbi etici e giuridici<sup>5</sup>.

Tuttavia, come abbiamo visto in precedenza, nonostante l'impegno della società civile e la richiesta da parte di ben sessantasei Stati di avviare ne-

<sup>4</sup> <https://www.amnesty.it/amnesty-international-e-stop-killer-robots-siamo-ancora-in-tempo-per-fermare-i-killer-robots/>

<sup>5</sup> <http://immoralcode.io/>

goziati su uno strumento giuridicamente vincolante, nel dicembre 2021 la Sesta Conferenza di revisione della CCW si è rivelata una delusione rispetto alle aspettative. Infatti un sostanziale blocco è stato messo in atto da Stati Uniti, Russia ed Israele, che considerano prematura la creazione di uno strumento giuridico vincolante.

Il ruolo della società civile diventa quindi essenziale per sollecitare i governi mondiali e le istituzioni intergovernative a votare un mandato che si possa tradurre, il più velocemente possibile, in un Trattato con valore legale. La creazione di una rete internazionale formata da ricercatori delle scienze naturali, sociali e umanistiche ha permesso la circolazione di report e documenti consultabili da esperti così come da comuni cittadini con la possibilità, per questi ultimi, di venire a conoscenza delle problematiche che caratterizzano la IA applicata alle armi.

Gli umani devono rimanere autori e controllori della tecnologia, in grado di prevenire le contraddizioni e gli squilibri di potere che la tecnologia stessa dovesse esacerbare. L'obiettivo è contrastare la disumanizzazione digitale per evitare un futuro in cui le macchine possano prendere decisioni sulla vita e sulla morte di esseri umani. Anche coloro che sono incaricati di una funzione complessa e delicata come la Difesa – cioè i militari – non sono esonerati dal partecipare a questo processo, tutt'altro. Essi sono chiamati a portare la loro esperienza e la loro competenza per prevenire un futuro nel quale il controllo fosse non più delle persone sulle macchine, ma delle macchine sulle persone. Ciò che aprirebbe la strada a scenari strategici doppiamente apocalittici.

## Riferimenti bibliografici

- Accoto C. (2019), *Mondo ex Machina. Cinque brevi lezioni di filosofia dell'automazione*, Egea Editore, Milano.
- Amnesty International (2021), *Siamo ancora in tempo per fermare le macchine assassine*, testo disponibile al sito: <https://www.amnesty.it/amnesty-international-e-stop-killer-robots-siamo-ancora-in-tempo-per-fermare-i-killer-robots/>
- Amoroso D. e Tamburrini G. (2019), *What makes human control over weapon systems “meaningful”*, Working paper #4, International Committee for Robots Control, testo disponibile al sito: <https://www.icrac.net/research/>
- Business Standard.com (2022), *Global artificial intelligence spending to reach \$434 bn in 2022: Report*, February, testo disponibile al sito: [https://www.business-standard.com/article/technology/global-artificial-intelligence-spending-to-reach-434-bn-in-2022-report-122022000195\\_1.html](https://www.business-standard.com/article/technology/global-artificial-intelligence-spending-to-reach-434-bn-in-2022-report-122022000195_1.html)
- Human Rights Watch (2012), *Loosing Humanity. The Case against killer robots*, testo disponibile al sito: [https://www.hrw.org/sites/default/files/reports/arms\\_1112\\_ForUp\\_load.pdf](https://www.hrw.org/sites/default/files/reports/arms_1112_ForUp_load.pdf)

- IDC (2022), *Forecasts Companies to Increase Spend on AI Solutions by 19.6% in 2022*, testo disponibile al sito: <https://www.idc.com/getdoc.jsp?containerId=prUS48881422>
- Pascolini A. (2019), “Nuove Wunderwaffen: i missili ipersonici”, *Scienza e ricerca*, testo disponibile al sito: <https://ilbolive.unipd.it/blog-page/nuove-wunderwaffen-missili-ipersonici>.
- Pascolini A. (2020), “Armi ipersoniche”, *IRIAD Review*, n. 12, Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD.
- Pax for Peace (2019), *Breakthrough: Dutch parliament calls for international rules on killer robots*, testo disponibile al sito: <https://paxforpeace.nl/news/overview/breakthrough-dutch-parliament-calls-for-international-rules-on-killer-robots>
- Pax for Peace (2019), *State of AI, Artificial Intelligence, the military and increasingly autonomous weapons*, testo disponibile al sito: <https://paxforpeace.nl/media/download/state-of-artificial-intelligence--pax-report.pdf>.
- Pax for Peace (2020), *Save your University from killer robots*, testo disponibile al sito: <https://paxforpeace.nl/media/download/pax-booklet-save-your-university-form-killer-robots.pdf>
- Raviart M. (2018), *Onu: la Santa Sede condanna l'uso di robot automatici in guerra*, testo disponibile al sito: <https://www.vaticannews.va/it/vaticano/news/2018-04/santa-sede-onu-armi-jurkovic0.html>
- Santagata E. e Melegari A. (2018), “Come dovrebbero ragionare le armi autonome del futuro?”, *Analisi e Difesa*, testo disponibile al sito: <https://www.analisi-difesa.it/2018/10/come-dovrebbero-raionare-le-armi-autonome-del-futuro>
- Say M. (2022), “AI investments soared in 2021, but big problems remain”, *Artificial Intelligence*, testo disponibile al sito: <https://www.techrepublic.com/article/ai-investments-soared-2021-big-problems-remain/>.
- Schlosser E. (2015), *Comando e controllo. Il mondo a un passo dall'apocalisse nucleare*, Mondadori, Milano.
- Stanford.edu (2022), “The AI Index Report. Measuring trends”, *Artificial Intelligence*.
- Statista.com (2022), *Projected artificial intelligence spending in Europe in 2019, 2020, and 2023*, testo disponibile al sito: <https://www.statista.com/statistics/1115464/ai-spending-europe/>
- Sun Tzu e Sun Pin (2010), *L'arte della Guerra*, tr. it. Neri Pozzi Editore, Vicenza.
- Warrick J. (2017), *Use of weaponized drones by ISIS spurs terrorism fears*, *Washington Post*, 21 febbraio 2017, testo disponibile al sito: [https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401\\_story.html](https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html)



