SLJ STRATEGIC LEADERSHIP JOURNAL

Numero 1 – Anno 2025

ISSN 2975-0148 – ISBN 9791255150992

CENTRO ALTI STUDI DIFESA

SCUOLA SUPERIORE UNIVERSITARIA

I NOSTRI VALORI

INNOVAZIONE COME SFIDA

Viviamo l'innovazione con coraggio e curiosità, come una sfida entusiasmante in grado di generare valore nella formazione e nella ricerca per far fronte con successo alla complessità del mondo attuale.

SPIRITO DI SQUADRA E APPARTENENZA

Crediamo nello spirito di squadra e nel senso di appartenenza che, attraverso la lealtà reciproca, la condivisione e l'armonia nelle relazioni, assicurano il benessere individuale e il successo organizzativo.

ECCELLENZA NELLE COMPETENZE

Ci ispiriamo all'eccellenza nel nostro agire quotidiano, impegnandoci a riconoscere con equità le competenze di ciascuno e a potenziarne i talenti e mirando ad essere punto di riferimento per l'offerta formativa e l'attività di ricerca a cui come Istituzione siamo chiamati.

RESPONSABILITÀ AL SERVIZIO DEL PAESE

Fondiamo sull'etica e sull'integrità il nostro operare, in continuità con la tradizione, a favore della cultura di una leadership responsabile al servizio del Paese e della comunità internazionale.

VALORIZZAZIONE DELLE DIFFERENZE

Siamo convinti che un approccio aperto e integrativo, che nell'altro riconosca e valorizzi tutte le peculiarità che lo rendono unico, permetta l'espressione e la crescita delle capacità individuali e costituisca leva strategica per lo sviluppo di network capaci di facilitare il conseguimento degli obiettivi organizzativi ed istituzionali.

Centro Alti Studi Difesa

Scuola Superiore Universitaria

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS AND ORGANIZATIONAL DEVELOPMENT

Numero 1 – Anno 2025

Centro Alti Studi Difesa – Scuola Superiore Universitaria

Direzione e Redazione Palazzo Salviati
Piazza della Rovere, 83, 00165 – Roma
www.casd.it
Tel 06 4691 23208 – e-mail: irad.usai@casd.difesa.it

ISSN 2975-0148 – ISBN 9791255150992

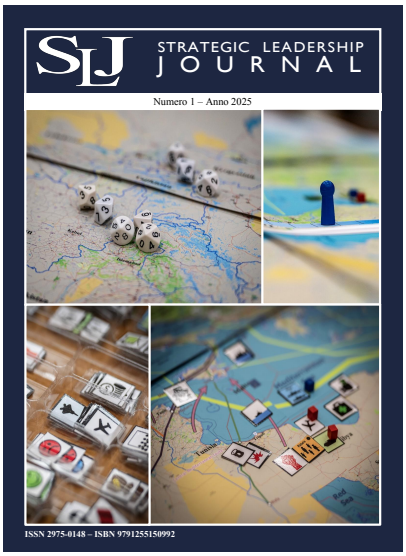


Foto di Stefano Guerrieri

A cura di
Massimo Lanfranco

L'immagine di copertina di questo numero richiama le operazioni connesse all'evento di *Wargaming* che si è svolto presso il CASD nei giorni 4-5 dicembre 2024.

Nato come un gioco da tavolo già a partire dal medioevo, il moderno *Wargame* si è sviluppato intorno al XVIII secolo per merito dell'interesse suscitato dalle sue possibili applicazioni in campo militare e in quello civile.

I governi di diverse Nazioni, infatti, ritengono oggi il *Wargame* un importante strumento, utile per elaborare strategie senza le implicazioni che le operazioni reali comportano, per mezzo del quale è possibile stimare i potenziali risvolti delle decisioni intraprese senza tema di complicazioni o danni concreti. Uno strumento, quindi, molto utile anche per formare dirigenti militari e civili che tramite le attività ludiche riescono a sviluppare *soft skills* desiderabili per ogni leader, quali: capacità di pianificare ed organizzare; conseguire obiettivi; problem solving; capacità decisionale e comunicativa; capacità di lavorare in squadra; resistenza allo stress; leadership.

La recente integrazione del *Wargaming* con l'Intelligenza Artificiale ha notevolmente amplificato la quantità di dati analizzabili, moltiplicando le possibili interazioni tra mondo reale e mondo virtuale. L'utilizzo dell'AI proietta di fatto scenari potenziali a situazioni finora impreviste, affinando l'accuratezza dell'analisi strategica e perfezionando conseguentemente il ventaglio decisionale a disposizione degli utilizzatori.

STRATEGIC LEADERSHIP JOURNAL

CHALLENGES FOR GEOPOLITICS AND ORGANIZATIONAL DEVELOPMENT

INDICE

Ministero della Difesa

Periodico della DifesaRegistrazione Tribunale di Roma n. 88/2023
in data 22.06.2023Codice Fiscale 97042570586
ISSN 2975-0148 – ISBN 9791255150992

Tutti gli articoli di questo volume riflettono esclusivamente il pensiero dei singoli autori e non quello degli organi della Rivista né di Istituzioni militari e/o civili

STRATEGIC LEADERSHIP JOURNAL

ARTICOLI

DANILO CECCARELLI MOROLLI

Membro Corrispondente del Pontificio Comitato di Scienze Storiche; Professore Ordinario nella Facoltà di Diritto Canonico Orientale della Pontificia Università Gregoriana; Prof. Ass. nella Università Telematica "G. Marconi". Ufficiale Superiore della Marina Militare Italiana (Riserva Selezionata)

ALCUNI "INDIZI" DI HUMAN RESOURCE MANAGEMENT NELLA CODIFICAZIONE GIUSTINIANEA: NOTE PER UNA DIFFERENTE "LETTURA"

ABSTRACT

L'articolo analizza la codificazione giustinianea attraverso una lente contemporanea, in particolare considerando elementi di leadership partecipativa e gestione delle risorse umane (HRM). Viene evidenziato come Giustiniano, oltre a codificare il diritto, avesse l'intenzione di formare una classe giuridica competente, mettendo in atto strategie che anticipano concetti moderni di HRM.

This paper analyzes Justinian's codification through a contemporary lens, focusing on participatory leadership and human resource management (HRM). It highlights how Justinian, besides codifying the law, aimed to train a competent legal class by implementing strategies that foreshadow modern HRM concepts.

Keyword: codificazione giustinianea; leadership partecipativa; Human Resource Management; élite giuridiche

1. Premesse

La storia dell'Impero Romano, come ben noto, si "sdoppia" aggiungendo così un millennio come Impero Romano d'Oriente, dal 330 fino alla caduta di Costantinopoli, avvenuta nel 1453. Il punto di cerniera, anche per ciò che poi sarà il diritto di quella che *sic et simpliciter* chiamiamo "civiltà bizantina", è certamente Giustiniano, che regna in Costantinopoli dal 527 al 565. Egli è Imperatore più di mezzo millennio dopo Ottaviano Augusto, che trasformò la *Res Publica* in Principato[1]. Il parallelismo tra Ottaviano e Giustiniano non è peregrino se si considera il ruolo delle *élite* e quindi della leadership del *princeps* prima e del βασιλεύς poi. Chiaramente tra Augusto e Giustiniano intercorrono quasi sei secoli di storia e Giustiniano "eredita" un Impero che non è più ovviamente il principato augusteo; infatti Giustiniano muove da un dato ormai certo ed assunto, ovvero la βασιλεία (*basiléia*), cioè la regalità imperiale e la fede cristiana, che ispira l'Imperatore in ogni sua azione normativa, divenendone fondamento teologico anche del diritto per cui si potrebbe parlare, a ragione, di "teologia del diritto" (giustinianeo).

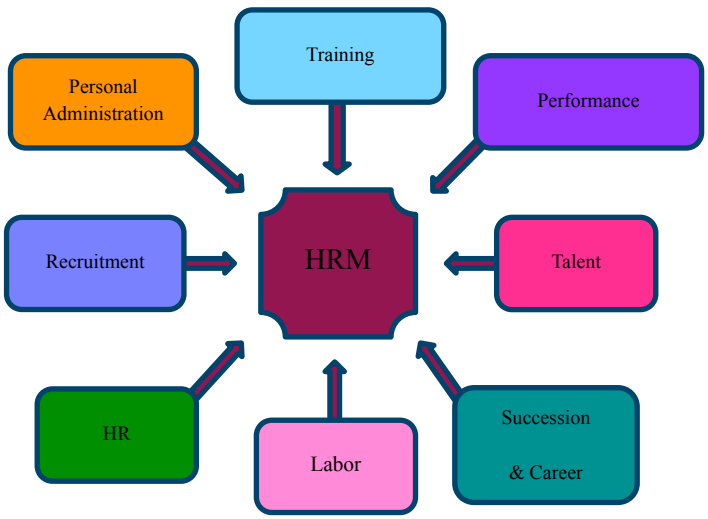
Di certo non è questa la sede per realizzare uno studio comparativo tra i due grandi personaggi storici della civiltà romana (giova ricordare che i Romani d'Oriente si sono sempre auto-definiti come οἱ Ῥωμαῖοι, cioè "i Romani", nel Medio Evo detti "Romei"). Se

[1] FABBRINI F., *L'Impero di Augusto come ordinamento sovrannazionale*, Milano 1974; LICANDRO O., *La transizione augustea tra legislazione e poteri*, in *Index* 45 (2017), pp. 39-48; ed in generale sul tema di Augusto, si segnala: FERRAY J.L., *Dall'ordine repubblicano ai poteri di Augusto. Aspetti della legislazione romana*, «Fra Oriente e Occidente» 4, Roma 2016. LICANDRO O., Augusto e la Res Publica imperiale, studi epigrafici e papirologici, Torino 2018.

infatti esistono innumerevoli studi e monografie su Giustiniano[2] e se, parimenti, tutti i manuali di storia del diritto romano o anche quelli di storia del diritto medievale riportano l'impresa codificatrice di questo grande Imperatore, in realtà non sembra che ci si sia soffermati sulla visione che egli, necessariamente, aveva delle "risorse umane" al fine di realizzare il suo titanico progetto. Tuttavia, prima di procedere, ritengo necessaria un'ulteriore premessa.

La teoria di ciò che noi denominiamo come "gestione delle risorse umane" che si sviluppa sostanzialmente in età moderna a livello teoretico a partire dagli studi sul "*Participatory Management*" di Rensis Likert (1903-1981)[3] oggi è approdata ad un livello più completo ed organico, ossia è nota come *Human Resources Management* (HRM).

In estrema sintesi, si può affermare che la HRM è basata su di un nuovo modo di gestire le risorse umane come forme di decentramento decisionale e di flessibilità organizzativa, utilizzando un approccio partecipativo, promuovendo così coesione integrazione e qualità. Da ciò discendono tre ambiti di applicazione: a) un livello ideologico-culturale, cioè sono i "pronunciamenti" riguardo il ruolo e la rilevanza delle risorse umane nella "filosofia" aziendale; b) le politiche di gestione del personale atte a promuovere un'efficace cooperazione del fattore lavoro, c) le pratiche e gli strumenti messi in atto che ricoprono uno spettro ampio di attività. Volendo ricorrere ad una rappresentazione grafica, è possibile delineare il seguente quadro



Ma tutto ciò a cui è approdato il mondo contemporaneo è un *quid novi* oppure Giustiniano potrebbe rappresentare una sorta d'esempio prodromico in tal senso?

Per rispondere a tale domandaci ci si focalizzerà, brevemente, su alcuni "momenti" della codificazione giustinianea.

Il motivo di questa scelta è semplice: possediamo le fonti che hanno illustrato ai contemporanei di allora il processo di codificazione e l'obiettivo della stessa; sono queste le costituzioni imperiali emanate da Giustiniano con le quali lo stesso Imperatore fornisce notizie, dati e informazioni non solo sul progetto, sugli scopi dello stesso, ma anche – come vedremo – sulla modalità. In poche parole, le costituzioni imperiali di tale monumentale opera, possono essere non solo le tracce ma anche gli indizi del modo di ragionare in merito a

[2] A mero titolo d'esempio riportiamo, tra le molte citabili, alcune monografie: SARRIS P., *Justinian. Emperor, Soldier, Saint*, New York 2023; CAPIZZI C., *Giustiniano tra politica e religione*, Soveria Mannelli 1994; ARCHI G.G., *Giustiniano legislatore*, Bologna 1970.

[3] LIKERT R., *The Human Organization: Its Management and Value*, New York 1967; Idem, *New Patterns of Management*, New York 1961;

come *leadership* e HRM si siano intrecciati un millennio e mezzo fa per portare a compimento una delle opere più importanti, se non la più importante, della storia del diritto occidentale, ovvero la codificazione giustinianea, espressa dal *Codex*, dalle *Institutiones* e dal *Digestum* o *Pandectæ*.
In particolare, anche al fine di restringere il campo della ricerca, mi soffermerò su alcuni brani delle seguenti costituzioni[4]: Cost. *Imperatoriam* del 21 novembre 533 promulgante le *Institutiones*; Cost. *Deo auctore* dal 15 dicembre 530, sancente il progetto del Digesto; Cost. *Tanta-Δέδωκεν* del 16 febbraio 533, promulgante i *Digesta*; Cost. *Omnem*, del 15 dicembre 533, riformulante l'organizzazione del ciclo di studi giuridici.

2. Alcuni "indizi" di HMR nelle costituzioni giustinianee

Un primo "indizio" lo possiamo rintracciare nella Cost. *Imperatoriam* che pubblica le *Institutiones*. Il fine di Giustiniano è chiaro: creare un manuale di studio del diritto ad uso degli studenti ma anche dei docenti. Se fino ad allora le generazioni di giuristi si formavano sulle *Institutiones* del giurista Gaio (vissuto nel II sec. d.C.)[5], ora è l'Imperatore stesso che prende a cuore l'educazione giuridica, realizzando appunto le proprie istituzioni. Questo poiché l'Imperatore non è solo "adornato" di armi bensì anche dal diritto. Così, infatti, recita la prefazione della Costituzione:

"*La maestà dell'Imperatore non deve essere ornata solamente dalle armi, ma deve essere anche armata dalle leggi, affinché possa governare correttamente sia i tempi di guerra che quelli di pace e affinché il principe romano possa emergere vittorioso non solo nelle battaglie contro nemici esterni, ma anche scacciando le ingiustizie dei calunniatori per vie legittime, e che diventi tanto religioso nel rispetto del diritto quanto trionfatore sui nemici vinti*"[6].

L'intento è quindi successivamente esplicitato nel paragrafo terzo della medesima costituzione in cui l'Imperatore asserisce:

"*E quando questo è stato compiuto con la propizia volontà divina, abbiamo convocato specialmente Triboniano, uomo illustre e magister e precedentemente questore del nostro sacro palazzo, insieme a Theophilo e Dorotheo, uomini illustri antecessori, di cui abbiamo già riconosciuto la sagacia, la conoscenza delle leggi e la fedeltà ai nostri comandi attraverso molti segni. Abbiamo incaricato con la nostra autorità e le nostre sollecitazioni che compongano le Institutiones* (…)"[7].

L'Imperatore menziona Triboniano, suo ministro e gli *antecessores*, ovvero i docenti di diritto, Teofilo[8] e Doroteo[9]. La menzione di costoro è un segno tangibile della gratitudine imperiale.

Successivamente, la Cost. *Deo auctore*, sul concepimento dei *Digesta*, possiede nel suo

---

[4] I testi e le traduzioni, in lingua italiana, sono tratti dall'opera curata da SCHIPANI S., *Iustiniani Augusti Digesta seu Pandectæ. Testo e traduzione*, vol. I, 1-4, Milano 2005
[5] BRIGUGLIO F., *Introduzione allo studio delle Istituzioni di Gaio*, Biblioteca Gaiana, Vol. I, USA, 2015 (2 ed.); HONORÈ T., *Gaius*, Oxford 1962.
[6] La traduzione riportata sopra è di chi scrive; ecco il testo in lingua latina: «*Imperatoriam maiestatis non solum armis decoratam, se etiam legibus oportet esse armata, ut utrumque tempus bellorum et pacis recte possit gubernari et princeps Romanus victor existat non solum in hostilibus proeliis, sed etiam Per legitimts tramites calumniantium iniquitates expellens, et fiat tam iuris religiosissimus quam victis hostibus triumphator*» (ARANGIO RUIZ V. – GUARINO A., *Breviarium Iuris Romani*, Milano 1998[8], p. 209).
[7] La traduzione riportata sopra è di chi scrive; ecco il testo in lingua latina: «*Cumque hoc Deo propitio peractum est, Triboniano viro magnifico magistro et ex quæstore sacri palatii nostri, nec non Theophilo et Dorotheo viris illustribus antecessoribus, quorum omnium sollertiam et legum scientiam et circa nostroas iussiones fidem iam ex multis rerum argumentis accepimus, convocati specialiter mandavimus, ut nostra auctoritate nostrique suasionibus componant institutiones* […]» (ARANGIO RUIZ V. – GUARINO A., *Breviarium Iuris Romani*, Milano 1998[8], p. 209-210).
[8] Teofilo realizzò un Indice in lingua greca ai *Digesta* e una Parafrasi al *Codex*.
[9] Doroteo era docente a Beirut e stilò un indice completo al Digesto, sempre in greco.

insieme non solo una valenza nomotecnica[10] ma anche programmatica, in quanto esprime come avrebbe dovuto procedere la commissione per la redazione dei *Digesta*. Non ci soffermeremo su tale costituzione, ma accenneremo soltanto al fatto che la regalità nell'Impero Romano d'Oriente è intimamente connessa all'elemento divino, ovvero sempre agganciata al credo trinitario niceno[11] e quindi il lettore contemporaneo non si stupirà se tale cost. principia "con l'ausilio di Dio" (*Deo auctore*, appunto).