## Appendice. I principali modelli di LAWS

di Michael Malinconi, Juan Carlos Rossi

### Munizioni *loitering*

**AEROVIRONMENT SWITCHBLADE:** ampiamente utilizzato dalle truppe americane in Afghanistan, è stato rilevato anche in Iraq e Siria. Progettato per la rapida sorveglianza e la ricognizione su un obiettivo BLOS (*Beyond line of sight*) fino a 10 km di distanza, può anche garantire una soluzione di attacco con una testata esplosiva da 40 mm. Sono stati prodotti diversi modelli e può essere azionato manualmente o autonomamente.

**ASN-301:** definito come un sistema mobile antiradiazioni che presenta molte similitudini con il modello israeliano Harpy<sup>1</sup>, fa parte dell'arsenale cinese insieme ai CH-901 e i WS-43.

**HARPY:** prodotta dalla IAI (Israel Aerospace Industries) è capace di volare e aspettare il momento giusto per attaccare il bersaglio anche per più di due ore e fino a 500 chilometri di distanza. È stato pensato per fornire agli operatori un controllo fino all'ultimo minuto, inclusa la possibilità di cessare l'attacco in qualunque fase.

**KARGU:** è unUCAV ad ala rotante, ideato per scenari di guerre asimmetriche o operazioni antiterrorismo in quanto può rispondere in maniera rapida contro obiettivi fissi e mobili. La STM, società di proprietà statale turca, sta attualmente implementando le capacità del suo bombardamento tramite l'utilizzo della IA, compreso il riconoscimento facciale. Attraverso l'inserimento delle coordinate del bersaglio, è in grado di sviluppare un'autonoma capacità di *fire and forget*<sup>2</sup>. È stato schierato in Siria e Libia.

**KYB:** La Zala Aero, sussidiaria del gruppo Kalashnikov è l'unica compagnia a sviluppare UAV per la Russia, e ha presentato i suoi modelli *loitering* KYB e Lantset (PAX, 2019a, p. 23-24).

**ORBITER 1K MUAS:** utilizza una testata a frammentazione esplosiva con palline di tungsteno per colpire oggetti fisici o umani. Pur con una modalità *man in the loop*, una volta lanciato può scovare, tracciare e attaccare bersagli in completa

<sup>1</sup> Israele ha venduto il "drone suicida" Harpy alla Cina negli anni '90. Fonte disponibile anche a [www.israeldefense.co.il/en/node/28716](http://www.israeldefense.co.il/en/node/28716).

<sup>2</sup> Modalità di guida missilistica che non richiede ulteriori istruzioni dopo il lancio.

autonomia. Possiede una durata di due ore e mezza con un raggio d'azione superiore ai 100 km. Come gli Herop, questi mezzi sono stati fondamentali nella vittoria azera nella guerra in Nagorno-Karabakh dell'autunno 2020.

SKYSTRICKER: prodotto da Elbit Systems, possiede una lunga autonomia ed elevata velocità. Dispone di un sistema di navigazione autonoma durante le diverse fasi e può essere bloccato su un bersaglio dall'operatore mediante un sensore elettro-ottico.

WARMATE 2: prodotta dalla polacca WB Electronics, il lancio avviene tramite una catapultata con una testata anticarro, anti-implosione (termobarica). A quest'ultimo modello, è stata aggiunta una termocamera a infrarossi nella fusoliera, consentendo così non solo il target automatico, ma anche la possibilità di valutare un obiettivo prima di colpirlo.