Maggiormente utile, per il nostro tema, risulta certamente la cost. bilingue *Tanta* – Δέδωκεν, con cui Giustiniano promulga i *Digesta*. L'Imperatore, pur partendo dal ringraziamento a Dio per questa immensa impresa, afferma che: "*Tutto quindi è stato compiuto, perché il Signore Dio nostro Gesù Cristo ne ha concesso la possibilità sia a noi sia ai nostri collaboratori in quest'opera*"[12]. L'Imperatore spiega poi il perché del nome di tale opera:

"[…] *tutto ciò che era più utile è stato raccolto in cinquanta libri e tutte le ambiguità sono state decise, senza lasciar nulla che possa suscitare disordine. A questi libri abbiamo dato il nome di Digesti o Pandette perché contengono al proprio interno tutte le questioni discusse e le decisioni in tema di diritto, e hanno recepito nel proprio seno ciò che è stato raccolto da ogni dove, concludendo l'intera opera nella somma di circa centocinquantamila righe. E li abbiamo ordinati in sette parti, non a caso né senza motivo, ma considerando la natura e la scienza dei numeri ed operando una suddivisione delle parti conforme ad esse*"[13].

Su questo "scenario" generale, Giustiniano scende poi nel dettaglio per illustrare la *nomotecnica* utilizzata e, successivamente, indugia nel descrivere gli uomini che hanno realizzato i *Digesta*, esaltando fra tutti Triboniano che viene onorato e menzionato come segue:

---

[10] Tale vocabolo è un neologismo risultato della crasi di due sostantivi (νόμος e τέχνη), creato da Dimitri Salachas, insigne canonista orientale contemporaneo. Egli parla di *nomotecnica* in riferimento al *Codex Canonum Ecclesiarum Orientalium* (promulgato il 18 ottobre 1990 da S. Giovanni Paolo II, come codice comune a tutte le Chiese cattoliche orientali). Dunque *nomotecnica* sta anche a significare "tecnica della redazione e della codificazione del diritto stesso" e, nelle fonti, la modalità con cui queste si esprimono. SALACHAS D., *Teologia e nomotecnica del "Codex Canonum Ecclesiarum Orientalium"*, in *Periodica de re morali canonica liturgica* 82/2 (1993), pp. 317-338. Circa il ruolo di Salachas nella canonistica orientale cfr. CECCARELLI MOROLLI D., *Dimitrios Salachas ed il suo contributo scientifico alla canonistica orientale contemporanea*, in LORUSSO L. – SABBARESE L. (a cura di), *Oriente e Occidente: respiro a due polmoni. Studi in onore di Dimitrios Salachas*, «Studia Canonica» 67, Roma 2014, pp. 13-20.

[11] Alcuni cenni bibliografici sulla regalità dell'Impero Romano d'Oriente: DAGRON G., *Emperor and Priest. The Imperial Office in Byzantium*, Cambridge 2003 (edizione inglese dell'originale francese: *Empereur et prêtre. Étude sur le "cesaropapisme" byzantin*, Paris 1996); PITSAKIS K., *L'empereur romain d'Orient: un laïc*, in *Kanon* 15 (1999), pp. 196-221. CECCARELLI MOROLLI D., *Εὐσεβέστατος Βασιλεύς: ovvero l'Imperatore attraverso i* Sacri Canones *del primo millennio*, in *Minima Epigraphica et Papyrologica* anno 23, fasc. 25 (2020), pp. 65-74; IDEM, *Per una geopolitica del diritto dell'Impero Romano d'Oriente*, «Geo» I, Roma 2020, pp. 22-36. La Cost. *Deo auctore* così principia: «*Con il sostegno di Dio, governando l'impero che a noi è stato consegnato dalla Maestà celeste, abbiamo condotto a termine felicemente le guerre, abbiamo onorato la pace, abbiamo sorretto lo stato della repubblica, e abbiamo elevato il nostro animo verso l'aiuto di Dio onnipotente, in modo tale che non confidiamo né nelle armi, né nei nostri soldati, né nei condottieri delle guerre, o nel nostro ingegno, ma rimettiamo ogni nostra speranza nella sola provvidenza della somma Trinità, dalla quale sia derivarono gli elementi primi di tutto il mondo, sia è stato prodotto il loro ordine nell'orbe terrestre*»; «*Deo auctore nostrum gubernantes imperium, quod nobis a cælesti maiestate traditum est, et bella feliciter peragimus et pacem decoramus et statum rei publicæ sustentamus: et ita nostros animos ad Dei omnipotentis erigimus adiutorium, ut neque armis confidamus neque nostris militibus neque bellorum ducibus vel nostro ingenio, sed omnem spem ad solam referamus summæ providentiam trinitatis: unde et mundi totius elementa processerunt et eorum dispositio in orbem terrarum producta est*» (SCHIPANI S., p. 23).

[12] SCHIPANI S., p. 40: «*Omnia igitur confecta sunt domino et deo nostro Ihesu Christo possibilitatem tam nobis quam nostris in hoc satellitibus præstante*» (*Tanta*, *præf*, in finale).

[13] *Tanta*, I: «[…] *et in quinqueginta libros omen quod utilissium erat collectum et et omnes ambiguitates decisæ nullo seditioso relicto. Nomenque libris inposimus digestorum seu pandectarum, quia omnes disputationes et decisiones in se habent ligitimas et quod undique fuit collectum, hoc in sinus suos receperunt, in centum quinqueginta pæne milia versuum totum opus consummantes. Et in septem partes eos digessimus, non perperam neque sine ratione, sed in numerorum naturam et artem respicientes et consentaneam is divisionem partium conficientes*», SCHIPANI S., pp. 40-1.

"*Tutto ciò è stato realizzato per mezzo di Triboniano, uomo eccelso, nonché espertissimo ministro posto a capo degli uffici pubblici, ex questore ed ex console, il quale essendo egualmente versato nelle arti della retorica e della scienza giuridica, si è messo in luce proprio nella concreta esperienza e nulla ha mai considerato più importante e a lui più caro dei nostri ordini; ed altresì è stato portato a compimento per mezzo di altri uomini magnifici e molto amanti della cultura, cioè Costantino […], Teofilo […] Doroteo […] Anatolio […] Cratino […]. Tutti costoro sono stati prescelti per il compimento dell'opera summenzionata insieme con Stefano, Mena, Prosdocio, Eutolmio, Timoteo, Leonide, Leonzio, Platone, Jacopo, Costantino, Giovanni, uomini molto esperti, che da un lato sono avvocati patrocinanti presso l'altissima corte della prefettura preposta ai distretti orientali […]. E una volta riuniti insieme sotto la direzione di Triboniano, uomo eccelso, per poter realizzare una così grande opera con il nostro sostegno, con il favore di Dio l'opera è giunta a compimento nei cinquanta libri dei quali si è detto sopra*"[14].

L'Imperatore elogia, *in primis*, Triboniano ricordandone la fulgida carriera e le cariche pubbliche[15]. Unitamente a ciò, l'Imperatore desidera anche ricordare tutti gli *antecessores*[16], ovvero quei docenti di diritto della scuola di Costantinopoli e di Beirut (Berito), che hanno preso parte alla realizzazione dei *Digesta*. Così, se Triboniano è appellato come uomo "eccelso" ed "espertissimo", non di meno gli *antecessores* sono denominati come persone "magnifiche" ed "amanti della cultura". Infine, l'Imperatore ringrazia gli ulteriori esperti, ovvero gli avvocati, elencandoli per nome. Per la cronaca, grazie a queste menzioni, conosciamo i nomi di coloro che presero parte alla commissione per i *Digesta*. Tutti questi nominativi diventano ancor più rilevanti poiché ci indicano la scelta fatta da Giustiniano come supremo "manager" per la realizzazione dell'ambiziosissimo progetto quale fu appunto il Digesto. Infatti, se il Digesto è l'obiettivo, questo lo si è perseguito creando un *cœtus*, un gruppo di esperti del massimo livello capaci e coordinati da un "manager" come Triboniano. Si potrebbe parlare, forse e non a caso, di un vero e proprio "management per obiettivi" [17] che Giustiniano affida a Triboniano e, a cascata, agli altri.

Questo è dunque il modello manageriale giustinianeo, cioè ciò che gli storici del diritto denominano come "commissione" ma che appare in realtà come qualcosa di più complesso. Infatti, a capo della Commissione Giustiniano pone Triboniano, che non è solo un burocrate, ma anche un giurista, attuando così una prima scelta, esercitando un *ius in eligendo*. La decisione di Giustiniano è una decisione "critica", perché egli sa bene che è necessaria una chiara identificazione degli obiettivi.

---

[14] Cost. *Tanta*, 9 : «*Quæ omnia confecta sunt per virum excelsum nec non prudentissimum magistrum ex quæstore et ex console Tribonianum, qui similiter eloquentiæ et legitimæ scientiæ artibus decoratus et in ipsis rerum experimentis emicuit nihilque maius nec carius nostris unquam iussionisbus duxit: nec non per alios viros magnificos et studiosissimos perfecta sunt, id est Consatantinum* […] *Theophilum* […] *Dorotheum* […] *Antatolium* […] *Cratinum* […] *qui omenes ad prædictum opus electi sunt una cum Stefano, Mena, Prosodico, Eutolmio, Timotheo, Leonide, Leontio, Platone, Iacobo, Constantino, Iohanne, viris prudentíssimas, qui patroni quidem sunt causarum apud maximum sedem præfecturæ* […]. *Et cum omnes in unum convenerunt gubernatione Triboniano viri excelsi, ut tantum opus nobis auctoribus possint conficere, Deo propitio in prædictos quinquaginta libros opus consummatum est*» (SCHIPANI S., p. 44).

[15] Poco conosciamo della vita di Triboniano (500-542 ca.), se non alcuni suoi passaggi di carriera: *magister officiorum* (528), *quæstor sacri palatii* (529-532), quindi nuovamente *magister officiorum* (533-534) e poi di nuovo *qæstor sacri palatii* (535); cfr. ORESTANO R., s.v. *Tribniano (Tribonianus*), in *Novissimo Digesto Italiano*, vol. XII, t. 2, p. 463. Per la cronaca, il *magister officiorum* – carica istituita da Costantino – era il capo di tutte le attività della segreteria imperiale raccogliendo diversi uffici di nevralgica importanza per la cura imperiale; mentre il *qæstor sacri palatii* era l'equivalente di ciò che oggi diciamo essere il ministro della giustizia.

[16] Cfr. TROIANOS S., *Le fonti del diritto bizantino*, Torino 2015, pp. 57 ss.; CECCARELLI MOROLLI D., *Il diritto dell'Impero Romano d'Oriente. Introduzione alle fonti e ai protagonisti*, «Kanonika» 21, Roma 2016, pp. 46 ss.; SCHELTEMA H.J., *L'enseignement de droit des antécesseurs*, Leiden 1970. Il vocabolo *antecessor* (pl. *antecessores*; in gr.: ἀντικήνσορες), mutuato dal mondo militare, divenne identificativo di docente di diritto.

[17] Cfr. GREENWOOD R.C., *Managment by Objectives: ad developed by Peter Drucker assisted by Harlod Smiddy,* in *Academy of Managment Review* 6/2 (1981), pp. 225 ss.; DRUCKER P.F., *The Practice of Management*, New York 1954.

Così crea un gruppo di lavoro tutto sommato ristretto – la commissione – composta da esperti del settore: i docenti di diritto e gli avvocati. Teoria e pratica, dottrina e prassi, sembrano essere stati i riferimenti nella mente di Giustiniano e, quindi anche, di Triboniano. Questi "uomini magnifici" – per citare la cost. *Tanta* – sono stati in grado, in un triennio, di portare a compimento un'opera titanica come il Digesto in ben cinquanta libri. Per la cronaca, Procopio di Cesarea, nella sua *Storia Segreta*, si scaglia contro Triboniano dipingendolo come uno, utilizziamo un'espressione moderna, "*yes man*" ambizioso e senza scrupoli.

Tuttavia, al di là degli inevitabili intrighi di palazzo, ancora oggi si discute su quanto si debba a Triboniano per la realizzazione dei *Digesta*, ovvero se – senza di lui – Giustiniano avrebbe potuto realizzare tale opera. Leggendo tra le righe della Cost. *Tanta*, oggi ci sembra di intuire una sincera gratitudine ed ammirazione di Giustiniano verso il suo giurista, non senza ricordare e menzionare l'intervento e l'ausilio divino (*Deo propitio*). L'Imperatore pare esultare ricordando quanto la realizzazione dell'opera, nelle previsioni, si preannunciasse lunga, mentre il compimento della stessa ha superato ogni più rosea previsione: solo tre anni[18]. Del resto, i 50 libri del Digesto, a distanza di mille e cinquecento anni, sembrano testimoniare la titanicità di tale impresa che, fortunatamente, è giunta fino ai giorni nostri.

Giustiniano conclude, nel finale della costituzione, affermando che i *Digesta* debbono essere dati a tutti i giudici, ciascuno secondo la propria giurisdizione[19]. Questo implica il concetto dell'accessibilità del diritto – almeno in parte, cioè da parte dei diretti interessati – e, parimenti, la volontà che i giudici siano "istruiti" cioè conoscano i *Digesta* al fine di poter giudicare le cause loro attribuitegli.

Risulta dunque che l'intento giustinianeo sia stato non solo codificatorio, ma anche "didattico", cioè formare ed educare. Egli aveva intuito, brillantemente, che le *élite* vanno formate, cioè alimentate nella loro competenza. A tale scopo egli crea il Digesto che diviene così strumento di conoscenza e apprendimento non solo per gli studenti e per i docenti, ma anche per i giudici, ovvero gli "operatori" pratici del diritto stesso.

Come si può facilmente intuire dalle righe che precedono, "gestione delle risorse" e "leadership" appaiono argomenti intimamente collegati fra loro. Da qui la "preoccupazione" imperiale di formare la classe dirigente, è propriamente espressa apertamente con la cost. *Tanta*, che non va letta – a parere di chi scrive – solo come una notevole fonte storico-giuridica, ma anche nell'ottica di come l'Imperatore attuasse una forma di management della *leadership* stessa. Se infatti da un lato elogia, ringrazia e consegna a perpetua memoria gli uomini che hanno preso parte al processo codificatorio, dall'altra egli dà le ragioni per cui il lavoro di codificazione è stato fatto. Nel §10 della medesima costituzione, si sottolinea il rispetto per l'antichità (*tanta autem nobis antiquitati habita est reverentia*) e con essa l'importazione nei *Digesta* dei frammenti dei giuristi antichi. Qui non interessa il problema dei tagli e degli eventuali emendamenti – le interpolazioni – attuati dalla commissione verso i giureconsulti del passato, ciò che conta è invece rimarcare come l'Imperatore agganci il presente al passato, ancorando così il suo lavoro a ciò che era prima, come a dire: i *Digesta* sono il frutto del passato e quindi sono già per questo autorevoli e pertanto necessariamente indispensabili al giurista: *"[...] nessuno osi confrontare quello che contenevano gli scritti degli antichi e quello che ha introdotto la nostra autorità*"[20]. Anche per questo Giustiniano vuole che nei *Digesta* compaiano i nomi dei grandi giuristi romani del passato (Paolo,

---

[18] Cost. *Tanta*, 12: «[…] *e avendo condotto a termine in tre anni ciò che, non appena si erano iniziati i preparativi, non si sperava di poter completare neanche in un intero decennio, con animo devoto abbiamo offerto a Dio onnipotente anche quest'opera, diretta a essere sostegno per gli uomini e abbiamo reso abbondanti grazie al sommo Dio* […] » - «[…] *perfecta in tribus annis consummata, quæ ut primum separari cœpit, neque in totum decennium compleri separabatur: omnipotenti Deo et hanc operam ad hominum sustentationem piis optulimus animis uberesque gratias maximæ deitati reddimus* […]» (SCHIPANI S., p. 46-7).

[19] Cost. *Tanta*, 24: «*Omnes itaque iudices nostri pro sua iurisdictione easdem leges suscipiant et tam in suis iudiciis* […]» (SCHIPANI S., p. 52).

[20] *Tanta*, 10: «*nemine audente comparare ea quæ antiquitas habebat et quæ nostra auctoritas introduxit*» (SCHIPANI S., p. 45).

Modestino, Celso, Ulpiano, Papiniano, ecc.).
Ancor di più l'attenzione di Giustiano verso l'educazione è chiaramente sancita dalla cost. *Omnem*, con la quale riordina gli studi di diritto in Costantinopoli. Nel proemio di tale costituzione, egli afferma che insegnare agli studenti significa far sì che essi diventino ottimi e preparati giuristi (*optimi atque eruditissimi*)[21]. La cost. *Omnem* ha come effetto quello di creare un ciclo di studi quinquennale – sia a Costantinopoli che a Beirut (Berito) – durante il quale gli studenti apprendono la codificazione giustinianea (*Digesta, Codex* ed *Institutiones*). L'influsso di tale costituzione si evidenzierà anche poi nel Medio Evo[22].

3. Conclusione

Guardando all'azione codificatrice di Giustiniano ci si accorge di come egli avesse chiaro, già all'epoca, il concetto di "management delle risorse umane" e parimenti dell'uso della *leadership* partecipativa.
Uno degli effetti o dei propositi della codificazione giustinianea è infatti certamente quello di formare una classe di giuristi, preparati. Da qui la Cost. *Omnem* [23], scansendo per ogni anno i testi specifici delle *Istitutitiones*, dei *Digesta* e del *Codex* da studiare. Non di meno egli si rivolge ai docenti e agli studenti con queste parole:

"*Iniziate dunque, con la guida di Dio, a trasmettere agli allievi il sapere giuridico e ad aprire loro la via che abbiamo individuata, affinché diventino ottimi servitori della giustizia e della* res publica *e voi siate accompagnati da grandissimo onore per tutti i secoli, perché ai vostri tempi è stato effettuato un tale mutamento del diritto (…) stabiliamo che tutto ciò valga in ogni tempo, tanto dai professori quanto dagli studenti di diritto e dai copisti e soprattutto dagli stessi giudici*"[24].

A Giustiniano sta a cuore attuare degli strumenti per formare giuristi organizzandone il percorso formativo. Professori e studenti sono facce della stessa medaglia, servitori della giustizia imperiale, tanto coloro che formano quanto coloro che apprendono. L'intera filiera dell'apprendimento è contemplata, poiché come posto nelle prime righe degli stessi *Digesta*: "*Iustitia est constans et perpetua voluntas ius suum cuique tribuens*"[25].
Si potrebbe asserire che Giustiniano abbia soddisfatto il "ciclo" dell'HRM, in quanto egli progettò, scegliendo il personale adeguato ed individuandone i singoli i talenti, creò delle relazioni di lavoro, amministrò, formò e sviluppò il progetto, prevedendone poi gli effetti e premiando i collaboratori. In conclusione, la *lesson learned* di Costantinopoli appare dunque molto moderna, anche a distanza di quindici secoli e, in parte, sembrerebbe prodromica della contemporanea HRM.

---

[21] *Omnem*, praef.: «[…] *necessarium studiosis credimus, tu ex hoc optimi atque eruditissimi efficiantur; ideo præsentem divinam oratione ad vos præcipue faciendam existimamus…*»; trad.: «*noi crediamo che sia necessario insegnare agli studenti, in modo che questi, in conseguenza di ciò, diventino ottimi e preparatissimi "giuristi"; perciò riteniamo di indirizzare in modo particolare a voi la presente orazione imperiale…*» (SCHIPANI S., p. 29).
[22] Cfr. PASQUINO P., *La fortuna di 'Omnem' in età medievale: i luoghi di insegnamento del diritto*, in *Teoria e Storia del Diritto Privato* 8 (2014), pp.1-38 [www.teoriaestoriadeldirittoprivato.com].
[23] Cfr. Cost. *Omnem*, §§2-5.
[24] Cost. *Omnem*, §11: «*Incipite igitur legum doctrinam eis dei gubernatione tradere et viam aperire quam nos invenimus, quatenus fiant optimi iustitiæ et rei publicæ ministri et vos maximum decus in omne sæculum sequator: quia vestris temporibus talis legum inventa est permutatio,* […] *quæ omnia optinere sancimus in omne ævum, ab omnibus tam professoribus quam legum auditoribus et librariis et ipsis et iudicibus observanda*» (SCHIPANI S., p. 37).
[25] D.1.1.10: trad.: "*la giustizia è la costante e perpetua volontà di attribuire a ciascuno il suo diritto*".

WANDA NOCERINO

È Dottore di ricerca in Scienze Giuridiche (XXXIII Ciclo), presso l'Università degli Studi di Siena dal 16 dicembre 2020. Attualmente è Ricercatore universitario a tempo determinato presso il Dipartimento di Scienze Sociali dell'Università di Foggia. Dal 2017 è docente presso scuole dottorali, nonché Corsi di formazione della Polizia di Stato e dell'Arma dei Carabinieri e presso il Ministero dell'Interno.

LA NECESSARIA CONTAMINAZIONE DEL MAINSTREAM MILITARE IN RISPOSTE ALLE NUOVE MINACCE ALLA SICUREZZA NAZIONALE

ABSTRACT

Il contributo si propone di individuare soluzioni innovative per supportare una transizione digitale per la Difesa in termini "efficientisti", partendo dall'elevato grado di potenzialità/capacità informativa degli apparati militari e puntando sulla loro dimensione operativa per rispondere alle vecchie e nuove minacce – come quelle cibernetiche – con un approccio "sistemico" e integrato.

This paper aims to identify innovative solutions to support a digital transition for Defense in "efficient" terms, starting from the high degree of information potential/capacity of military systems and focusing on their operational dimension to respond to old and new threats - such as cyber ones - with a "systemic" and integrated approach.

Il contesto di riferimento

In via preliminare – ancor prima di affrontare le criticità giuridiche che si frappongono al pieno asservimento operativo dei progressi maggiormente dirompenti recati dalle nuove tecnologie digitali –, pare doverosa una riflessione circa il peculiare momento storico-politico e l'attuale evoluzione geo-economica che coinvolge l'assetto planetario in cui la Repubblica italiana riveste un ruolo di prim'ordine, in ragione della sua collocazione strategico-territoriale rispetto a uno dei punti geografici più sensibili agli "smottamenti" geo-politici.

É ben noto che il terrorismo internazionale, le minacce cibernetiche, la manipolazione informativa e – ancor di più – la recente "restaurazione" di un contesto geo-politico di *Cold War* stanno ridisegnando le forme di manifestazione degli attacchi alla stabilità della Repubblica che, in molte circostanze, si concretizzano in pericoli in cui vi è un totale appiattimento tra prevenzione e repressione.

Si tratta, in buona sostanza, di una "minaccia liquida" [26], caratterizzata dall'assenza di un fronte ben definito: di fatto, oltre a non esistere un pericolo materiale da collocare in una precisa area geografica, non è neppure dato individuare un *target* fisico da abbattere, posto che le insidie di cui si discorre promanano dall'etere digitale e si manifestano nel mondo reale.

Ciò significa che la "guerra" si combatte anche con metodi diversi da quelli tradizionali (meglio, convenzionali); non sono sempre ravvisabili formazioni militari paragonabili a brigate, divisioni e corpi d'armata, così come non sono sempre presenti le armi convenzionali quali unici strumenti di lotta all'integrità dello Stato.

Quindi, il concetto tipico di guerra non risulta più universalmente applicabile e le attività condotte al di sotto della soglia del tradizionale conflitto armato rappresentano le nuove forme di minaccia per la sicurezza dello Stato e l'integrità della Repubblica.

Come già sostenuto, «[I]l tipico campo di battaglia [...] non è più, o è solo raramente, quello classico in cui si contrastano le Forze armate di Paesi sovrani avvalendosi della potenza di

[26] DI LIDDO M., *La minaccia liquida*, in «Insurance review» (2019), p. 1.

fuoco e della capacità di manovra nel generale, ancorché non universale, rispetto delle norme del diritto internazionale di guerra»[27].

Ci si trova, così, a confrontarsi con uno scenario internazionale caratterizzato da uno stato di competizione permanente tra gli attori (c.d. *continuum of competition*), in cui il confine tra confronto e conflitto è labile, sfumato e rischia di perdere il suo significato tradizionale.

Si pensi in particolare alla minaccia cibernetica[28], una guerra dematerializzata in grado di danneggiare gravemente le infrastrutture strategiche del Paese. Si tratta di pericoli che, seppur immateriali, sono in grado di produrre ricadute assai violente nella realtà fisica, attentando così alla sicurezza nazionale[29].

Come evidenziato già nel 2017, «[L]e prossime guerre tra gli Stati non saranno certamente condotte soltanto con i tradizionali strumenti di offesa e di difesa via terra, mare e aria, ma saranno accompagnate e probabilmente iniziate – e in qualche caso vinte – con attacchi perpetrati attraverso lo spazio cibernetico. Questi sono infatti suscettibili di infliggere al nemico danni gravissimi, con effetti sulla società che gli esperti considerano paragonabili a quelli di armi convenzionali»[30].

Il conflitto in Ucraina rappresenta l'esempio lampante dell'arretratezza del concetto del "sotto-soglia". L'Italia, infatti, seppur non soggetta ad alcun attacco armato convenzionale, ha subito e sta subendo forti pressioni (vere e proprie minacce) indirette che si ripercuotono sugli assetti diplomatici (si pensi alle minacce nucleari alla NATO), sugli assetti informativi (con campagne di *fake news* capaci di minare la sovranità nazionale), e sugli assetti economici (si pensi alle ripercussioni sui mercati dell'energia e dei prodotti alimentari).

Dunque, i frequenti attacchi malevoli allo spazio cibernetico che colpiscono processi vitali dell'amministrazione o della vita democratica (si pensi alle *fake news* o alle manipolazioni comunicative) sono atti a provocare danni materiali paragonabili a quelli di guerra, mediante il sabotaggio a distanza di macchine e dispositivi (centrali elettriche, nucleari, dighe, torri di controllo aeroportuali, sistemi di navigazione aerea, nonché fabbriche altamente automatizzate, che impieghino *robot* interconnessi, ecc.), ben al di fuori delle regole dello "*ius in bello*", che vengono in buona sostanza aggirate e la cui assenza determina una disparità di condizioni che per il sistema Difesa si traduce in un *vulnus* giuridico, fonte di mortificazione del grado di operatività e di efficienza dello Strumento militare[31].

Di conseguenza, il *mainstream* militare è chiamato a mettere in cantiere operazioni caratterizzate da schemi "atipici", strumenti tecnologici che richiedono un elevato grado di

---

[27] Così PISANO V., *L'intervento militare quale moltiplicatore del terrorismo globale? Apporto e limiti delle forze armate e dell'intelligence militare nella lotta contro il terrorismo*, «www.difesa.it» (2008). Come si legge nel *Dossier* della Camera dei Deputati sulla *Sicurezza e Difesa nello spazio cibernetico,* del 21 dicembre 2017, p. 1, «[L]a guerra e la difesa cibernetica tra Stati sono ad oggi, a parte alcune avvisaglie, uno scenario soltanto possibile, al pari della guerra nucleare. Come tuttavia evidenziato da un numero crescente di analisi strategiche, lo spazio cibernetico è il nuovo fondamentale campo di battaglia e di competizione geopolitica dell'umanità».

[28] Per minaccia cibernetica deve intendersi il complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanziano – in particolare – nelle azioni di singoli individui od organizzazioni, statali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a controllare indebitamente, danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi. Gli attacchi cibernetici – che possono originare da qualsiasi punto della rete globale – sono in grado di determinare rilevanti conseguenze anche sulle infrastrutture informatizzate critiche di interesse nazionale: sono quindi caratterizzati da forte asimmetria. Cfr. DPCM 23 gennaio 2013 e DPCM 17 febbraio 2017.

[29] Non va dimenticato che il pregiudizio alla sicurezza nazionale è stato di recente cristallizzato nell'art. 1 del D.P.C.M. n. 131 del 20 luglio 2020, che lo declina come «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale». L'azione offensiva può essere minacciata o realizzata da uno Stato contro un altro Stato per uno qualsiasi degli scopi tradizionalmente perseguiti con il ricorso alla guerra e allo strumento militare. Quando l'attacco è portato attraverso lo spazio cibernetico, si parla di "guerra cibernetica" (cyber-warfare) e correlativamente di "difesa cibernetica" (cyber-defence).

[30] Dossier della Camera dei Deputati sulla Sicurezza e Difesa nello spazio cibernetico, del 21 dicembre 2017, 1

[31] Sul punto, cfr. nt. 27 e 28.

competenza tecnica e contraddistinti dall'incalcolabilità di rischi ed effetti collaterali.

L'importanza delle informazioni nel modello DIME e nelle operazioni multidominio

Come si è avuto modo di evidenziare, lo spettro delle possibili tipologie di conflittualità in cui il sistema Difesa ha il dovere di inserirsi è (e sarà) ancora più ampio rispetto a quello affrontato nel recente passato. Nel campo militare, infatti, la circostanza che la tecnologia ICT (*Information and Communications Technology*) sia munita di potenzialità offensive assimilabili a quelle dell'attacco armato convenzionale (ma viceversa meno ponderabili sul piano degli effetti sulla stabilità dell'ordine interno) implica che la Difesa, per poter assolvere in modo efficiente la funzione che le è propria, reagisca all'attacco con una rapidità di azione tale da non garantire agli operatori "nemici" di mettere in campo le più adeguate strategie e manovre.

Sul piano metodologico, l'assenza di un congruo lasso temporale di reazione che permetta un'adeguata ponderazione strategica dell'attività difensiva da porre in essere, rende pertanto necessario l'implementazione della capacità informativa quale prodromo essenziale di ogni processo decisionale, al fine di pianificare in modo preventivo le soluzioni per neutralizzare la potenziale minaccia.

Inevitabilmente, in questo rinnovato contesto, la Difesa è chiamata ad assumere il controllo del dominio cibernetico – quello che viene definito il «sesto continente»[32] –, da intendere sia come spazio, ambiente "autonomo", sia come ambito funzionale a garantire la piena capacità operativa ai domini più tradizionali (terrestre, marittimo, aereo, spaziale); del resto le azioni condotte a livello *cyber,* pur sviluppandosi in una dimensione immateriale ed eterea, producono effetti concreti nel mondo reale[33].

Perché questo accada, è indispensabile garantire al comparto militare la superiorità informativa – cioè la capacità di acquisire, proteggere e processare la mole di informazioni necessarie per il conseguimento di una più approfondita conoscenza e di un maggiore apprezzamento delle situazioni di rischio per aspirare alla sovranità digitale[34] –, funzionale a preservare la superiorità decisionale nella gestione degli attacchi contro la Repubblica tramite l'implementazione del già avviato processo di integrazione interforze: occorre, cioè, acquisire le informazioni strategiche necessarie a rendere efficiente le attività della Difesa nei diversi "teatri operativi", avvalendosi del supporto di strutture di Comando e Controllo compiutamente multidominio.

Si intende dire che il presupposto per creare un vantaggio decisionale è rappresentato dalla c.d. "superiorità informativa" che, al pari di quella cognitiva[35], è un *asset* immateriale imprescindibile dell'arsenale della Difesa, in grado di determinare il controllo degli equilibri strategici.

Dunque, per poter decifrare e comprendere le minacce circostanti, gestendo al contempo risposte efficaci, tempestive e capaci di generare effetti duraturi nel tempo e in tutti i domini di riferimento (terra, mare, aria, *cyber* e spazio), oltre che nell'ambiente informativo e nella sfera cognitiva, la Difesa ha l'esigenza di possedere reali capacità multidominio, in grado di assicurare la sincronizzazione delle azioni e degli effetti.

---

[32] Così CALIGIURI M., *Cyber Intelligence: tra libertà e sicurezza*, Roma 2016, p. 4.

[33] CHAUMETTE, A. L., *International Criminal Responsibility of Individuals in Case of Cyberattacks,* in «International Criminal Law Review» 18 (2018) pp. 1-35, per cui i *cyber* attacchi mettono in discussione il tradizionale principio di territorialità del diritto internazionale. La geo-localizzazione dell'attacco è tuttavia un passo fondamentale nella definizione del contesto delle condotte criminali internazionali, ad esempio nella valutazione dell'esistenza di un'aggressione, nella definizione di un conflitto come IAC (*International Armed Conflict)* o NIAC (*Non-International Armed Conflict*) o nella valutazione della giurisdizione territoriale della Corte Penale Internazionale (*ICC, International Criminal Court*).

[34] *Documento programmatico pluriennale della Difesa per il triennio 2022-2024,* Ed. 2022, p. 40.

[35] Quella cognitiva è una delle tre dimensioni degli effetti strategici, insieme a quelle fisica e virtuale. In particolare, la dimensione cognitiva afferisce alla sfera delle percezioni e delle decisioni, nella quale possono essere conseguiti effetti sociali e psicologici che influenzano il comportamento di un individuo ottenendo così un risultato duraturo.

In tale contesto, lo Strumento militare deve contribuire a garantire la difesa del Paese e degli interessi nazionali attraverso un'azione integrata e sincronizzata con gli altri strumenti del *national power* (c.d. DIME - Diplomatico, Informativo, Militare ed Economico), nell'ambito del *continuum of competition* per influenzare gli avversari e contrastarne le azioni, tutelando, al contempo, i propri interessi.

È quindi indiscutibile che il moderno concetto di sicurezza nazionale, «ossia quel novero di valori indispensabili sui quali si basa la stessa sopravvivenza della Repubblica [intesa] come comunità di istituzioni e di cittadini e quelle indefettibili necessità ultra-individuali legate al mantenimento delle condizioni essenziali per tenere una nazione unita e proteggerne lo sviluppo»[36], abbia inglobato nel suo paradigma la protezione dello spazio e del dominio *cyber*.

Tale modernità la si coglie nel fatto che, accanto alle esigenze più tradizionali – quali la difesa dello Stato democratico e delle istituzioni poste dalla Costituzione a suo fondamento –, vengono individuate nuove aree di intervento (economia, industria, energia, tecnologia) che richiedono un approccio metodologico integrato e un *mainstream* militare "allargato".

In sostanza, sul piano socio-politico, si assiste a un processo di emancipazione della dimensione della sicurezza che non è più circoscritta allo Stato-apparato (in cui è lo Stato stesso ad essere monopolista dei beni giuridici da proteggere), ma assume una nuova conformazione, riferita allo Stato-comunità e alle sue plurime e trasversali espressioni in campo sociale, industriale, economico, scientifico e cibernetico.

Questo stato di cose spinge il sistema Difesa verso un processo di "riassetto", che tenga conto, nella propria organizzazione, del ruolo operativo della prevenzione, che allo stato attuale rappresenta l'unica metodologia in grado garantire un intervento efficace e tempestivo di contrasto e neutralizzazione delle minacce alla sicurezza nazionale[37].

Occorre, in altre parole, cominciare a considerare le dinamiche del mondo cibernetico dal punto di vista militare. Così, «[U]na volta chiarito che è possibile usare la cibernetica come arma, si pongono per essa le stesse questioni che riguardano ogni altra tipologia di arma (carri armati, navi, aerei, etc.): servono regole di ingaggio per il suo utilizzo e cornici normative per stabilire chi, quando e come può decidere di impiegarla»[38].

Come è stato precisato, «[O]ggi non si può pensare di pianificare, condurre e portare a termine un'azione militare senza il supporto di un efficace sistema di *intelligence* che sia in grado di garantire ai decisori, di tutti i livelli, gli elementi di informazione necessari a prendere le opportune decisioni, sia per la pianificazione dello strumento militare, sia per la condotta delle operazioni e delle missioni»[39].

In quest'ottica, dal punto di vista militare, la consapevolezza di ciò che accade nelle aree di interesse consente di intervenire quando e dove necessario, in presenza di "anomalie", ottimizzando e sincronizzando le risorse disponibili.

I sistemi investigativi "prestati" alla Difesa: un'auspicabile contaminazione per l'efficienza del comparto militare

L'applicazione delle tecnologie digitali (sempre più pervasive e performanti) rappresenta il mezzo principale e irrinunciabile per conseguire un vantaggio computazionale rispetto all'attuale esigenza di approvvigionare e gestire la più elevata mole di dati e informazioni

[36] Corte cost., 23 febbraio 2012, n. 40.

[37] Già nel 2006 l'Amm. Rinaldo Veri, Capo del III Rep. Pianificazione Generale dello SMM, nel corso di una Conferenza su "*Sorveglianza e controllo del Mediterraneo",* precisava che «[I] profondi mutamenti economico-sociali, correlati al lanciato processo di digitalizzazione, postulano [...] una progressiva tendenza al superamento degli interessi di parti, in settori di competenza o aree geografiche tradizionalmente definite, e l'approdo a forme di cooperazione e di integrazione sempre più articolata ed estese».