## **Sistemi d'arma ravvicinati o a corto raggio (CIWS)**

CENTURION C-RAM: il Counter-Rocket, Artillery, Mortar, sviluppato in parte da Northrop Grumman, è stato inizialmente pensato per proteggere le basi statunitensi in Iraq. Il C-RAM, in realtà, è la versione terrestre del Phalanx e per questo presenta funzioni simili, come la cadenza di tiro e il tipo di cannone. Tra i due modelli, tuttavia, sussistono alcune differenze significative. Il C-RAM adopera la *forward looking infrared*, tecnologia di visione basata sulla rilevazione della radiazione infrarossa, e i suoi proiettili hanno una probabilità maggiore di causare danni collaterali se mancano il bersaglio. Per questo, a differenza della sua controparte, i suoi proiettili si autodistruggono prima di colpire il suolo.

Generalmente, detiene un tasso di abbattimento del 60-70%.

DARDO: prodotto dalle italiane Breda e Oto Melara, è equipaggiato con cannoni binati da 40 mm. Le sue ingenti dimensioni e il costo hanno scoraggiato la sua vendita all'estero. È capace di sparare 600-900 colpi al minuto.

GOALKEEPER SGE30: progetto congiunto tra l'olandese Signaal e la statunitense General Electric è ora di proprietà di Thales Nederland. Introdotto inizialmente alla fine degli anni '70, ha avuto diversi upgrade. Questo CIWS è un'arma ravvicinata contro missili e aerei con sette canne da 30 mm e una cadenza di tiro di 4 200 colpi al minuto. Il sistema esegue automaticamente sia il processo della sorveglianza sia quello della rilevazione. Può tracciare fino a trenta obiettivi per poi selezionarne i quattro più pericolosi ed ingaggiarli con una velocità di circa 0,2 secondi per obiettivo. Thales sta migliorando le capacità opto-elettriche del sistema e i suoi algoritmi.

IRON DOME: Israele, vivendo sin dalla sua nascita una situazione di insicurezza territoriale, dal 2011 presidia i confini con i suoi Iron Dome, dotati di venti missili intercettori Tamir della Rafael. Pensato come contromisura difensiva al lancio di razzi balistici a corto raggio dalla Striscia di Gaza, Libano, Siria e dalla Penisola del Sinai (Rossi, 2016) è capace di intercettare minacce a corto raggio in un range compreso tra i 3 e i 72 km in tutte le situazioni meteo. Si basa su tre componenti essenziali: un radar EL/m-2081 in grado di individuare i razzi e tracciarne la traiettoria; un sistema di gestione BMC capace di determinare dove atterrerà l'ordigno, valutarne la minaccia e calcolare il punto d'impatto in aria e l'unità mobile di lancio dei



missili, composto da venti missili Tamir per batteria dotati di sensori elettro-ottici, guida GPS e otto pinne per virare in aria. Per ogni minaccia da intercettare, vengono lanciati due Tamir, uno per aprire la zona d'impatto e l'altro per distruggere la minaccia.

**NBS MANTIS:** già operativi e schierati dalla Germania in Afghanistan a protezione delle proprie basi, sviluppato da Rheinmetall Air Defence, per la difesa aerea, è dotato di un sistema di controllo a terra, due sensori e sei Oerlikon Millennium Guns da 35 mm altamente automatizzati.

**PANTSIR-M:** questo CIWS russo ha sostituito gli obsoleti modelli sovietici AK-630 e 3K87 Kortik. Può tracciare bersagli aerei di varia natura fino a 40 km di distanza ed ingaggiarli entro 20 km dall'unità navale su cui è imbarcato. Possiede otto missili terra-aria e due cannoni GSh-6-30K a canne rotanti capaci di generare una potenza di fuoco pari a 10 000 colpi al minuto. È un sistema completamente automatizzato, basato su sistemi di guida elettro-ottici e radar, che non richiede l'utilizzo di un operatore benché vi sia la possibilità di essere controllabile. Il tempo di reazione ad una minaccia rilevata dal sistema è tra i 3 ed i 5 secondi.

**PHALANX MK15/16:** progettato da Raytheon Systems Company per l'US Navy, di cui è diventato un modello standard anche per il suo apparato semplice e relativamente economico. Si presume che siano stati sperimentati anche in forma offensiva dagli Stati Uniti già quaranta anni fa. Possiede sei cannoni rotanti da 20 mm e una cadenza di tiro di 4 500 colpi al minuto. Un suo limite è la mancanza del sistema identificativo *friend or foe* (IFF), poiché si basa esclusivamente sui dati radar per distinguere oggetti ostili o amici.

**TYPE 730:** CIWS cinese progettato per difesa navale ravvicinata, la variante 730 possiede una mitragliatrice Gatling con sette canne rotanti da 30 mm e una cadenza di tiro di 5.800 colpi al minuto mentre la variante 1130 ne possiede undici con 10.000 colpi al minuto. Inoltre, la Repubblica Popolare ne sta sviluppando un nuovo modello con venti canne rotanti per le sue unità navali.

## **Unmanned Combat Aerial Vehicles (UCAV)**

**BAE SYSTEMS TARANIS:** Nel 2010 il Regno Unito ha presentato questo prototipo di aereo da combattimento autonomo senza pilota invisibile ai radar definito come il velivolo dimostrativo tecnologicamente più avanzato mai costruito, con uno stanziamento di 185 milioni di dollari. Il Taranis sarebbe in grado di raggiungere un'area predefinita tramite una traiettoria programmata per identificare e mirare automaticamente al bersaglio. I dati raccolti vengono inviati all'operatore che poi concede il via libero per l'attacco. Può essere controllato via satellite da qualunque parte nel mondo ed è progettato per missioni intercontinentali. Se armato, inoltre, è in grado di colpire con precisione bersagli a lunga distanza sia in aria sia sul suolo.

**MQ-8C FIRE SCOUT:** definito come l'elicottero autonomo di prossima generazione della Marina americana, è in grado di eseguire compiti di intelligence, sorveglianza, ricognizione e acquisizione del bersaglio (ISR&T) tramite un puntatore laser in tempo reale. A contraddistinguerlo non sono né la sua autonomia di 12 ore, né

la sua velocità massima di 135 nodi, ma la sua capacità di decollare e atterrare autonomamente su qualsiasi nave o zona di sbarco anche non adeguatamente predisposta. Un miglioramento significativo che ha di fatto aumentato anche la sua portata e la sua resistenza (più del doppio) oltre alla capacità di carico utile (più del triplo) rispetto alla versione precedente MQ-8.

nEUROn: Grecia, Francia, Italia, Spagna, Svezia e Svizzera nel 2006 hanno iniziato a sviluppare il programma di droni nEUROn<sup>3</sup>. Sviluppato nell'ambito di un programma dimostrativo da 405 milioni di euro è progettato dalla francese Dassault con il supporto di Leonardo. Ha visto il suo primo volo nel 2012. Con capacità autonoma di attacco aria-suolo, è progettato per portare due bombe da 250 kg a guida laser contenute nella stiva interna. È classificato come il sistema d'arma più autonomo attualmente in fase di sviluppo. Inoltre, nel 2015 Germania, Francia, Spagna e Italia hanno firmato un accordo per la progettazione di un euro-drone, chiamato EuroMALE, tutt'oggi in fase di studio<sup>4</sup>.

SHARP SWORD GJ-11/ S-70 OKHOTNIK-B: UAV di sesta generazione con tecnologia stealth, hanno un raggio d'azione tra i 4 000 e i 6.000 km e velocità di 1.000km/h. Possono trasportare fino a due tonnellate di munizioni. Questi due modelli sono esempi di come anche la Cina e la Russia prestino molta attenzione agli sviluppi in questo campo.

X-47B: progettato per lanci carrier-based, il programma X-47 della DARPA, impiega tecnologie già note come il GPS, tecnologia stealth, l'autopilota, sistema di comunicazione Link 16 e sistema anticollisione. La sua caratteristica principale risiede nella capacità di auto-rifornimento in volo, tecnologia attualmente esclusivo appannaggio della Northrop Grumman, la quale permette così di aumentare non solo il suo range, ma anche la sua durata e la sua flessibilità operativa, sebbene sia attualmente progettato solo per compiti di intelligence, sorveglianza e ricognizione. A maggio del 2015 il programma per i test di collaudo è stato dichiarato completato, portando il progetto in stand-by.

## **Munizioni guidate di precisione**

AGM-158C LRASM (Long-Range Anti-Ship Missile): È un missile cruise anti-nave a lunga gittata, armato di un penetratore e di una testata a frammentazione esplosiva, in grado di localizzare ed eliminare eventuali minacce attraverso il radar in tutte le condizioni atmosferiche. LoAGM-158C è anche in grado di colpire obiettivi terrestri. È progettato per volare per centinaia di chilometri, sfuggire ai radar e operare senza contatto radio con il personale di controllo. Mentre il Pentagono sostiene che si tratti di un missile semi-autonomo, ovvero incapace di selezionare il bersaglio ma solo di attaccarlo, dubbi rimangono su come l'arma decida di ingaggiare gli obiettivi.

<sup>3</sup> L'Italia, tramite Leonardo e con un esborso di 90 milioni di euro, è il secondo maggior contributore del progetto dopo la Francia.

<sup>4</sup> Progettato in collaborazione da Leonardo, Dassault Aviation ed Airbus.