[38] *Dossier* della Camera dei Deputati sulla *Sicurezza e Difesa nello spazio cibernetico,* 2017.

[39] TRENTA E., *Difesa e Sicurezza: prevenire il radicalismo per contrastare il terrorismo,* in «www.difesa.it» (2018).

circolanti nelle svariate "corsie" dei domini oggi esistenti.
Il mondo dei *Big Data* di cui si discorre rappresenta, come noto, una nuova e incalcolabile fonte di ricchezza che ha dato vita ad un "mercato" dai tratti del tutto peculiari.
Di fatto, la "corsa" all'approvvigionamento dei *data,* oltre che essere priva di una cornice giuridica adeguata, è altresì caratterizzata dalla presenza di *competitors* il cui profilo soggettivo è indecifrabile, così come sono indecifrabili gli scopi per cui tali soggetti concorrono ad accaparrarsi la fetta più grande e importante di informazioni.
Si assiste, in buona sostanza, a un panorama conflittuale in continua evoluzione, in cui il tratto comune tra i *players* è la sola necessità di approvvigionamento sovraesposta.
Pertanto, gli Stati sovrani si trovano spesso in competizione con nuove forze concorrenti, il cui profilo è "meta-nazionale", in quanto espressione di interessi e poteri non riconducibili alle classiche forze politiche territoriali, il cui perseguimento è spesso contrastante con la stabilità e la sicurezza dell'ordine costituito.
Il sistema in parola nella sua globalità è ricco di articolazioni e la forte interdipendenza dei singoli elementi che lo compongono richiede, per chi è chiamato ad assicurare la difesa, la necessità di agire in maniera integrata per comprenderne la complessità e intervenire in maniera repentina.
In tale contesto, occorre innanzitutto mettere da parte il tradizionale modello binario, in cui classicamente si discorre di "pace e guerra", poiché si presenta inadatto a fronteggiare le moderne forme di minaccia perpetrate attraverso mezzi e strategie non convenzionali: dunque, dalla consapevolezza che anche la superiorità acquisita nei domini tradizionali potrebbe essere insufficiente e addirittura compressa in un'era in cui si assiste ad una proliferazione ininterrotta delle tecnologie a disposizione di attori statuali e non, nasce l'esigenza di un cambio di paradigma.
Tale *framework* competitivo, osservato attraverso la lente di una nuova prospettiva orientata da integrazione e interdisciplinarietà, sembra presentare – *mutatis mutandis* – gli stessi profili critici che interessano il comparto Giustizia: pur considerando che l'attività di repressione delle fattispecie delittuose è di appannaggio esclusivo dell'attività congiunta delle Forze di Polizia (c.d. polizia giudiziaria) e del sistema giudiziario, non può non rilevarsi come la descritta indecifrabilità offensiva delle nuove minacce all'integrità della Repubblica presenti tratti ontologici di indubbia comparabilità al "microcosmo" della criminalità interna o, per meglio dire, civile.
A riprova degli aspetti di cui si discorre, è emblematico fare riferimento al "palcoscenico" delinquenziale, che ha per primo somatizzato l'impatto dell'evoluzione digitale. Va, infatti, constatata la circostanza che lo spazio cibernetico, per effetto dell'indecifrabilità e per la sua peculiare capacità dispersiva, rappresenta l'ambiente ideale per celare traffici, attività illecite e l'identità di chi le attua, generando non poche difficoltà per gli inquirenti e gli investigatori nella ricostruzione dei fatti e nell'identificazione dell'autore.
Nello specifico, gli investigatori sono alle prese con una forma evoluta di criminalità, che costringe gli "addetti ai lavori" all'acquisizione di competenze strettamente tecniche, oltre che giuridiche: le Forze di Polizia, infatti, sovente necessitano dell'ausilio di figure estranee al mondo investigativo per ricostruire il fatto di reato e identificare il colpevole.
In effetti, sempre più spesso, ci si trova di fronte ad un panorama criminogeno in cui i passaggi essenziali di un disegno criminoso vengono posti in essere con l'ausilio di mezzi e tecniche innovative, difficili da identificare ed intercettare.
Si pensi alle criptovalute usate come mezzo di pagamento per la conclusione di affari illeciti, in particolare nell'ambito del narcotraffico e della ricettazione, ovvero alla creazione di aree cibernetiche "franche" (c.d. *deep web*) in cui, avvalendosi di sofisticate strumentazioni tecnologiche, è possibile mettere in piedi veri e propri *market-places* del crimine in cui è garantito – attraverso l'impiego della tecnologia *blockchain* – non solo l'anonimato degli utenti, ma altresì un elevato grado di "certezza" della conclusione degli affari illeciti, che

pertanto diventano per i loro autori più proficui e sicuri.
Da ultimo, è doveroso porre in evidenza come la tecnologia sia impiegata in via principale per criptare lo scambio di comunicazioni intercorrenti tra i protagonisti dei traffici criminosi in parola: di recente, infatti, gli investigatori si sono trovati al cospetto dei c.d. criptofonini, strumenti che consentono uno scambio comunicativo indecifrabile (*rectius:* non intercettabile) a fronte dell'elevato grado di crittografia che li caratterizza[40].
Ebbene, all'evoluzione delle forme di manifestazione del crimine corrisponde un cambiamento del modo di investigare, soggetto ad un ineluttabile adattamento al nuovo *modus delinquendi*: gli inquirenti, infatti, si trovano di fronte all'esigenza di utilizzare apparecchiature ad alto potenziale tecnico, le cui caratteristiche richiedono competenze "specifiche", solitamente estranee al *background* che caratterizza la formazione della "prassi operativa".
Pertanto, le contrapposte esigenze – da un lato garantire un'attività inquisitoria efficiente e al passo con il darwinismo tecnologico-delinquenziale, dall'altro dotare il comparto investigativo di elevate competenze tecniche estranee al sostrato culturale degli addetti ai lavori – hanno determinato un processo di contaminazione "coatta" del *mainstream* investigativo che, al fine di rendersi efficace nel compito di repressione del crimine, è stato interessato dal reclutamento di esperti "esterni" al comparto investigativo[41].
Dunque, «[N]ella rinnovata era digitale al giurista viene richiesto uno sforzo ulteriore che trascende dall'analisi del dato tecnico e impone di soffermarsi sulla realtà che dà voce al diritto. Ciò in una duplice prospettiva: da un lato, garantire una visione olistica e non più parcellizzata delle problematiche che sottendono le scelte legislative e disciplinari; dall'altro, vedere il prodotto normativo calandolo nella dimensione del presente, passato e futuro»[42].
Di conseguenza, si determina una contaminazione anche del comparto Giustizia, il cui riverbero – per diretta esperienza di chi scrive – ha dato luogo ad una rivisitazione del settore della Ricerca di area giuridica, sempre più improntata alla conoscenza del sostrato tecnico per comprendere al meglio le problematiche giuridiche determinate dall'evoluzione tecnologica.
In uno scenario come quello descritto, i tratti comuni all'evoluzione del *modus* "di delinquere" e quello "di fare guerra" rappresentano i presupposti utili a supportare un processo di contaminazione del mondo militare con istanze di stretta pertinenza di una "fetta" del mondo giuridico, più precisamente quello investigativo.
Ebbene, i tangibili riscontri positivi derivanti dalla contaminazione del sistema Giustizia – il cui risultato ha portato ad un'efficiente attività repressiva della *Criminal-tech* –, e i profili di compatibilità degli assetti problematici comuni al sistema di Giustizia e a quello di Difesa, pongono la presente ricerca a prospettare un approccio "mutualistico" dallo Strumento militare a quello investigativo.
Di qui si propone per la Difesa un percorso di contaminazione assimilabile a quello intercorso nel sistema giudiziario, tenendo in debita considerazione il maggior vantaggio che le Forze

---

[40] Sul punto, per tutti, CURTOTTI D., RIZZI V., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale,* in «Sistema penale» 6 (2023), pp. 173-196.
[41] Si pensi a quanto è accaduto in rapporto all'uso investigativo dei *virus Trojan*. Più che altrove, infatti, l'indagine sul dato tecnico-operativo diviene imprescindibile oltre che doverosamente virtuosa per il giurista: di fronte alla natura anfibia e polivalente del *software*, solo un preliminare vaglio circa il funzionamento del programma rende possibile l'individuazione delle problematiche che sottendono l'impiego del captatore informatico nelle indagini e nel processo penale. Più precisamente, un approfondimento delle differenti opzioni funzionali del *virus* consente, da una parte, di rintracciare le similitudini e le differenze che intercorrono tra i risultati investigativi prodotti dall'impiego del *Trojan* rispetto ai tradizionali istituti processuali; dall'altra, di misurare l'impatto derivante dalla tecnologia applicata al processo sullo spazio vitale (fisico e digitale) protetto e riconosciuto dalla Carta fondamentale e dalle Convenzioni internazionali. Tentando una semplificazione, solo la prodromica analisi tecnico-operativa ha consentito di individuare il punto di equilibrio tra ciò che è possibile (sotto il profilo tecnico) tramite l'ausilio del *Trojan* e ciò che è anche lecito secondo le norme processuali e i relativi "corredi" interni e sovranazionali.
[42] NOCERINO W., *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Padova 2021, p. 2.

Armate possono trarre dalle capacità operative delle tecnologie investigative, il cui potenziale è compresso dal *civil use* a cui esse sono destinate.
In altri termini, si potrebbe paventare la possibilità di "prestare" al sistema Difesa quell'insieme di tecnologie di indagine di ultima generazione impiegate dalle procure con finalità d'indagine, ma utilizzate al "minimo" nel settore investigativo per effetto degli "scopi civili" che animano la funzione giudiziaria, la quale inevitabilmente deve tener conto delle garanzie costituzionali e convenzionali poste a presidio delle libertà fondamentali degli indivudui.
Ebbene, le *skills* gestionali-operative di cui sono muniti tali strumenti sembrano poter rappresentare un'utile soluzione per il comparto militare, allorquando il campo d'azione non presenti i tratti tipici del conflitto bellico, essendo l'attività di Difesa condotta anche in condizioni "ordinarie".
In quest'ottica, le Forze Armate, perseguendo scopi di difesa della Repubblica che vanno oltre le garanzie individuali, sarebbero autorizzate ad impiegare la tecnologia investigativa al massimo delle sue potenzialità operative.
Ciò implica la necessità di migliorare il quadro giuridico di riferimento che, allo stato dell'arte, non sembra consentire alla Difesa (quando si è al di sotto della soglia di conflitto) di sviluppare adeguatamente le proprie capacità militari.
Inoltre, il vantaggio apportato da tale "contaminazione" – oltre ad essere quantificato in termini di efficacia operativa – potrebbe altresì determinare un innalzamento dell'efficienza del sistema Difesa.
Nello specifico, si vuole fare riferimento al superamento di un *bias* funzionale insito nella ripartizione di competenze cui si accennava in precedenza tra servizi di informazione e Difesa.
In buona sostanza, la capacità informativa propria degli strumenti investigativi in parola, conferirebbe al *mainstream* militare maggior "completezza" sul piano dell'operazione da attuare, in quanto l'uso di tali tecnologie permetterebbe, "*uno actu*", di ottenere informazioni sensibili e operare prontamente, senza dover necessariamente incorrere nell'attesa del tempo necessario a ricevere dati per pianificare e intervenire tempestivamente.
In sintesi, l'uso pressoché illimitato dei *tools* investigativi permetterebbe alla Difesa di coniugare in un unico strumento capacità ed attività di competenza di comparti estranei al rispettivo dicastero, innalzando il livello di reattività e l'efficienza della neutralizzazione della minaccia, nell'ottica di un sistema difensivo multidominio integrato.

Le potenzialità multidirezionali degli strumenti tecnologici di "indagine"
Con il dichiarato intento di supportare la contaminazione del *mainstream* militare con l'utilizzo delle *skills* operative delle tecnologie d'indagine, si procede ora ad illustrare l'ampio spettro di potenzialità di cui il variegato arsenale degli strumenti tecnici di indagine è munito.
Prima è però doverosa una premessa di carattere metodologico: affrontando il tema sotto il profilo "giuridico-ordinamentale", ogni riferimento ad aspetti di natura puramente tecnica – ossia quelli relativi alle caratteristiche ontologiche degli strumenti oggetto d'interesse – dovrà intendersi meramente "descrittivo" e non rappresentativo di una rassegna tecnico-operativa delle funzionalità delle apparecchiature tecnologiche cui si fa riferimento.
Da alcuni anni, il mondo giuridico è stato chiamato a confrontarsi con tecnologie (*hardware* e *software*) che, in ragione delle enormi potenzialità intrusive e captative, rappresentano un agevole strumento di indagine.
In buona sostanza, nell'ultimo tempo, il contrasto alla criminalità da parte delle procure è stato reso efficiente da un affinamento della precisione investigativa attraverso l'impiego di *software* malevoli, i c.d. "*virus Trojan*" (anche chiamati captatori informativi), nonché tecnologie strumentali al miglioramento della loro applicazione, tra i quali di notevole

interesse è l'IMSI *Catcher*[43].
Ebbene, durante il loro impiego, è balzato agli occhi degli operatori di settore l'enorme potenziale insito in dette strumentazioni, la cui multifunzionalità si scontra con l'unico binario sul quale il sistema giudiziario è incardinato, ovvero quello investigativo.
Più nello specifico la "multidirezionalità" di cui si discorre si concretizza in:
A) capacità captativo-conservativa, di peculiare interesse dell'apparato Giustizia, che in modo "statico" consente agli inquirenti di accedere ad informazioni sensibili relative a target processualmente rilevanti con modalità non-convenzionali, in grado di assicurare un elevato standard di segretezza investigativa;
B) capacità gestionale, consistente nella possibilità, attraverso il virus malevolo, di compiere operazioni modificative del contenuto gestito dalla macchina bersaglio, attraverso un controllo da remoto che può tradursi in acquisizione, modificazione e cancellazione di contenuti;
C) capacità operativa, insita nel potenziale impiego del *software* malevolo non solo per gestire da remoto la macchina bersaglio, ma addirittura per impiegarla come mezzo d'azione; lo strumento controllato da remoto, infatti, può essere indirizzato al compimento di attività meccaniche capaci di provocare alterazioni del mondo esterno, oltre che dello status quo della macchina.
Precisamente, a fronte della cancellazione di una funzione vitale della macchina infettata (capacità gestionale), cui consegue la neutralizzazione della sua operatività, si potrebbe alterare la medesima funzione con il diverso effetto di deviare il corretto funzionamento della macchina, costringendola all'esecuzione di un comando difforme, in grado di provocare un danno (capacità operativa).
Nella piena consapevolezza dell'avanguardia operativa del comparto Difesa, conviene vagliare la possibilità di applicare tali sistemi in chiave difensiva: infatti, se sotto il profilo squisitamente investigativo i virus informatici sono utili a dar luogo ad attività captative (*rectius*: intercettazioni di flussi comunicativi anche in via informatico-telematica) per acquisire elementi utili alle indagini e/o a prevenire fatti di particolare allarme sociale, nel campo militare potrebbero consentire il pieno controllo di sistemi ostili in chiave strategica, per acquisire – nel più breve tempo possibile – dati e informazioni che consentano *de facto* di raggiungere la superiorità informativa e cognitiva.
Naturalmente, le capacità di cui si discorre devono essere ricondotte, sul piano fattuale, ad uno scenario "ordinario", al fine di assicurare al comparto Difesa efficienti mezzi di contrasto alle minacce "liquide" con una rivisitazione dell'architettura normativa che attualmente imbriglia la piena esplicazione dello Strumento militare in un contesto estraneo alla dimensione conflittuale.

Segue: La "sterilizzazione" giuridica alla luce del *civil use*

A dispetto delle enormi potenzialità informativo-investigative dei *software* malevoli, il mondo giuridico tende a "comprimerne" le funzioni in nome di precetti costituzionali e convenzionali che – inevitabilmente – si impongono nel circuito processual-penalistico, limitando l'uso di tecniche di indagine eccessivamente pervasive al fine di evitare una lesione ingiustificata delle garanzie fondamentali[44].
In altri termini, i principi costituzionali e convenzionali sono il principale argine

[43] NOCERINO W., *Il tramonto dei mezzi di ricerca della prova nell'era 2.0,* in «Diritto penale e processo» 8 (2021), pp. 1017-1030.
[44] Ci si riferisce, in particolare, all'art. 13 Cost., baluardo della libertà di ogni individuo, all'art. 14 Cost., posto a protezione del domicilio e all'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, nonché, spostando lo sguardo oltre i confini nazionali, il principio di proporzionalità che impone, ai sensi dell'art. 8 CEDU, la necessità di una perfetta corrispondenza tra i risultati perseguiti e i mezzi adoperati e, più in particolare, tra la potenziale forza invasiva del mezzo in esame e l'inevitabile lesione dei diritti fondamentali.

all'estrinsecazione delle proteiformi funzioni che le tecniche di indagine da remoto sono in grado di esperire.
In effetti, il legislatore nazionale – tra le diverse alternative prospettabili – ha scelto di limitare le funzionalità del *Trojan* alla sola captazione di conversazioni e comunicazioni tra presenti[45] e, a seguito di una più recente impostazione giurisprudenziale, alle intercettazioni telematiche[46].
Di conseguenza, il *virus* informatico può essere usato solo nei confronti di soggetti identificati[47], allorquando emergano "gravi" o "sufficienti" indizi di reato[48] ovvero "specifici elementi che giustificano l'attività di prevenzione"[49], per un tempo limitato[50], solo su autorizzazione dell'autorità giudiziaria[51], con il precipuo intento di evitare che il sistema si appresti ad accogliere forme di sorveglianza perpetua ritenute illegali perché in contrasto con le norme costituzionali (artt. 14 e 15 Cost.) e convenzionali (artt. 6 e 8 CEDU).
Sintetizzando: in nome della riserva di legge e di giurisdizione, le altre funzioni del *virus* – al netto delle intercettazioni – sono inibite dalla legislazione vigente[52]; dunque, nell'ordinamento nazionale, il "controllo" di qualsivoglia sistema "infetto" non può, allo stato dell'arte, essere ammesso in condizioni ordinarie.