DUAL-MODE BRIMSTONE: la maggior parte delle munizioni guidate in realtà fa affidamento su dati preassegnati per rintracciare e colpire i bersagli. L'autonomia dell'arma dunque non è relativa alla selezione del target, ma piuttosto all'esecuzione dell'attacco. Questo missile di precisione da attacco terra-aria a guida laser prodotto da MBDA<sup>5</sup> viene, invece, identificato come una delle poche munizioni guidate con un certo grado di autonomia nella selezione del bersaglio. A differenza dei normali missili guidati, ma come i JSM/NSM, viene loro assegnato una determinata area, nella quale avranno il compito di individuare bersagli che corrispondono ad un modello predefinito.

JSM: il Joint Strike Missile sviluppato da Kongsberg Defence & Aerospace è un missile cruise di quinta generazione, pensato per essere integrato in diversi veicoli da combattimento, compreso l'F-35. Ha un riconoscimento del bersaglio autonomo, reso possibile da un seeker di immagini a infrarossi. Tra le sue caratteristiche vi è un sistema avanzato di pianificazione del coinvolgimento ed un collegamento di dati di reti bidirezionale con funzionalità di aggiornamento del target, re-target ed interruzione missione. A differenza della maggior parte degli attuali missili guidati, i JSM non sono assegnati ad un bersaglio specifico, bensì ad un'area dove avranno il compito di scovare obiettivi predefiniti.

MIM 104 PATRIOT: è stato uno dei primi sistemi d'arma ad introdurre l'autonomia. Operativo nell'esercito americano già dal 1984, il sistema di difesa missilistico conta ben quattro funzioni operative (sorveglianza radar, command and control, comunicazione e guida del missile) che lavorano insieme per rilevare, identificare e abbattere missili balistici tattici, missili cruise, droni e altre minacce. L'ingaggio del bersaglio può essere effettuato in modalità manuale, semi-automatica o automatica.

MK 48 MOD 6 AT: modello degno di nota, il siluro pesante che con continui upgrade è stato progettato per un'efficacia ottimale contro tutti gli obiettivi sia in ambienti costieri sia in acque profonde. È dotato di un sonar e segnale digitale avanzati. La guida e il controllo basati su software consentono operazioni autonome e tattiche di *fire and forget*, insieme a un ingaggio simultaneo sia di più bersagli multipli sia di attacchi ravvicinati.

S-400 TRIUMPH: sistema missilistico russo progettato e sviluppato da Almaz-Antey con un'elevata capacità contro minacce aeree e missilistiche. Con una risposta inferiore ai 10 secondi, il sistema può individuare 36 obiettivi contemporaneamente in un raggio che va dai 40 ai 400 km. Ogni batteria, infatti, montata su un vettore, dispone di quattro differenti missili guidati che con la loro diversa gittata possono essere combinati per ottimizzare la sua capacità di intercettare la minaccia in arrivo. LoS-400 è in grado di rilevare e intercettare molteplici velivoli: bombardieri strategici, velivoli radar, aeromobili per la guerra elettronica, aerei da trasporto tattici, missili balistici e missili cruise di tutte le dimensioni. Sono in servizio alle forze armate russe dal 2007.

SeaRAM: è un sistema missilistico di difesa contro minacce subsoniche, supersoniche, missili cruise, droni ed elicotteri. Combina precisione, un esteso range ed un'elevata manovrabilità con una rapida e affidabile risposta. Il SeaRAM è in grado

<sup>5</sup> Una joint venture composta dai tre leader europei nel settore aerospaziale e della difesa: Airbus (37,5%), BAE Systems (37,5%) e Leonardo (25%).

di rilevare, localizzare e coinvolgere in modo autonomo i bersagli nemici, con un'elevata capacità di colpire più bersagli contemporaneamente, attraverso l'uso di una radio frequenza passiva automatizzata dual-mode e a guida a infrarossi.

## Unmanned Ground Vehicles (UGV)

ARMATA T-14: il super carro armato orgoglio delle forze armate russe, è stato pensato per il controllo da remoto ed è in fase di sviluppo una sua variante completamente autonoma.

GLADIATOR: concepito e sviluppato dagli Stati Uniti (NREC & BAE Systems) negli anni '90, come supporto ai Marines durante le operazioni STOM<sup>6</sup>, è un veicolo tattico a sei ruote e dispone di supporti per mitragliatrici M249 e M240G ed armi d'assalto multiuso. Prevede un'opzione anche per l'utilizzo di armi non letali. Sebbene sia stato sviluppato comprendendo una cabina di controllo per l'operatore, è stato definito il primo robot da combattimento multiuso al mondo.

I-MPUGV: la Corea del Sud, attraverso la Hanwha Defense, ha sviluppato questo modello a guida autonoma, totalmente elettrico, basato su tecnologia AI ed equipaggiato con una base di fuoco controllata da remoto. Pensato per offrire supporto ravvicinato alle unità di fanteria, è capace, inoltre, di localizzare la provenienza di fuoco tramite segnali acustici.

K9A3 THUNDER: il K9 Thunder è attualmente il più iconico pezzo d'artiglieria semovente al mondo. Prodotto dalla sudcoreana Hanwha Defense, è in uso al confine tra le due Coree. Possiede cannoni da 155 mm e una gittata superiore ai 40 km. La sua nuova variante A3 punta a renderlo totalmente autonomo tramite l'intelligenza artificiale.

MISSION MASTER: l'UGV della tedesca Rheinmetall rientra in una categoria più ampia. Oltre alle versioni cargo e di sorveglianza, dispone di una vasta gamma di opzioni nel suo arsenale, tra cui una con due lanciarazzi realizzata da Thales con otto missili da 70 mm ciascuno. Il Mission Master ha un'autonomia di otto ore e una velocità massima di 30 chilometri l'ora.

NEREKTHA: piccolo veicolo da combattimento autonomo già in dotazione alle forze russe, può raggiungere autonomamente un bersaglio in modalità silenziosa per poi esplodere e distruggere carri armati nemici o addirittura interi edifici.

ROBATTLE LR-3: l'UGV della IAI è stato pensato per operazioni di combattimento ravvicinato e può essere equipaggiato con diversi tipi di armi, tra cui il Pitbull, un *Remote Weapon Station* (RWS) sviluppato da General Robotics. Può anche supportare missioni ad ampio raggio di intelligence, sorveglianza, acquisizione del bersaglio, ricognizione e protezione di convogli. Secondo l'azienda il sistema può operare anche in modo autonomo a diversi livelli nonostante attualmente funzioni a controllo remoto.

<sup>6</sup> La manovra *Ship to Objective* (STOM) è un concetto tattico che può essere applicato a tutti i tipi di operazioni anfibe, specie assalti e raid, ma in genere implica il superamento di ostacoli allo sbarco.

SHADOW RIDER: prodotto dalla turca FNSS, è equipaggiato con una torretta telecomandata da 25 mm e una capacità di carico di quattro tonnellate. L'IA ne ha significativamente aumentato l'autonomia. Non detiene ancora capacità di fuoco diretto.

SHARP CLAW I: Norico, società cinese, sta cercando di aprire la strada cinese nel settore dei UGV, sviluppando il suo cingolato leggero Sharp Claw I. Dotato di una stazione d'arma a controllo remoto con una mitragliatrice e un paio di lancia-razzi. Pur con alti livelli di autonomia, mantiene sempre un operatore al comando.

THEMIS ADDER: presentato nel 2015, il sistema cingolato estone, prodotto da Milrem, è un veicolo terrestre senza equipaggio, provvisto del sistema di armi remote ST Kinetics Adder (Singapore Technology), in grado di trasportare diversi tipi di mitragliatrici. Integrato con un sistema di tracciamento video, che gli consente il coinvolgimento di obiettivi fissi e mobili. L'Adder offre anche telecamere diurne e notturne, un telemetro laser e un sistema di munizione da 40 mm opzionale. Un sistema a controllo autonomo installato nell'UGV provvede ad una verifica autonoma in tempo reale capace sia di evitare gli ostacoli, sia di dirigere il mezzo lungo il percorso/obiettivo desiderato.

URAN 9: prodotto da JSC 766 UPTK, è un carro armato leggero senza pilota prodotto in massa, dotato di una mitragliatrice calibro 30 mm e missili guidati anti-carro, è stato schierato in Siria dove l'esperienza in combattimento ha portato a un suo ulteriore aggiornamento.

## Unmanned Marine Vehicles (UMV)

AN2-ANACONDA: ideato per le operazioni di superficie vicino alla costa senza equipaggio, è in grado di trasportare fino a cinque sistemi d'arma. L'USV Anaconda interamente in alluminio è una nave autonoma prodotta da Swiftships Shipbuilders che offre funzionalità avanzate di sorveglianza e ricognizione, identificazione e intercettazione. Il concetto di base è quello di sviluppare un'imbarcazione in grado di navigare autonomamente tramite l'ausilio di sensori e un GPS. Con l'IA dovrebbe diventare una imbarcazione completamente autonoma ed eseguire così manovre tattiche ed evasive in una determinata area per lunghi periodi di tempo, il tutto senza bisogno di alcun intervento umano.

JARI: anche la Cina ha mostrato interesse nel campo degli UMV: infatti, si contano già in sviluppo diversi modelli di veicoli di superficie, come lo JARI per operazioni antisommersibile, anti-superficie e antiaerea, veicoli subacquei senza pilota (UUV) e una nuova serie di grandi sottomarini senza pilota. A questo proposito il "Progetto 912", un programma classificato, dovrebbe essere preposto all'elaborazione di robot subacquei militari di nuova generazione (Saalman, 2019, p. 44-45).

POSEIDON: al fine di compensare lo svantaggio navale nei confronti degli Stati Uniti, la Russia, mira a produrre dei veicoli subacquei senza pilota. Il Poseidon (nome in codice Uran-6), è una piattaforma autonoma senza pilota a propulsione nucleare con portata intercontinentale (*ivi*, p. 41).