La "crisi" dei limiti nell'attuale panorama concettuale del "conflitto bellico"
Come poc'anzi evidenziato, l'esercizio delle *skills* sussumibili nelle capacità gestionali e operative delle tecnologie ad uso investigativo risente della compressione giuridica operante sotto l'egida del garantismo delle istanze individuali che – com'è giusto – non possono sopportare una restrizione "ingiustificata".
Per esser chiari, in campo "militare", è da considerarsi "ingiusta" ogni intrusione nella dimensione privata al di fuori delle condizioni di straordinarietà che si palesano in ipotesi di

---

[45] Una simile impostazione traspare nitidamente dai criteri direttivi contenuti nella legge delega (fr. art. 1, comma 84, lett. *e*, n. 1 della l. 23 giugno 2017, n. 103, per cui «l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto»), dal successivo decreto attuativo (il d.lgs. 29 dicembre 2017, n. 216, infatti, procede alla modifica del solo art. 266, comma 2 c.p.p. al fine di prevedere una nuova modalità di esecuzione delle intercettazioni tra presenti mediante l'inserimento di un captatore informatico inoculato su dispositivi elettronici portatili) e dagli spasmodici interventi riformatori. A ben guardare, né la l. 9 gennaio 2019, n. 3, né la l. 28 febbraio 2020, n. 7, apportano modifiche all'impianto predisposto dal legislatore precedente in relazione all'inquadramento giuridico dell'attività condotta tramite *Trojan*.
[46] Cass., Sez. V, 30 maggio 2017, n. 48370, in *C.E.D. Cass.,* n. 271412.
[47] Cfr. art. 267, comma 1, c.p.p.
[48] Nel caso di intercettazioni "processuali" (ossia quelle esperiti nel corso di un procedimento penale già avviato), affinché il giudice proceda ad autorizzare l'attività captativa, è necessario che sussistano «gravi indizi di reato» e che l'intercettazione sia «assolutamente indispensabile alla prosecuzione delle indagini». Per i reati "gravi" (rientranti nel c.d. "doppio binario investigativo), quali ad esempio terrorismo o criminalità organizzata, l'art. 13 del d.l. 152 del 1991 prevede che bastano "sufficienti indizi" e la mera "necessità" della captazione.
[49] Ci si riferisce alle intercettazioni preventive, di cui all'art. 226 disp. att. c.p.p., per cui è possibile ricorrere all'uso del *virus* informatico.
[50] Nel caso di intercettazioni giudiziarie, per i reati tradizionali, la durata delle intercettazioni non può superare i quindici giorni, prorogabile per periodi successivi di quindici giorni, ovvero per quelli "speciali", la durata non può superare i venti giorni, prorogabile di ulteriori venti giorni. Nel caso di intercettazioni preventive, la durata massima è di quaranta giorni, prorogabile per periodi successivi di venti giorni ove permangano i presupposti di legge.
[51] Il giudice procedente, nel caso di intercettazioni giudiziarie, ovvero il procuratore della Repubblica, nel caso di intercettazioni preventive "di polizia" o il procuratore generale presso la Corte d'Appello di Roma, nel caso di intercettazioni preventive "d'*intelligence).*
[52] ORLANDI R., *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in *La giustizia penale preventiva. Ricordando Giovanni Conso*, Milano 2021, pp. 37-46; SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Torino 2018, pp. 10 e ss.

conflitto bellico[53].

Pertanto, per autorizzare un impiego operativo delle tecnologie digitali di controllo nel senso sopra illustrato, devono inevitabilmente essere accertate concrete circostanze critiche per la difesa nazionale e, dunque, un "conflitto armato" in grado di consentire un abbassamento delle garanzie individuali in nome delle esigenze di sicurezza collettiva[54].

Non va, però, sottovalutato il cambio di paradigma cui si assiste nell'ultimo tempo. Il contesto nazionale, infatti, si mostra particolarmente instabile rispetto al passato[55]: oggi, ci si confronta con nuove minacce ibride, particolarmente insidiose perché trasversali, multiformi e "silenti", in continua evoluzione e spesso sotto la soglia dell'aperta aggressione.

Di conseguenza, il concetto tipico di conflitto militare non risulta più universalmente applicabile e le attività condotte al di sotto della soglia rappresentano una crescente minaccia per la sicurezza al pari delle minacce fisiche.

In quest'ottica, occorre interrogarsi sull'attuale validità del c.d. "sotto-soglia" in un contesto in cui il concetto di "conflitto" assume dimensioni non convenzionali e nel quale gli attacchi all'integrità del Paese sono tutt'altro che visibili, ma non per questo meno dannosi di quelli esperiti sul campo di battaglia[56].

Le recenti vicissitudini storiche sono emblematiche di quanto si discorre. Infatti, è palese come, nonostante le accreditate informazioni concernenti i nefasti effetti sanitari della diffusione del Covid-19 nella città di Wuhan e le correlate informative provenienti dai servizi di informazione di diversi Paesi, non si sia potuto procedere a un preventivo isolamento e neutralizzazione della minaccia in nome dell'impossibilità giuridica di limitare la circolazione di mezzi, cose e persone, di fronte ad un'ipotesi "flebile" di un'attuale pericolosità di contagio.

In altri termini, l'insussistenza di un grado di "attualità" e "concretezza" della minaccia[57] hanno impedito di scongiurare la diffusione globale di una pandemia, provocando *ex post* una maggiore compressione delle libertà fondamentali di quella necessaria a prevenire l'importazione in Occidente di una pandemia dagli effetti globali catastrofici.

L'insegnamento che il modo di affrontare le avvisaglie della pandemia ha lasciato in eredità al mondo giuspolitico è quello di dover ripensare all'impostazione del concetto di "ordinarietà" e di conseguenza rielaborare i tratti ontologici delle idee di "conflitto" e "difesa" nazionale, con ciò imponendo una rivisitazione dei parametri posti alla base del principio di proporzionalità che, come detto, è il principale limite all'uso militare della tecnologia in contesti di (apparente) non ostilità (fisica).

---

[53] L'assenza di una definizione di "minaccia di uso della forza" o "uso della forza" nella Carta delle Nazioni Unite ha portato a un problema di interpretazione. Questa lacuna è stata colmata con l'adozione della risoluzione 3314 dell'Assemblea generale delle Nazioni Unite sulla definizione di aggressione (1974), con la quale gli Stati hanno stabilito per consenso che per forza, ai sensi dell'articolo 2, paragrafo 4, della Carta delle Nazioni Unite, si intende la forza armata. Sul punto cfr., su tutti, ROSCINI, M., *Cyber Operations and the Use of Force in International Law*, Oxford 2018. Va comunque precisato che la Corte Internazionale di Giustizia (ICJ) ha stabilito che l'articolo 2, paragrafo 4, della Carta delle Nazioni Unite si applica a "qualsiasi uso della forza, indipendentemente dalle armi impiegate". Pertanto, l'assimilazione di alcuni attacchi informatici con la forza armata consente al Consiglio di sicurezza delle Nazioni Unite di agire ai sensi del capitolo VII e agli Stati di reagire per autodifesa (articolo 51 della Carta delle Nazioni Unite).

[54] Secondo OHLIN, J., GOVERN, K. AND FINKELSTEIN, C., *Cyber War: Law and Ethics for Virtual Conflicts*, 2015, sono tre i livelli di prova necessari per attribuire un attacco informatico a uno Stato specifico, affinché il diritto internazionale sia applicabile: "In primo luogo, il computer o i computer, o il server o i *server* da cui hanno origine le operazioni devono essere localizzati; in secondo luogo, è l'individuo che è dietro l'operazione che deve essere identificato; e in terzo luogo, ciò che deve essere provato è che l'individuo ha agito per conto di uno Stato in modo che la sua condotta sia attribuibile ad esso".

[55] In passato la pericolosità delle forze ostili era principalmente legata alla valenza politica e al potenziale militare.

[56] Si pensi al fatto che in occasione del vertice di Varsavia del 2016, la NATO ha riconosciuto che un attacco cibernetico può arrivare a causare danni paragonabili a quelli di un attacco armato e, quindi, diventare un caso di difesa collettiva ai sensi dell'art. 5 del Trattato di Washington.

[57] Per dovere di completezza, si precisa che l'attualità e la concretezza della minaccia rappresentano, in astratto, le circostanze fattuali che giustificano una limitazione delle libertà fondamentale, in nome del principio di proporzionalità.

Orbene, allargando le maglie del discorso, si pone il quesito se sia ancora il caso di subordinare l'autonomia di azione della Difesa alla sussistenza di contingenze il cui manifestarsi non segue più logiche belliche e dinamiche convenzionali.
A ben riflettere, la fluidità delle minacce cui si è fatto riferimento non può che riverberarsi sull'essenza del concetto di conflitto che – come largamente esposto – è ormai esteso alle aree strategiche riferibili al modello DIME.
Il dittico "ordinario-straordinario" appare, dunque, privo di un valido significato in un'epoca in cui guerra e attori bellici non sono determinabili sulla base di rivendicazioni e responsabilità espressamente dichiarate.
Sintetizzando: in un contesto come quello descritto, in cui inevitabilmente va ridisegnato il concetto di "conflitto", occorre anche ripensare al rapporto tra ordinarietà e straordinarietà. Nella consapevolezza che la guerra non è più solo quella fisica, ma anche quella esperita con armi invisibili, è opportuno rielaborare in chiave moderna il principio di proporzionalità tra il grado di offensività dell'arma (*rectius:* dello strumento difensivo da impiegare) e il bene giuridico da proteggere, consentendo il ricorso alle tecnologie digitali quali strumenti di emancipazione del sistema Difesa dal determinismo di altri settori dell'ordinamento, rafforzando l'influenza del comparto militare nei vari settori afferenti al DIME.
In altri termini, in chiave futuribile, deve immaginarsi che l'attività della difesa della Repubblica passi attraverso operazioni dai tratti ontologici che si discostano dall'intervento militare convenzionale e che, in particolare, richiedono l'abbandono della causa di giustificazione dello stato di necessità[58].

L'applicazione militare dei *tools*

Alla luce della ricostruzione offerta, può dirsi che il comparto Difesa sia tenuto ad agire sempre, con peso specifico differente a seconda del momento, anche sotto soglia, in uno sforzo tempestivo, integrato e nell'ambito di un unico disegno strategico nazionale.
Si intende, perciò, rielaborare l'attuale impostazione ordinamentale nella convinzione per cui appare anacronistico e privo di utilità classificare l'attività della Difesa secondo le categorie "ordinarie".
Se si estende il concetto di conflitto e si ridisegna il principio di proporzionalità, è inevitabile ripensare allo spazio operativo concesso alla Difesa nelle situazioni "ordinarie" (*rectius:* allorquando si è al di sotto della soglia conflitto): allo stato dell'arte, si ritiene utile attribuire ulteriori poteri cognitivi alla Difesa, legittimando il comparto ad utilizzare gli strumenti tecnici di controllo remoto anche al di sotto della soglia di conflitto armato, così da adeguare lo *standard* difensivo al mutamento degli interessi e degli obiettivi degni di protezione in quanto espressione di un allargato concetto di stabilità della Repubblica.
In quest'ottica, l'uso di tecnologie "invasive" da parte delle Forze armate non può più ritenersi *stricto sensu* attività militare e come tale esercitabile (ed autorizzata) in sole condizioni di eccezionalità, ritenendosi viceversa doverosa e necessaria in ogni dimensione del modello DIME.
In particolare, allorquando gli operatori del settore, nell'esercizio delle rispettive attribuzioni, ravvisino la sussistenza di indici sintomatici di un danno grave e irreparabile, ancorché potenziale, a centri di interesse sensibili e strategici in grado di comprometterne il regolare funzionamento, deve ritenersi possibile l'uso di strumenti tecnici in grado di porre tempestivo rimedio alla situazione di pericolo attraverso attività operative e gestionali proprie dei *software* malevoli.
L'esercizio "generalizzato" di simili poteri cognitivi, per poter essere applicato nel rispetto del (seppur rinnovato) principio di proporzionalità, necessita di apposite linee guida e protocolli operativi che ne indirizzino l'impiego.

---

[58] Cfr. *Considerazioni conclusive.*

Più concretamente, la pluralità degli interessi in gioco richiede l'instaurazione di un Tavolo Tecnico di coordinamento composto dagli Strumenti del Potere nazionale e dagli esponenti del mondo giuridico, con lo scopo di definire i parametri, le regole, i limiti e le condizioni per consentire un uso "adeguato" e proporzionato dei sistemi di cui si discorre.
L'obiettivo finale – in aderenza a quanto già accade in altri Paesi alleati[59] – è quello di garantire al comparto militare l'autonomia operativa nel suo complesso e, al suo interno, l'esercizio delle attribuzioni nel pieno rispetto della catena di comando, anche attraverso la creazione di un organo interforze per pianificare gli indirizzi strategici delle politiche estera, di difesa e di sicurezza, in cui, a fronte di una composizione puramente "tecnica", il controllo di legittimità sia affidato ad una Commissione bicamerale *ad hoc*[60].
Al contempo, la proposta consente di favorire la cooperazione tra Difesa e settore privato, chiamato a sviluppare – in fase di approvvigionamento – le tecnologie necessarie a preservare la superiorità nazionale dell'Alleanza e realizzare soluzioni idonee a soddisfare i requisiti operativi.

Rischi e criticità

Giunti a questo punto della ricerca, occorre interrogarsi sulla fattibilità a livello pratico e operativo del supporto tecnologico al *mainstream* militare oggetto di proposta.
In questa prospettiva, è indispensabile esaminare il rapporto tra le "rinnovate" esigenze di Difesa e la tutela di taluni diritti inviolabili che presenta, *prima facie*, le medesime criticità che impegnano il mondo giuridico tutte le volte in cui è chiamato ad interfacciarsi con il più "tradizionale" tema della raccolta di informazioni in sede giudiziaria o preventiva[61], che (non di rado) determina una compressione di situazioni giuridiche soggettive costituzionalmente e convenzionalmente garantite (artt. 14 e 15 Cost. e art. 8 CEDU).
Va peraltro considerato che un'attività pubblica limitativa delle libertà positive risulta ancor meno tollerata allorquando, oltre ad essere condotta in assenza di un quadro indiziario e circoscritta ad operazioni di *surveillance* strategica, implichi – come nell'ipotizzata applicazione operativa delle *skills* militari dei *tools* investigativi – anche l'invasione sostanziale della sfera privata[62].
A ben guardare, l'uso operativo delle tecnologie di indagine per finalità strategiche – secondo quanto proposto dal presente lavoro – da un lato rappresenta un valido e innovativo strumento capace di fronteggiare in modo "attivo" gravi *pericula* di attacco all'integrità della Repubblica, dall'altro realizza un'alterazione della libera autodeterminazione individuale.
Si tenga inoltre presente che, in assenza dei presupposti costituzionali per procedervi (riserva di legge e di giurisdizione), il *vulnus* determinato da operazioni che, seppur condotte per finalità difensive, non tengano conto delle predette cautele, rischia di generare un paradosso giuridico: in nome della difesa della stabilità e della sicurezza dell'assetto costituito, si finisce per violare i principi che ne sono alla base.
In primis, è il caso di precisare che il sistema giuridico italiano contempla forme di limitazione alle libertà personali, purché queste – oltre che essere astrattamente ammesse da una previsione legislativa *ad hoc* – siano in concreto autorizzate, solitamente in via preventiva, dalla sussistenza di un provvedimento giurisdizionale che effettui una valutazione specifica dell'adeguatezza della restrizione alla "pericolosità" del soggetto e della circostanza che la misura limitativa mira a neutralizzare (art. 13 Cost.).

---

[59] Si pensi a quanto accade in altri Paesi (come Francia, Gran Bretagna, Israele, Canada, Australia, Brasile, Romania e Sudafrica) che si sono dotati di un Consiglio di Sicurezza Nazionale per la predisposizione di strategie volte alla tutela degli interessi nazionali.
[60] Sulla proposta *de qua,* cfr. *Considerazioni conclusive.*
[61] Ci si riferisce, più concretamente, all'istituto delle intercettazioni sia in ambito procedimentale (artt. 266 ss. c.p.p.) che in ambito preventivo (art. 226 disp. att. c.p.p.).
[62] CINELLI C., *Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani*, in «Ordine internazionale e diritti umani» (2020), pp. 588-608.

Inoltre, sul piano squisitamente tecnico, le tradizionali misure limitative della libertà personale sono identificabili in atti ablativi e non "additivi" ovvero "operativi": nessun provvedimento giurisdizionale – nemmeno in rapporto ad un reato o circostanza di eccezionale gravità – può autorizzare il compimento di atti con capacità manipolative dello *status quo* riferibile ad un individuo o ad una situazione di fatto ad egli riconducibile, in grado di avere ripercussioni sulla realtà esterna.

Invero, estendendo la panoramica a contesti istituzionali "satellitari" a quello strettamente processual-penalistico (dal quale viene mutuata la presente proposta di contaminazione del *mainstream* militare), va evidenziata la *vacatio legis* relativa alla regolamentazione delle tecniche di sorveglianza di massa[63] che, come noto, sono appannaggio del comparto *intelligence*, il quale – tra i settori della Struttura protettiva dell'ordine costituito – è quello più affine al sistema Difesa.

Ebbene tale assenza regolamentare, agli occhi del giurista, pone le fondamenta per un quesito che ha i tratti di un'aporia.

Ci si chiede, infatti, se l'assenza di un espresso intervento legislativo sia il frutto di una precisa scelta di politica criminale del legislatore, il quale intenzionalmente lascia avvolta dal mistero un'attività vitale per la stabilità della Repubblica, oppure sia espressione dell'ovvia impossibilità di ammettere una così vistosa intrusione degli apparati dello Stato nella sfera privata individuale.

È allora il momento di verificare se, limitatamente all'impiego delle capacità gestionali-operative dei *tools* oggetto di proposta, anche il sistema Difesa possa essere destinatario del medesimo trattamento che il legislatore riserva al comparto *intelligence* attraverso il silenzio normativo.