SEAGULL: considerato il primo sistema senza pilota al mondo per le missioni

ASW e antimine (mine countermeasure- MCM), il SeaGull può eseguire missioni in acque profonde per quattro giorni di fila fino ad una distanza visiva di 100 km, riducendo i rischi per la vita umana e riducendo drasticamente i costi di approvvigionamento e operativi. L'USV può essere controllato da un unico *mission control system* (MCS) ed è disponibile in modalità con o senza pilota. Questa imbarcazione può inoltre essere impiegata anche in missioni di intelligence, sorveglianza e ricognizione, guerra elettronica, sicurezza marittima e idrografia.

SEA HUNTER: lanciata nel 2016, la nave<sup>7</sup> è in grado di operare autonomamente, senza il supporto di equipaggio a bordo, per lunghi periodi di tempo (fino a due o tre mesi in autonomia) e percorrere lunghe distanze rispettando le normali regole di navigazione ed evitando le collisioni. È progettata principalmente per scovare sottomarini nemici (ASW) e può svolgere anche operazioni quali la posa e la rimozione di mine oppure di ricognizione e sorveglianza. Attualmente viene utilizzato come un banco di prova scientifico e tecnologico. Nel 2019, il Sea Hunter è stato il primo USV a navigare autonomamente da San Diego a Pearl Harbor, nelle Hawaii.

## Sentinelle robotiche

SENTRY TECH: sviluppato nel 2007, le autorità israeliane lo hanno utilizzato per proteggere i confini lungo la Striscia di Gaza. È una struttura fortificata modificata (*pillbox*), equipaggiata con la stazione di armi a distanza stabilizzata Samson Mini di Rafael, protetta da scudi pieghevoli. Una serie di questi scudi, essendo collegata in rete e combinata con vari sensori, trasmette le informazioni a un singolo operatore che agirà dopo l'identificazione e la verifica da parte del comandante. Sono stati progettati non solo per sorvegliare e controllare eventuali sconfinamenti territoriali, ma anche per proteggere da possibili attacchi con razzi di precisione. Una volta che i sensori IDF individuano un potenziale bersaglio, l'operatore può verificare, localizzare e coinvolgere il bersaglio grazie ai sensori giorno/notte elettro-ottici (EO). Rafael starebbe sviluppando anche un sistema autonomo che non richiederà l'intervento umano.

SGR-A1 SENTRY GUARD ROBOT: la Corea del Sud (Hanwha Techwin) ha investito in questo modello per il suo potenziale dispiegamento lungo l'area demilitarizzata<sup>8</sup>. La SGR-A1 ha una mitragliatrice da 5,56 mm ed un lanciagranate da 40 mm e rileva gli intrusi tramite sensori a infrarossi. È dotata di rilevatori di calore e di movimento ed attraverso tali strumenti può percepire persone e mezzi nel raggio di due miglia e decidere, dietro un comando umano, ogni azione consequenziale. Utilizza un software di riconoscimento dei pattern per individuare soggetti umani e può inoltre riconoscerne eventuali movimenti di resa. L'SGR-A1 possiede sia una

<sup>7</sup> Un multiscafo comprendente uno scafo principale e due scafi più piccoli (o galleggianti) attaccati ad esso con travi laterali.

<sup>8</sup> In realtà, in virtù dell'Armistizio tra le due Coree che proibisce il dispiegamento di armi nella zona, non è mai stato impiegato nella DMZ (Zona Demilitarizzata). Tuttavia, è stato schierato su base sperimentale in Afghanistan e Iraq.

modalità supervisionata sia non supervisionata. In modalità senza supervisione, la SGR-A1 identifica e tiene traccia degli intrusi, finendo per sparare contro di loro senza ulteriori interventi da parte degli operatori.

SUPER AEGIS II: per la prima volta in funzione nel 2010, è una torretta automatizzata sudcoreana che può essere montata con una mitragliatrice, un lanciatore automatico di granate da 40 mm o un missile terra-aria portatile. Opera con un raggio di rilevamento anche nell'oscurità totale, utilizzando sensori termici IR, telecamera a colori con ingrandimento e illuminatore laser. Dispone di rilevamento automatico, mentre il tracciamento, puntamento e accensione può essere sia manuale sia automatica. Può percepire, inoltre, se un bersaglio umano trasporta esplosivi o meno sotto i propri indumenti. Attualmente l'arma non ha modo di distinguere tra amico o nemico.





## *Gli autori*

**Fabrizio Battistelli**, Presidente di Archivio Disarmo. Già direttore del Dipartimento di Scienze Sociali ed Economiche, è professore onorario all'Università di Roma la Sapienza. È autore di libri e saggi sugli aspetti sociali della sicurezza interna e internazionale, della gestione delle crisi e dei processi di pace.