Orbene, va in primo luogo precisato che, sul piano "teleologico", lo scopo difensivo caratterizzante l'esercizio dell'attività militare cui sono riconducibili le applicazioni operative oggetto di proposta non ha un rilievo costituzionale deteriore rispetto all'interesse che le predette attività di *intelligence* mirano a garantire; anzi, potrebbe evidenziarsi come il concetto di Difesa abbia un "rango" più elevato e sia inclusivo dell'integrità dell'ordine pubblico e della stabilità interna (la cui tutela è affidata anche ai Servizi di Informazione e Sicurezza).

Ma la questione maggiormente problematica si pone però sul piano sostanziale.

Di fatto – a differenza dell'attività "silente" di mera sorveglianza – l'attività gestionale-operativa può essere caratterizzata da un'alterazione della realtà preesistente che è invece in grado di manifestarsi nel mondo fisico, lasciando traccia delle violazioni in questione.

Tale peculiarità potrebbe mettere in discussione la "reputazione" del sistema e, d'altra parte, non pare conciliarsi con il silenzio legislativo e normativo.

Pertanto è auspicabile che, a differenza di quanto accade per l'attività di sorveglianza, la proposta di condurre attività operative intrusive sia circondata da una procedura che, seppur sganciata dalle lungaggini e dagli ostacoli riferibili alle ordinarie forme di adempimento della riserva di legge e di giurisdizione, dia sicurezza giuridica e legittimità ordinamentale allo Strumento e, più in generale, all'attività militare.

---

[63] La distinzione tra sorveglianza mirata e massiva viene ricavata dal *dictum* del Comitato di sorveglianza dei Servizi di Intelligence e Sicurezza (CTIVD), Relazione annuale 2013–2014, L'Aia, 31 marzo 2014, 45 s., per cui «si definisce sorveglianza di massa la raccolta da parte delle autorità di un'enorme quantità di informazioni su ciò che un gran numero di persone fa con il proprio telefono, computer o altri dispositivi "intelligenti" *online*. [...] Questo è ciò che si intende per "sorveglianza" mirata, perché è rivolta ad una persona specifica che è sospettata di reati particolari. Questo tipo di interferenza con la *privacy* è compatibile con la normativa sui diritti umani solo se esistono garanzie a tutela dell'utilizzo di questi poteri di controllo da parte delle autorità e solo se viene esercitata nei confronti di reali autori di reato o terroristi. Si tratta infatti di un modo estremamente efficace per raccogliere prove, anche se per monitorare continuamente un sospettato sono necessari molto personale e molto denaro. A differenza della sorveglianza mirata, la sorveglianza di massa non è incentrata su singoli individui. [...] La sorveglianza di massa è talvolta definita come una sorveglianza "non targettizzata" o "in Rete". Si riferisce ad una situazione in cui centinaia di migliaia o milioni di informazioni vengono raccolte ogni giorno in un determinato paese su centinaia di migliaia o milioni di persone».

Il diritto alla riservatezza e alla *privacy* nel quadro dei diritti fondamentali

Tra le criticità "accessorie" all'impiego operativo delle tecnologie d'indagine va annoverata la potenziale violazione del diritto alla riservatezza e alla *privacy*.

In effetti, rispetto ad altri precetti, tali diritti risultano più o meno direttamente coinvolti allorquando si procede alla raccolta di informazioni strategiche per il tramite di strumenti tecnologici in situazioni "ordinarie", ossia quando si versi in condizioni che sono da considerarsi al di sotto della soglia di conflitto.

Partendo da una simile consapevolezza, si ritiene utile individuare la sfera operativa dei diritti *de quibus,* troppo spesso impropriamente confusi e definiti come prerogative non "fondamentali", ossia precetti non rientranti nel c.d. "nocciolo duro" dei diritti inviolabili (artt. 13, 14 e 15 Cost.) che possono essere compressi solo a condizione che sia rispettata la doppia riserva, di legge e di giurisdizione.

Il diritto alla riservatezza può essere inteso sia come «rispetto all'intimità della vita privata»[64], ossia «all'inaccessibilità della sfera intima dell'individuo comprensiva delle sue proiezioni spaziali e comunicative»[65] (c.d. riservatezza in senso stretto), sia quale «potere di controllare e gestire ogni informazione personale»[66] (c.d. *privacy*).

Da ciò si desume che, se da un lato il termine "riservatezza in senso stretto" contempla tutte le situazioni che prospettano un'ingerenza di tutela dell'intimità personale, dall'altro il termine "*privacy*" individua circostanze più complesse che finiscono per simboleggiare l'insieme delle libertà che sono implicate nel trattamento dei dati personali, ossia l'*habeas data*[67].

Pur se legate da un rapporto di genere a specie, può dirsi che tanto la riservatezza quanto la *privacy* si stagliano quali diritti autonomi, tutelati in quanto tali dal sistema giuridico.

Una volta delineato il contenuto dei precetti in esame, sembra doveroso esaminare la peculiare natura giuridica di tali diritti, al fine di poterli annoverare, senza alcuna riserva, nel *genus* delle prerogative fondamentali di ogni individuo.

Il punto di partenza dell'analisi del diritto alla riservatezza non può che essere la consapevolezza della mancata previsione, nell'assetto costituzionale nazionale, della protezione espressa del diritto alla vita privata che, viceversa, trova esplicito riconoscimento nel diritto sovranazionale pattizio nell'art. 8 CEDU e nell'art. 16, paragrafo 1, TFUE[68]: nel silenzio legislativo "interno", la tendenza preminente di garantire margini di protezione specifica della riservatezza attraverso un procedimento di derivazione da quelle disposizioni che hanno ad oggetto valori ad essa direttamente riferibili, poiché ne rappresentano aspetti particolari.

Secondo tale prospettiva, il diritto al rispetto della vita privata troverebbe tutela implicita negli artt. 13, 14 e 15 Cost., posti a presidio del complesso di diritti della personalità; impostazione questa meritevole di adesione perché nel commisurare il *quantum* di tutela all'eterogeneità dei profili di volta in volta in considerazione, coglie la precisazione normativa sottesa alla tecnica redazionale dei costituenti, scongiurando i rischi contrapposti legati, da un lato, a un'eccessiva cristallizzazione dei valori tutelati e, dall'altro, ad una ricostruzione riduttiva del concetto di riservatezza.

A questo punto, di fronte alla dinamica evolutiva di tale nozione, non pare superfluo vagliare se la protezione dati personali, anch'essa del tutto assente nella Carta fondamentale, si attaglia

---

[64] AULETTA T.A., *Riservatezza e tutela della personalità,* Milano 1978, pp. 37 e ss.; RESCIGNO F., *Il diritto all'intimità della vita privata,* in *Scritti in onore di F. Santoro Passarelli,* Napoli 1993, pp. 119-124.

[65] CAPRIOLI F., *Colloqui riservati e prova penale*, Torino 2000, pp. 18-30.

[66] RODOTÀ S., *La* privacy *tra individuo e collettività*, in «Politica del diritto» (1974), pp. 545-551.

[67] RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma–Bari 2014, pp. 44 e ss.

[68] Altrettando ampia e compiuta appare la disciplina del diritto alla riservatezza contenuta nella Carta dei diritti dell'Unione Europea, che garantisce una tutela *ad hoc* sia al diritto al rispetto della vita privata (art. 7) che al diritto alla protezione dei dati personali (art. 8); nonché dagli artt. 12 della Dichiarazione Universale dei diritti umani e 17 del Patto internazionale sui diritti civili e politici.

con il nuovo diritto di rango e valore costituzionale.
Interpretando in senso evolutivo le norme costituzionali, si potrebbe ritenere che il diritto alla *privacy* sia ricompreso tra i diritti inviolabili della persona e, quindi, tutelato dall'art. 2 della Costituzione: in questa prospettiva, l'art. 2 Cost. non è più una formula riassuntiva dei diversi diritti della persona costituzionalmente riconosciuti, «ma una clausola generale attraverso la quale operare il continuo adeguamento delle garanzie giuridiche con le esigenze di tutela della persona»[69].
Una volta riconosciuta la dignità costituzionale ai diritti in esame, occorre comprendere se e in che misura tali precetti possano subire una compressione legittima in uno Stato di diritto.
In questo senso, la soluzione può essere rintracciata nella previsione di cui al paragrafo 2 dell'art. 8 CEDU, il quale precisa che il diritto alla riservatezza e alla *privacy* possono subire una restrizione da parte della pubblica autorità, purché l'intervento si sostanzi in «misure necessarie in una società democratica» per perseguire interessi collettivi (quali la sicurezza nazionale, l'ordine pubblico, il benessere economico, prevenzione dei reati) o individuali (protezione di diritti libertà altrui)[70].
Segue il ragionamento: se l'ordinamento sovranazionale – e, di riflesso, quello interno, posta la clausola di "adattamento automatico" di cui all'art. 117 Cost.[71] – consente una compressione delle prerogative in esame in nome della protezione di altri interessi di rango superiore, deve considerarsi ammissibile l'uso di strumenti investigativi da parte della Difesa per garantire la tutela dell'integrità della Repubblica anche in condizioni "ordinarie", posto che tali attività rientrano *tout court* nel concetto di "necessarietà" per il perseguimento di interessi collettivi che, certamente, devono essere considerati preminenti e prevalenti.

Difesa *vs* libertà: alla ricerca di un difficile bilanciamento tra interessi (solo formalmente) contrapposti

Una volta analizzati i principi fondamentali che possono entrare in conflitto con la presente proposta, occorre approfondire il rapporto che lega le esigenze della Difesa e la tutela dei diritti fondamentali individuali[72].
Come più volte chiarito, il ricorso agli strumenti investigativi prestati allo Strumento militare è funzionale a tutelare il più generale bisogno di difesa collettiva, quale bene costituzionale «imprescindibilmente legato alla vita, all'incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona»[73].
Rebus sic stantibus, sembrerebbe che l'enigma posto dalla contrapposizione difesa *vs* libertà possa trovare soluzione attraverso il riconoscimento del valore che deve essere considerato "primario", potendosi in tal modo legittimare la soccombenza del più debole rispetto al più forte.
In questo gioco di forze, c'è chi ritiene che l'esigenza di sicurezza che è alla base dell'attività

---

[69] NIGER S., *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali,* Padova 2006, p. 43.
[70] Corte EDU, Grande Camera, 26 marzo 1987, *Leander c. Svezia*, cit. Nello stesso senso, Corte EDU, sez. III, 17 luglio 2003, *Perry c. Regno Unito*, cit. Da ultimo, Corte EDU, sez. IV, 18 settembre 2014, *Brunet c. Francia*, n. 21010/10, §§ 31–45.
[71] L'adesione dell'Italia ai Trattati convenzionali e internazionali determina l'automatico ingresso della disciplina *ivi* contenuta nell'ordinamento nazionale attraverso la c.d. clausola di adeguamento di cui all'art. 117 Cost. Con specifico riferimento alla CEDU, assai interessante è la questione legata all'efficacia della stessa nell'ordinamento interno. Nelle c.d. "sentenze gemelle" del 2007 si è affermato che il novellato art. 117 Cost. posiziona le norme CEDU ad un livello gerarchico interposto tra la legge ordinaria e la Costituzione. Si è escluso, per converso, che le disposizioni della stessa Convenzione possano avere diretta applicazione nell'ordinamento interno in forza dell'art. 117 Cost. e che il giudice nazionale possa disapplicare la normativa interna contrastante con essa senza sollevare questione di legittimità costituzionale. Cfr. Corte cost., 22 ottobre 2007, n. 348, in *Giur. it.,* 2008, pp. 573 ss.; Corte cost., 22 ottobre 2007, n. 349, *ivi*, pp. 205 ss.
[72] WHITMAN J.Q., *The Two Western Cultures of Privacy: Dignity Versus Liberty,* in «Yale Law Journal» (2004), pp. 1151-1157.
[73] CERRINA FERONI G. E MORBIDELLI G., *La sicurezza: un valore superprimario,* in «Percorsi costituzionali» (2018) 1, pp. 10-26.

di Difesa dell'ordinamento rappresenti il bene giuridico fondamentale, la cui protezione legittima un netto restringimento o il completo annullamento delle garanzie dei soggetti coinvolti e chi, per converso, ritiene imprescindibile considerare la sussistenza di un nucleo di diritti inviolabili che, indipendentemente dal contesto, non possono subire compressioni[74].

A ben guardare, nessuna delle due prerogative sembra potersi atteggiare come preminente sull'altra: libertà e sicurezza (*rectius:* difesa) non rappresentano valori contrastanti, ma due facce della stessa medaglia, parimenti meritevoli di tutela per l'ordinamento costituito[75].

Non sembrando quindi possibile operare in ragione di un'espressa gerarchia giuridica, il "moderno" giurista si trova a dover operare un complesso bilanciamento tra le due forze centrifughe; bilanciamento che «è sempre ricompreso tra diritti fondamentali. Anche quando vengono chiamati in causa interessi fondamentali della collettività (integrità dello Stato, sicurezza, salute, ecc.) è necessario, sia per il legislatore che per gli interpreti, scomporre idealmente l'interesse generale invocato, per vedere se la lesione ipotizzata, che giustifica la limitazione, colpisca uno o più diritti fondamentali compresi nell'area del principio invocato in opposizione».

Allora l'obiettivo del giurista è quello di ricercare il delicato equilibrio tra l'esigenza di assicurare la difesa nazionale da potenziali minacce e la protezione dei diritti individuali inviolabili[76], al fine di evitare l'«eccedenza dell'esigenza di giustizia rispetto alle possibilità di realizzazione umane»[77].

A tal fine, il "faro" che guida le scelte operative deve essere rappresentato dal principio di proporzione – o, meglio, della ragionevolezza – della misura rispetto allo scopo perseguito, nel senso che qualunque restrizione dei diritti fondamentali non può risultare eccedente rispetto alla gravità dei motivi che la giustificano, nel completo rispetto del principio di "stretta necessità", secondo quanto previsto dall'art. 8, paragrafo 2, CEDU).

Il principio *de quo*, lungi dal rimanere confinato al ruolo di mero enunciato normativo astratto, rappresenta assai spesso il più importante momento di verifica in cui si articola il complesso giudizio di legittimità delle disposizioni nazionali limitative delle prerogative individuali.

Lo scrutinio di ragionevolezza, in questi ambiti, impone di verificare che il bilanciamento degli interessi costituzionalmente rilevanti non sia stato realizzato con modalità tali da determinare il sacrificio o la compressione di uno di essi in misura eccessiva, e pertanto incompatibile con il dettato costituzionale.

Ebbene, gli aspetti dottrinali passati in rassegna, unitamente all'analisi delle contingenti vicissitudini storiche, impongono una rivisitazione metodologica dell'attuale sistema di garanzie.

In altri termini, il concetto di difesa assume connotati "meta-giuridici", nel senso che lo scopo cui è volta l'attività militare è quello di assicurare in via prodromica la stabilità di un assetto costituito, di cui l'essenza giuridica rappresenta una delle dimensioni paradigmatiche dello stesso. Il bilanciamento di cui si discorre deve pertanto tener conto della multidimensionalità cui è diretta l'attività militare e va, quindi, collocato in una fase postuma governata dall' *id quod plerumque accidit,* che è espressione del principio di ragionevolezza logica, sciolto da sovrastrutture ideologiche.

In buona sostanza, l'abuso giuridico dell'attività militare, a prescindere dalle condizioni in cui

---

[74] ORLANDI R., op. cit., p. 17.

[75] MINNITI M., *Sicurezza è libertà*, Milano 2018, p. 33.

[76] La necessità della misura, nell'ambito di una società democratica, che garantisca la tutela dei diritti dei singoli e della collettività, «impone il giusto bilanciamento tra le esigenze di tutela degli interessi generali e la protezione dei diritti individuali». Così Corte EDU, Grande camera, 7 luglio 1989, *Soering c. Regno Unito,* n. 14038/88, in *Riv. it. dir. proc. pen.,* 1990, pp. 334 ss.

[77] CARTABIA M., *Edipo re*, in CARTABIA M. E VIOLANTE L. (a cura di), *Giustizia e mito*, Roma–Bari 2018, p. 50.

essa è esercitata, va valutato secondo un giudizio che – seppur seguendo il metodo prognostico – sia condotto *ex post*, non potendo essere tollerato che garanzie di carattere individuale, nonché limiti ordinamentali congegnati per il regolare esercizio delle funzioni statuali tra consociati e istituzioni, possano tradursi in ostacoli all'autoconservazione della stabilità democratica affidata alla Difesa.
Va inoltre specificato che la proposta di un controllo postumo della legittimità delle operazioni militari impingenti situazioni giuridiche soggettive individuali è pienamente coerente con il concetto stesso di "garanzia", che nell'immaginario collettivo si identifica con un meccanismo finalizzato a rendere indenne chiunque abbia subito una lesione illegittima.

L'esigenza di un riassetto organizzativo e normativo del sistema Difesa che favorisca l'impiego militare dei *tools* tecnologici in chiave informativa, strategica e operativa, sin dalla fase del c.d. "sotto-soglia"

All'esito della ricerca condotta emerge, da un lato, l'esistenza di un rinnovato contesto geo-politico caratterizzato da minacce "liquide", la cui proliferazione richiede nuove forme di intervento per la Difesa al fine di acquisire la superiorità informativa, cognitiva e decisionale; dall'altro, la sussistenza di un'architettura istituzionale vetusta, in cui la contrapposizione tra funzioni autorizzative e garanzie impedisce una piena esplicazione militare del potenziale tecnologico e, di fatto, ostacola il percorso evolutivo della Difesa nel complesso contesto competitivo con potenziali forze ostili.
Ebbene, tale "istantanea" dell'attuale panorama complessivo pone in evidenza la necessità di rielaborare una serie di concetti che sono alla base di meccanismi normativi capaci di imbrigliare l'efficace svolgimento dell'attività di difesa della Repubblica.
Di fronte alla fluidità soggettiva ed oggettiva delle nuove minacce, delle fonti da cui esse provengono e in particolare delle finalità che ne sono alla base, un'impostazione metodologica dell'attività di Difesa caratterizzata dal rispetto di schemi, procedure e veti "verticali" ed "orizzontali", oltre che essere priva di efficacia, appare altresì svuotata di significato e corre il rischio di esautorare lo Strumento Militare.
Pertanto, si propone in primo luogo di esaminare con un approccio che sia anch'esso "fluido" i classici concetti di difesa, attività militare e garanzie, al fine di mettere in piedi un sistema multilivello che garantisca alla Difesa di emanciparsi dalle sovrastrutture esistenti ed esercitare le proprie attribuzioni secondo un *mainstream* rinnovato dalla contaminazione con le esperienze di altri settori del modello DIME.
Partendo dalla Difesa, coerentemente con quanto finora esposto, il mutato paradigma degli interessi strategici oggetto di protezione e sensibili all'attacco destabilizzante di forze ostili determina non uno spostamento del baricentro difensivo, ma una sua moltiplicazione.
In buona sostanza, a fronte della lotta alle ancora esistenti minacce convenzionali, la stabilità e la sicurezza cui è deputata la funzione "difesa" hanno ad oggetto frontiere elastiche ed eclettiche, la cui protezione prescinde dall'esistenza di una situazione di conflitto manifesta.
Di conseguenza, la moltiplicazione quantitativa e qualitativa degli obiettivi da proteggere impone la rielaborazione del concetto di "attività militare", che assume una dimensione estensiva comprendendo, oltre al complesso di attività riconducibili alla difesa bellica dello Stato, anche attività funzionali alla protezione delle nuove frontiere statali ora descritte.
Pertanto, su un piano esclusivamente dottrinale, la qualificazione di un'attività come "militare" non dovrà tener conto della natura oggettiva degli atti che la caratterizzano, prediligendo un'impostazione centrata sull'elemento soggettivo-teleologico: sarà qualificata come "militare" ogni attività condotta dal comparto Difesa a prescindere dalla natura dei procedimenti, degli strumenti, degli atti materiali e del personale di cui ci si avvale, in quanto l'elemento qualificante l'attività, sul piano ontologico, è lo scopo difensivo cui essa è diretta e la circostanza che sia esercitata dal sistema Difesa.
Passando ora alla natura e al ruolo delle garanzie che, come ampiamente visto, ad oggi

rappresentano il principale aspetto critico rispetto alla piena esecuzione del potenziale tecnologico degli strumenti digitali d'indagine, una considerazione preliminare va fatta sul concetto di ordinarietà.
Come noto, e come la recente esperienza pandemica ha avuto modo di *reminescere*, le situazioni giuridiche soggettive individuali, di rango costituzionale, non sono in assoluto incomprimibili; esse, infatti, in presenza di contingenze straordinarie possono essere sacrificate, purché da tale sacrifico derivi il superamento di uno stato di pericolo e il ripristino dell'ordinarietà. Ebbene, il compito della Difesa, come dimostrato dall'affidamento della gestione della crisi sanitaria al comparto militare (Gen. Figliuolo), è proprio di contribuire ad assicurare un permanente stato di ordinarietà dell'ordinamento.
Appare ora evidente che, in un contesto in cui il pericolo di un attacco a obiettivi sensibili in grado di assicurare condizioni di ordinarietà sia caratterizzato dall'assenza di preventive manifestazioni indicative di una situazione "conflittuale", discorrere di ordinarietà e straordinarietà al fine di giustificare un'operazione militare "invasiva" della sfera soggettiva individuale, sia privo di validità.
In altri termini, il nuovo modo di aggredire gli interessi sensibili di una Nazione impone un innalzamento del grado di protezione e un'estensione dell'intervento difensivo, che non può essere ancorato alla manifestazione di uno stato di conflitto in ragione dell'indeterminabilità del pericolo.
Dalla rielaborazione concettuale pertinente le componenti strutturali e ambientali del sistema Difesa, consegue una proposta di ristrutturazione dell'attuale impalcatura culturale-ordinamentale posta alla base dell'attribuzione di funzioni e della regolamentazione dei diversi dicasteri, in modo da garantire alla Repubblica Italiana di essere dotata di un comparto militare emancipato e competitivo, fornito di uno Strumento militare pienamente operativo in ogni settore del modello DIME.

Le proposte possono essere così schematizzate:

a) Riassetto organizzativo

Come si è avuto modo di anticipare, il sistema Difesa è parte di un apparato istituzionale caratterizzato dalla rigida separazione di competenze tra i vari dicasteri (Diplomatico, Informativo, Militare ed Economico) che contribuiscono, nelle aree funzionali di competenza, all'attuazione della Strategia Nazionale di Sicurezza.
Tuttavia il mutamento della "funzione difesa" sta determinando l'impossibilità di distinguere in modo altrettanto netto la sicurezza interna ed esterna, e di conseguenza i confini tra politica estera, di difesa e di sicurezza sono destinati a scomparire.
In tale contesto, anche in considerazione delle linee contenute nel *Documento programmatico pluriennale della Difesa per il triennio 2022-2024* (Ed. 2022), appare indispensabile un riassetto organizzativo che si ponga come obiettivo finale l'adeguamento dell'architettura istituzionale in materia di sicurezza nazionale al mutato scenario di riferimento, e che parta dell'innovazione delle procedure di coordinamento, al fine di assicurare coerenza ed efficienza all'azione governativa, agilità decisionale, flessibilità e capacità di adattamento ai mutamenti, anche repentini, nell'ambito di scenari di sicurezza caratterizzati da un elevatissimo livello di volatilità.
Nello specifico, il cuore della presente ricerca ha posto l'accento su due punti nevralgici oggetto di intervento per un miglioramento competitivo del sistema Difesa: l'emancipazione del comparto militare da altre componenti del sistema Securitario Nazionale e il potenziamento del ruolo della Difesa nell'ambito della gestione informativa.
Entrambe le esigenze possono essere soddisfatte attraverso l'istituzione di uno specifico organo interforze che presenti le seguenti caratteristiche:
- Funzioni e competenze: efficientamento della capacità informativa del sistema Difesa per il

miglioramento competitivo della capacità cognitiva e decisionale (c.d. *core business*); acquisizione, raccolta, condivisione, elaborazione e gestione di dati e informazioni di interesse militare;
- Poteri: determinazione della dimensione strategico-militare, classificazione e secretazione contenutistica del flusso informativo-cognitivo acquisito, raccolto, condiviso ed elaborato in cooperazione con i comparti istituzionali pubblici e privati deputati alla funzione informativa;
- Composizione: partecipazione paritetica (in termini numerici) di esponenti del comparto militare, informativo e diplomatico, ciascuno deputato in ragione del dicastero di appartenenza all'autonomo esercizio di funzioni di classificazione contenutistica del flusso informativo-cognitivo;
- Natura: organo interforze e inter-dicasteriale (Ministeri della Difesa, degli Esteri e dell'Interno);
- Controllo esterno: l'attività svolta da tale organo sarà comunicata attraverso rapporti periodici ad una Commissione bicamerale costituita *ad hoc* e deputata ad effettuare un controllo di legittimità.

b) Riassetto normativo

Sotto il profilo normativo, partendo dalle precedenti considerazioni sulla inattualità della bipartizione "ordinarietà/straordinarietà" – intesa quale presupposto abilitante la piena capacità operativa dello Strumento militare –, si rende evidente l'adozione di una nuova impostazione metodologica basata sulla disattivazione della preventiva operabilità delle autorizzazioni giudiziarie.
Il tempo è maturo per comprendere che il "sotto-soglia" non rappresenta più una metrica utile a parametrare l'esistenza di un conflitto.
In effetti, come si è avuto modo di anticipare, nel rinnovato contesto bellico la "guerra" si combatte anche con metodi diversi da quelli convenzionali; gli attacchi non sono più solo fisici, potendo essere esperiti anche con armi invisibili che di certo non sono meno insidiose di quelle tradizionali.
Come precisato, «[L]e prossime guerre tra gli Stati non saranno certamente condotte soltanto con i tradizionali strumenti di offesa e di difesa via terra, mare e aria, ma saranno accompagnate e probabilmente iniziate – e in qualche caso vinte – con attacchi perpetrati attraverso lo spazio cibernetico. Questi sono infatti suscettibili di infliggere al nemico danni gravissimi, con effetti sulla società che gli esperti considerano paragonabili a quelli di armi convenzionali»[78].
A ben guardare, il recente conflitto in Ucraina rappresenta l'esempio lampante della vetustà del concetto del "sotto-soglia": seppur non soggetta ad alcun attacco armato convenzionale, l'Italia sta subendo forti pressioni (*rectius:* minacce) indirette che inevitabilmente attentano alla stabilità del Paese, ripercuotendosi sugli assetti diplomatici (si pensi alle minacce nucleari alla NATO), informativi (con campagne di *fake news* capaci di minare la sovranità nazionale) ed economici (si pensi alle ripercussioni sui mercati dell'energia e dei prodotti alimentari).
In questa circostanza, sembra inverosimile – oltre che assai pericoloso per la stabilità nazionale – non consentire l'estrinsecazione del potenziale militare perché nel "sotto-soglia": detto in altre parole, in ipotesi come quelle richiamate, aspettare che si realizzino le condizioni del "sopra-soglia" per consentire l'intervento della Difesa costituirebbe un colpevole ritardo e quasi certamente un'ipoteca sul fallimento.
Alla luce di tali considerazioni, si richiede di abbandonare il concetto di "sotto-soglia" e di rielaborare in chiave moderna il principio di proporzionalità: l'irrinunciabile esigenza dello strumento militare di proteggere obiettivi "civili" postula l'esercizio di un'attività militare al di fuori del contesto bellico, attraverso operazioni dai tratti ontologici che si discostano

[78] *Dossier* della Camera dei Deputati sulla *Sicurezza e Difesa nello spazio cibernetico,* del 21 dicembre 2017, p. 1.

dall'intervento militare convenzionale (e, dunque, il superamento della causa di giustificazione dello stato di necessità).
Inoltre, appare necessario estendere al personale della Difesa quel complesso di garanzie funzionali – le quali, come noto, sono concesse esclusivamente agli appartenenti di DIS, AISE e AISI – esonerandoli da responsabilità penale allorquando, nello svolgimento dei compiti istituzionali e in presenza di specifiche condizioni, si trovino a compiere azioni configurabili come reato – che, allo stato, risultano irrinunciabili per condurre attività preventive tanto a fini di Sicurezza quanto per scopi di Difesa.
Non certo si discorre di annullare le garanzie costituzionalmente e convenzionalmente poste a protezione dei diritti inviolabili, ma di posticipare il sindacato giurisdizionale in fase successiva se l'attività posta in essere sia qualificabile come militare secondo i criteri ermeneutici sopra menzionati.
Alla luce di quanto detto, appare doveroso un intervento legislativo volto – sul piano sostanziale – a ridefinire il concetto giuridico di "attività militare" al fine di tipizzare – sul piano procedurale – un *iter* procedimentale "speciale", riservato al solo comparto Difesa, in cui le ordinarie cautele giurisdizionali siano collocate in una fase posteriore all'attività oggetto di controllo, così da garantire che le stesse non ostacolino la prontezza operativa di intervento e, al contempo, assicurino un impiego legittimo dello Strumento militare.
Al fine di garantire coerenza ordinamentale alla proposta, in particolare nel processo di tipizzazione giuridica e individuazione dei soggetti investiti del potere di sindacato giurisdizionale dell'attività svolta, è auspicabile la predisposizione di un Tavolo Tecnico che preveda il coinvolgimento di esponenti dei Dicasteri coinvolti, della Magistratura e della Ricerca.

c) Impiego militare dei *tools* tecnologici

Una volta creato l'*habitat* organizzativo e normativo ideale, appare possibile per lo Strumento militare sfruttare il pieno potenziale tecnologico insito nei *tools* di matrice investigativa.
Più in particolare, una volta attribuito alla Difesa il potere di gestire le informazioni strategiche ed esteso il concetto di "attività militare" anche sotto la tradizionale soglia di "conflitto armato", è possibile legittimare il comparto Difesa ad avvalersi delle capacità multidirezionali (captativo-conservativa, gestionale e operativa) insite negli strumenti tecnologici, così da adeguare lo *standard* difensivo al mutamento degli interessi e degli obiettivi degni di protezione in quanto espressione di un allargato concetto di stabilità della Repubblica.
Si precisa che, al fine di garantire l'immediata applicazione operativa dei *tools*, è auspicabile per il sistema Difesa una fase iniziale di collaborazione interforze tra il comparto militare e altri corpi che – in ragione delle funzioni di polizia giudiziaria dai medesimi assolte – hanno acquisito esperienza pratica e dimestichezza nell'impiego delle tecnologie, in modo da porre in essere un completo processo di contaminazione del *mainstream* militare con *skills* caratteristiche dell'impostazione investigativa, per soddisfare la necessità di un approccio olistico e integrato dello Strumento militare.

DARIO CITATI

Analista politico, traduttore e interprete con formazione universitaria in Storia contemporanea e Lingue slave, incarichi di docenza e pubblicazioni scientifiche in ambito geopolitica, difesa e sicurezza.

L'INTESA FLESSIBILE. GEOPOLITICA E STRATEGIA MILITARE NELLE RELAZIONI TRA RUSSIA E CINA

ABSTRACT

L'articolo propone la seguente interpretazione delle relazioni Russia-Cina. Il primo paragrafo individua l'origine dei buoni rapporti attuali nella soluzione a una storica disputa sui confini. Nel secondo, si analizzano le esercitazioni militari congiunte dal 2004 al 2024, che mostrano una cooperazione in costante crescita tra le rispettive Forze Armate. Nel terzo, si esaminano alcune condotte di politica estera da cui emergono invece divergenze e mutamenti nei rapporti di forza: a seguito del conflitto in Ucraina, gli Stati ex sovietici dell'Asia centrale si sono avvicinati alla Cina a detrimento della Russia. In conclusione, il rapporto tra Mosca e Pechino viene definito una 'intesa flessibile' sulla cui evoluzione influiranno le politiche dell'Occidente, che potrebbe compattare i due Paesi trattandoli come un fronte unitario, oppure dividerli sfruttandone le rivalità a proprio beneficio.

Le basi del rapporto russo-cinese nel XXI secolo: l'accordo sui confini e l'Organizzazione per la Cooperazione di Shanghai

Nella plurisecolare e complessa storia delle relazioni russo-cinesi, uno snodo fondamentale d'epoca recente può essere senza dubbio considerato il trattato «Accordo Complementare sulla sezione orientale del confine tra Cina e Russia», firmato a Pechino il 14 ottobre 2004 e ratificato in Russia nel maggio 2005 con Legge Federale n. 52-FZ dalla Duma di Stato e dal Consiglio della Federazione Russa[79]. Dopo diversi anni di negoziati, con tale accordo – detto 'complementare' perché completava in modo definitivo l'atto omonimo stipulato nel 1991 – la Russia ha ceduto alla Cina l'isola Tabarov (toponimo cinese Yínlóngdǎo), la metà dell'isola Bol'šoj Ussuriskij (toponimo cinese Hēixiāzi Dǎo) e metà dell'isola Bol'šoj (toponimo cinese Ābāgāitú), mettendo fine a un'antica disputa tra due Paesi che condividono un confine di quasi 4300 km. Questi territori erano infatti stati occupati dall'URSS durante la guerra sino-sovietica del 1929, per divenire poi il teatro della crisi sino-sovietica del 1969, allorquando nelle aree di confine scoppiarono scontri armati che per poco non sfociarono in un aperto conflitto. Nei decenni successivi, questa controversia territoriale sarebbe rimasta il principale punto di attrito tra Mosca e Pechino[80].

La ratifica dell'Accordo complementare che vi ha posto fine nel 2004 è stata preceduta da un patto di non-aggressione siglato nel 2001[81]. Nello stesso anno i due Paesi hanno dato vita all'Organizzazione per la Cooperazione di Shanghai – nota con l'acronimo inglese SCO – con le repubbliche ex sovietiche di Kazakhstan, Kirghizistan, Uzbekistan e Tagikistan. Fondata con il proposito di sradicare i cosiddetti 'tre mali' (terrorismo, estremismo, separatismo) dell'Asia centrale e delle zone di frontiera russo-cinesi, essa ha costituito una piattaforma multilaterale per rafforzare i legami fra tutti gli Stati membri, consentendo a Mosca e Pechino di trovare un equilibrio tra la cooperazione in materia di sicurezza e la competizione in ambito

[79] L'atto di ratifica in lingua originale è consultabile su vari siti ufficiali istituzionali della Federazione Russa, tra cui quello del Ministero degli Interni: https://mvd.consultant.ru/documents/51299

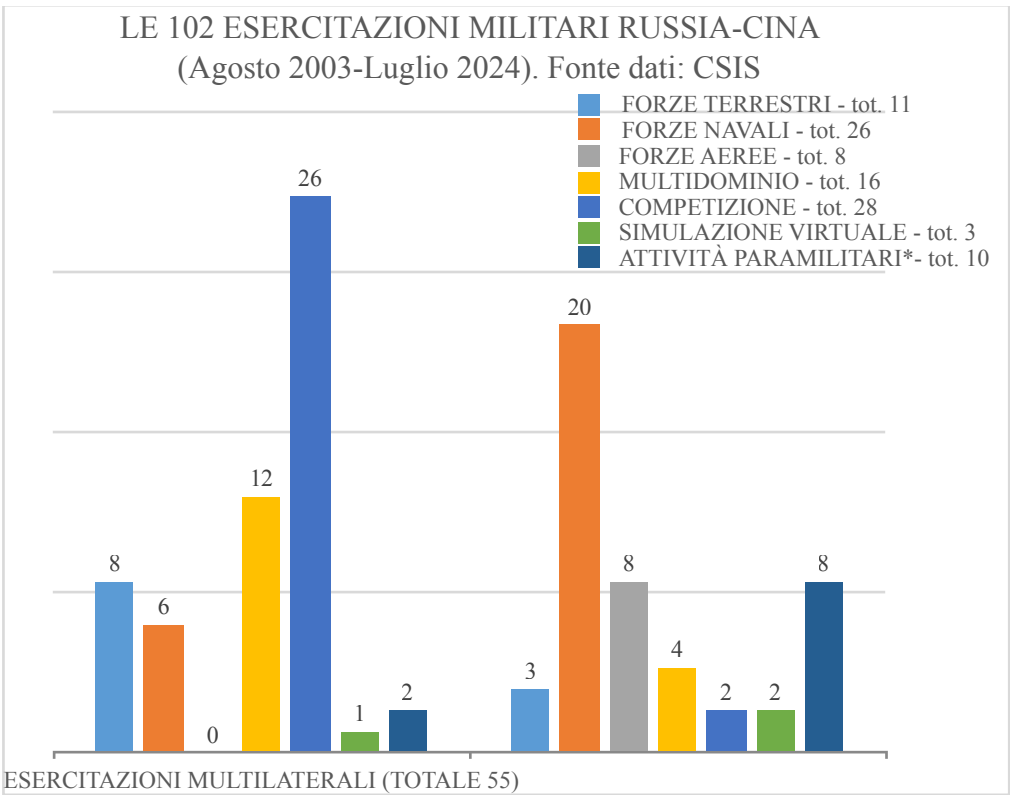
[80] Cfr. DMOCHOWSKI T., *The Settlement of the Russian–Chinese Border Dispute*, in «Polish Political Science Yearbook» 44 (2015), pp. 56-74.