**Sofia Bertieri**, laureata in Sviluppo economico e cooperazione internazionale all'Università degli Studi di Firenze e in Scienze Strategiche alla scuola di applicazione dell'esercito di Torino.

**Francesca Farruggia**, ricercatrice presso il Dipartimento di Scienze Sociali ed Economiche dell'Università di Roma la Sapienza, è Segretaria generale di Archivio Disarmo. È autrice di diversi saggi sui temi della sicurezza interna ed internazionale, così come dei micro-conflitti tra attori sociali nell'istituzione scuola, tra i generi, nel contesto migratorio.

**Barbara Gallo**, laureata in Sociologia l'Università di Roma la Sapienza, dal 2013 collabora con Archivio Disarmo e si occupa di tematiche relative alle spese militari internazionali, alle armi letali autonome ed alle armi di distruzione di massa.

**Adriano Iaria**, collabora come docente e analista con diverse università e think tank italiani. Ha pubblicato nei settori del disarmo, della sicurezza internazionale e del diritto internazionale umanitario.

**Diego Latella**, Primo Ricercatore CNR presso l'Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo", dove si occupa di Metodi Formali per l'Informatica. È membro del Consiglio Scientifico dell'USPID e del Consiglio Direttivo dell'ISO-DARCO.

**Michael Malinconi**, laureato in Sviluppo economico e Cooperazione Internazionale presso l'Università di Firenze con una tesi in Diritto Internazionale. Scrive di politica internazionale e analisi strategica.

**Juan Carlos Rossi**, laureato in Scienze Politiche e Relazioni Internazionali all'Università di Roma la Sapienza, nel 2015 ha conseguito il Master di II livello in Tutela dei diritti umani presso la stessa Università. Ha pubblicato sui temi degli armamenti e delle crisi internazionali.

**Maurizio Simoncelli**, Vicepresidente di Archivio Disarmo. Storico ed esperto di geopolitica, docente presso il Master Nuovi orizzonti di cooperazione e diritto internazionale della FOCSIV/Pontificia Università Lateranense. Dirige il mensile online *IRIAD REVIEW Studi sulla pace e sui conflitti* ed è editorialista della rivista mensile *Città Nuova* con la rubrica *Guerre e pace*.

**Gian Piero Siroli**, fisico subnucleare, si occupa di calcolo e sicurezza informatica in infrastrutture ed apparati di Fisica delle alte energie presso il CERN di Ginevra ed altri centri di ricerca. È attivo in ambito accademico e ONU nel dominio della cyber-security e cyber-war, su questioni relative ad ICT nella sicurezza internazionale.

**Guglielmo Tamburrini**, professore ordinario di Filosofia della scienza e della tecnologia all'Università di Napoli Federico II. È membro del Consiglio scientifico dell'USPID (Unione degli scienziati per il disarmo) e membro dell'ICRAC (International Committee for Robot Arms Control).

Il volume affronta la questione delle armi semi-autonome (droni) e autonome (i cosiddetti robot-killer). Numerosi miti ed episodi storici alludono alla possibilità di affidare in tutto o in parte le attività di combattimento alle macchine: anticipazioni simboliche dell'Intelligenza Artificiale che, applicata alla guerra, sta ispirando la ricerca, lo sviluppo e la futura operatività delle armi letali autonome (LAWS). Protagoniste del processo sono le principali potenze mondiali: Stati Uniti, Cina, Russia e alcuni Stati europei. A questo gruppo di testa potrebbero unirsi vari Paesi in via di industrializzazione, efficienti fornitori di droni, come la Turchia e l'Iran, nel conflitto russo-ucraino. Anche attori non statali, come alcune formazioni terroristiche e criminali, hanno già iniziato a utilizzare velivoli senza pilota.

In alternativa all'incombente proliferazione di macchine che sfuggono al controllo umano, due sono le possibili soluzioni. La prima è rappresentata dalla società civile, nella duplice articolazione delle prese di posizione della comunità scientifica internazionale e della mobilitazione dell'opinione pubblica; la seconda dagli accordi internazionali per il controllo delle armi semi-autonome e per la prevenzione e il divieto delle armi letali autonome.

**Scritti di:** Fabrizio Battistelli, Sofia Bertieri, Francesca Farruggia, Barbara Gallo, Adriano Iaria, Diego Latella, Michael Malinconi, Giorgio Parisi, Juan Carlos Rossi, Maurizio Simoncelli, Gian Piero Siroli, Guglielmo Tamburrini.

**Francesca Farruggia**, ricercatrice presso il Dipartimento di Scienze Sociali ed Economiche della Sapienza Università di Roma, è segretaria generale di Archivio Disarmo. È autrice di diversi saggi sui temi della sicurezza interna e internazionale, così come dei micro-conflitti tra attori sociali nell'istituzione scuola, tra i generi, nel contesto migratorio.