[81] Si veda il testo in traduzione ufficiale inglese, *Treaty of Good-Neighbourliness and Friendly Cooperation Between the PRC and the Russian Federation*, Ministry of Foreign Affairs of the People's Republic of China, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/200107/t20010724_679026.html

economico in tutta la regione centroasiatica[82]. La risoluzione della disputa sui confini e la creazione della SCO hanno dunque sancito l'inizio di una fase nuova nelle relazioni bilaterali russo-cinesi, caratterizzata da numerose forme di collaborazione di cui l'ambito militare costituisce uno degli esempi più significativi.

Le esercitazioni congiunte russo-cinesi: dati, informazioni, interpretazione

Nel ventennio 2004-2024 le esercitazioni armate congiunte tra Russia e Cina sono cresciute in maniera costante, con una particolare intensificazione nell'ultimo decennio. Il *think tank* statunitense *Center for Strategic & International Studies* (CSIS) ne ha contate in totale 102, pubblicandole in un *database* che le elenca in ordine cronologico dall'agosto 2003 al luglio 2024 specificando data, luogo, principali attività ed eventuali altri Paesi coinvolti in base alle informazioni reperibili da fonti aperte[83]. Dal punto di vista temporale, metà di queste esercitazioni (51) si sono svolte nei quindici anni compresi tra il 2003 e il 2017, l'altra metà nei sette anni compresi tra il 2017 e il 2024, dunque con un incremento statistico annuale di quasi il 50%. Al fine di valorizzare i dati raccolti dal CSIS e trarvi elementi informativi che consentano un *assessment* critico-analitico, li ho disaggregati e poi rielaborati in base a tre criteri: la tipologia di dominio o di Forze armate coinvolte (terrestri, navali, aeree o multi-dominio); la presenza eventuale di altri Paesi nelle esercitazioni (bilaterali se Russia-Cina, multilaterali se con altre nazioni); il rapporto tra il singolo dominio e la dimensione bilaterale/multilaterale. I risultati dell'elaborazione sono consultabili nel grafico seguente:



*Per attività paramilitari si intendono esercitazioni riguardanti attività di pubblica sicurezza e di polizia quali controlli anti-crimine, anti-droga, investigazione, pedinamenti, etc.

[82] Un'analisi aggiornata dell'evoluzione della SCO, con particolare focus sulla Russia, è ŠĆEPANOVIĆ J., *Russia and the Shanghai Cooperation Organization: a Question of the Commitment Capacity,* in «European Politics and Society» 23 (2022), Issue 5, pp. 712-734. Per una disamina dal punto di vista della Cina, si vedano invece SONG W., *Interests, Power and China's Difficult Game in the Shanghai Cooperation Organization (SCO)*, in «Journal of Contemporary China» 23 (2014), Issue 85, pp. 85-101; e il più recente CHAO W., *The Political Economy of China's Rising Role in the Shanghai Cooperation Organization (SCO): Leading with Balance*, in «The Chinese Economy» 55 (2022), Issue 4, pp. 293-302.

[83] Il *database* realizzato dal CSIS in formato excel è consultabile al link: https://chinapower.csis.org/data/china-russia-joint-military-exercises/.

Ciò che si inferisce dalla lettura delle voci più importanti del grafico è che le esercitazioni terrestri hanno riguardato spesso anche altri Paesi, mentre nel dominio marittimo e in quello aereo il *format* prevalente è, in modo quasi esclusivo, quello bilaterale. Su 11 esercitazioni che hanno coinvolto le sole Forze di terra, infatti, 8 sono state multilaterali e 3 bilaterali; nel dominio marittimo, invece, delle 26 esercitazioni navali ben 20 sono state bilaterali Russia-Cina e 6 si sono svolte in una cornice multilaterale; in quelle aeree, la totalità delle 8 esercitazioni hanno riguardato le sole aeronautiche di Mosca e di Pechino.
La maggior parte delle 16 esercitazioni multilaterali e multi-dominio si sono svolte con gli altri quattro Paesi membri della SCO. L'attività più importante, che ha la denominazione ufficiale – e non propriamente originale – di 'Missione di Pace' (in russo *Mirnaja Missija*), si è svolta con regolarità su base biennale dal 2009 al 2021 e ha sempre avuto un *focus* sull'addestramento alla contro-insurrezione e all'antiterrorismo, volto essenzialmente a prevenire scenari di instabilità nelle repubbliche ex sovietiche dell'Asia centrale, nel Xinjiang cinese, nel Caucaso e nelle regioni meridionali della Russia[84]. Attività di controguerriglia, controllo della folla, cinturazione e interdizione di aree, procedure tecnico-tattiche (TTP) d'assalto di squadra e liberazione ostaggi, supporto aereo tattico: un tipo di *training* basato soprattutto sull'esperienza passata della guerre 'interne' combattute dalla Russia in Cecenia e che consente a Mosca e Pechino di monitorare il livello di preparazione militare dei Paesi ex sovietici della SCO[85].
Pur essendo classificate dunque come 'multi-dominio', le varie edizioni di *Mirnaja Missija* non hanno riguardato complesse esercitazioni di manovra interforze in uno scenario di guerra su vasta scala, quanto piuttosto attività tattiche terrestri specialistiche con pochi assetti aerei di supporto (e ancor meno navali, avendovi partecipato essenzialmente reparti anfibi e fanteria di marina). In molte di queste attività addestrative – così come anche in alcune grosse esercitazioni bilaterali terrestri quali *Vostok 2018* ('Oriente 2018') e *Zapad 2019* ('Occidente 2019') – la Russia ha condiviso con la Cina l'esperienza del Gruppo Tattico di Battaglione (BTG, dal russo *Batal'ionnaja Taktičeskaja Gruppa*)[86]. Si tratta di un aspetto tecnico su cui vale la pena soffermarsi per i risvolti nella cooperazione militare.
Il BTG ha costituito per anni il *core* delle formazioni tattiche terrestri della Russia, incarnando il principio che la dottrina di Mosca definisce *Obščevojskovoj Boj* e noto in ambito anglosassone come *Combined Arms*. Il BTG è concepito come un'unità di manovra autonoma, di prontezza e appunto pluriarma – più piccola di una brigata ma alimentata da Armi differenti – in base al principio che le carenze di un tipo di Arma vengono compensate dalla presenza simultanea delle altre. Grazie soprattutto alla capacità di saturazione di aree circoscritte con fuoco indiretto, i BTG russi hanno mostrato buoni livelli di efficacia operativa in teatri come la Cecenia, la Georgia, in parte la Siria e il conflitto in Donbass del 2014, suscitando l'interesse di diverse Forze Armate nel mondo tra cui quelle di Pechino. Essi hanno rivelato però numerose lacune in una guerra di attrito su larga scala come il conflitto russo-ucraino: la tendenza a evitare il contatto; la poca efficacia nel combattimento urbano, la difficoltà a manovrare in profondità, l'insufficienza del sostegno logistico rispetto alla tempistica della manovra. Le cause di queste difficoltà incontrate dai BTG russi in Ucraina sembrano essenzialmente due: primo, la scarsità di fanteria meccanizzata e appiedata rispetto alle batterie di artiglieria e alla componente carri (sia in termini di organico sia di addestramento); secondo, un comando eccessivamente centralizzato, opposto alla nozione occidentale del *Mission Command*, particolarmente inadeguato in un teatro ove si richiede forte spirito

---

[84] RUMJANCEVA A. K. - RACHIMOV, R. *Rol' ŠOS v protivodejstvii terrorizmu v stranach Central'noj Azii* [*Il ruolo della SCO nel contrasto al terrorismo nei Paesi dell'Asia centrale*], in «Postsovetskie Issledovanija» 5 (2022), n. 8, pp. 835-846, disponibile online al link https://www.postussr.org/journals/202208/Румянцева%20А.К..pdf

[85] WEITZ, R., *Assessing Chinese-Russian Military Exercises. Past Progress and Future Trends,* Center for Strategic and International Studies (CSIS), July 9, 2021, https://www.csis.org/analysis/assessing-chinese-russian-military-exercises-past-progress-and-future-trends, p. 2.

[86] Il dispiegamento del BTG è ad esempio menzionato nel resoconto dell'edizione 2013 di *Mirnaja Missija* pubblicato dall'agenzia stampa TASS: *Rossija i Kitaj zaveršili planirovanie sovmestnich antiterrorističeskich učenij "Mirnaja Missija" - 2013 [Russia e Cina hanno concluso la pianificazione delle esercitazioni antiterroristiche congiunte 'Missione di Pace' 2013]*, https://tass.ru/politika/532811/amp. Schieramenti di BTG si sono avuti anche nell'esercitazione bilaterale *Vostok 2018*, come riporta KOFMAN, M. *Vostok 2018 Day 7 (September 17)* https://russianmilitaryanalysis.wordpress.com/2018/09/18/vostok-2018-day-7-september-17/.

d'iniziativa sul campo di battaglia[87]. Da quando la Russia ha lanciato la cosiddetta 'operazione militare speciale' in Ucraina, il format di esercitazioni multilaterali *Mirnaja Missija, con Cina e Paesi SCO* risulta sospeso. Dal punto di vista della Cina, ciò potrebbe indicare che il BTG e l'approccio *Combined Arms* applicato a piccole unità di manovra hanno perso l'attrattiva che avevano qualche anno fa. Da parte invece delle nazioni ex sovietiche SCO, l'interruzione si spiega probabilmente con la volontà di limitare la condivisione con la Russia di informazioni su propri mezzi, sistemi d'arma e procedure di impiego, nel timore che Mosca possa nutrire mire annessionistiche nei loro confronti come accaduto proprio con l'Ucraina.

Passando in rassegna le restanti esercitazioni multilaterali, in un paio di occasioni (esercitazione *Centr 2019* e *Kavkaz 2020*), ad esse hanno partecipato India e Pakistan, che dell'Organizzazione per la Cooperazione di Shanghai sono divenuti membri permanenti nel 2017. In ambito navale, come si è detto, Russia e Cina hanno condotto quasi sempre esercitazioni bilaterali, ma qualche volta si è aggiunto un terzo *partner* esterno più o meno inaspettato, quale l'Iran e o il Sudafrica. Al di là della prevalente dimensione bilaterale, la varietà geografica delle esercitazioni navali russo-cinesi indica una peculiarità specifica: quella di una proiettabilità marittima a vocazione globale.

Mentre infatti le esercitazioni terrestri e multi-dominio si sono svolte sempre nei territori di Russia, Cina e Paesi SCO, le Marine dei due Paesi hanno solcato insieme una buona parte dei mari del globo: Mar Mediterraneo (maggio 2014 e maggio 2015), Mar Baltico (2017), Mar del Giappone e Mar Cinese Orientale (undici volte tra il 2017 e il 2023), Mar Cinese Meridionale (2016 e 2024). La più imponente esercitazione navale di Russia e Cina – non inclusa nella lista del CSIS in quanto si è svolta tra il 10 e il 16 settembre 2024 – conferma pienamente tale tendenza: la *Okean 2024*, svolta sotto la diretta supervisione del Capo di Stato Maggiore della Marina della Federazione Russa, si è infatti svolta tra gli Oceani Pacifico e Artico, il Mar Caspio, il Baltico e il Mediterraneo. Si è trattato di un'esercitazione prevalentemente russa con la partecipazione della Marina cinese e una quindicina di Paesi osservatori[88]. Le 8 esercitazioni bilaterali nel dominio aereo, infine, hanno visto quasi sempre il dispiegamento congiunto dei bombardieri strategici russi Tu-95 e di quelli cinesi Xian H-6[89].

Mettendo a sistema i dati grezzi e le informazioni ricavate dalla loro rielaborazione analitica, l'interpretazione complessiva delle esercitazioni russo-cinesi può sintetizzarsi nei seguenti punti:

1. Russia e Cina hanno sviluppato un buon livello di interoperabilità tra le rispettive Forze Armate, soprattutto in eventuali interventi di stabilizzazione nelle aree di confine;
2. È soprattutto la Cina che ha beneficiato della maggiore esperienza in teatri operativi da parte della Russia, specie nel dominio terrestre;
3. La Russia – la cui flotta navale costituisce storicamente la componente meno equipaggiata e addestrata delle proprie Forze Armate – ha però senz'altro migliorato la capacità di proiezione marittima grazie alle esercitazioni con la Marina cinese;
4. Lo schieramento congiunto di assetti dei due Paesi in un eventuale teatro di guerra appare plausibile, allo stato attuale, in operazioni limitate nel tempo e nello spazio e non in conflitti su larga scala;
5. La possibilità che la Russia offra un supporto in eventuali operazioni militari cinesi in Asia è di gran lunga maggiore all'ipotesi che la Cina contribuisca a eventuali future campagne

---

[87] Cfr. TAKÁCS, M., *Short Study: Describing the Major Features of the Russian Battalion Tactical Group*, in «AARMS – Academic and Applied Research in Military and Public Management Science» 20 (2021), n. 2, pp. 49–65. Si vedano anche le eccellenti analisi degli Ufficiali dello US Army quali il Capitano FIORE N., *Defeating the Russian Battalion Tactical Group*, US Army MCOE, Spring 2017, https://www.moore.army.mil/armor/earmor/content/issues/2017/spring/2Fiore17.pdf, e ancor di più del Tenente Colonnello FOX, A.C., *Reflections on Russia's 2022 Invasion of Ukraine Combined Arms Warfare, the Battalion Tactical Group and Wars in a Fishbowl*, Association of the United States Army, Land Warfare Report n. 149, September 2022, https://www.ausa.org/publications/reflections-russias-2022-invasion-ukraine-combined-arms-warfare-battalion-tactical.

[88] Cfr. l'analisi del Capitano US Navy BOTT C., *Okean Returns: A Battered Russian Navy Brings Back a Soviet-Era Exercise*, in «Proceedings», US Naval Institute, 150/10 (October 2024), https://www.usni.org/magazines/proceedings/2024/october/okean-returns-battered-russian-navy-brings-back-soviet-era.

[89] Nell'ultima esercitazione, a luglio 2024, sono stati tracciati a circa 200 miglia dalle coste dell'Alaska: *NORAD Detects, Tracks and Intercepts Russian and PRC Aircraft Operating in the Alaska ADIZ,* 24/07/ 2024, https://www.norad.mil/Newsroom/Press-Releases/Article/3849184/norad-detects-tracks-and-intercepts-russian-and-prc-aircraft-operating-in-the-a/

militari della Russia in Europa o in Medio Oriente[90].
Secondo l'analista Richard Weitz, le esercitazioni russo-cinesi sono divenute «lo strumento fondativo per istituzionalizzare i legami nel campo della Difesa in assenza di un'alleanza militare formale»[91]. Si può partire da questa citazione per allargare il campo d'analisi politico-militare, e gradualmente estenderlo a quello politico-strategico.

L'Asia centrale e gli equilibri a rischio dopo il conflitto in Ucraina

La sospensione delle esercitazioni multilaterali di Russia e Cina con i Paesi SCO a partire dal conflitto in Ucraina, cui si è fatto riferimento in precedenza, aiuta a capire l'impatto della cosiddetta 'operazione militare speciale' nei Paesi ex sovietici dell'Asia centrale. Il vertice SCO di Samarcanda a settembre 2022, che avuto una discreta rilevanza mondiale come test di fiducia verso la Russia fuori dall'Occidente, si è chiuso con esiti contrastanti[92]. Le repubbliche ex sovietiche della SCO sono d'altronde Paesi abbastanza disomogenei per demografia, estensione territoriale, peso politico-economico, nonché per il grado di influenza esercitata da Mosca.

Il Kazakhstan, il più vasto dell'area, è l'unico a confinare direttamente con la Russia, con cui condivide una frontiera di ben 7645 km. Si tratta del Paese con cui Mosca ha complessivamente mantenuto i migliori rapporti, nonché tre installazioni militari: il sito anti-missilistico di Sary Šagan, il Cosmodromo di Baikonur e il Centro Test di Volo 929 'V.P. Čkalov' di Tajsojgan. Il Kazakhstan ospita però anche una significativa minoranza russa e, proprio per i legami economici con Mosca, è da sempre molto danneggiato dalle sanzioni occidentali contro la Russia e dalle contro-sanzioni di quest'ultima[93]. L'Uzbekistan, lo Stato più popoloso fra i quattro (oltre 36 milioni di abitanti), da anni ha rapporti molto più altalenanti con Mosca e la cooperazione militare è circoscritta all'ambito SCO. In Tagikistan e Kirghizistan, Paesi molto fragili e dal controllo territoriale limitato, la Russia mantiene una presenza significativa: nel primo, ha sede la 201ª Base militare russa – dislocata in due guarnigioni, nella capitale Dušanbe e al confine tagiko-afgano – considerata la più grande base di Mosca fuori dalla Russia. Nel secondo, vi sono 4 siti militari russi: la 999ª Base delle Forze aerospaziali (Aviobase di Kant); la 954ª Base di Addestramento armamenti antisommergibile (1609 metri sul livello del mare, nei pressi del golfo di Prževalskij, lago Issyk-Kul'); Il 338° Centro di Comunicazione 'Marevo' nei pressi del fiume Ašmara; il 17° Laboratorio Radio-sismico di Mailuu-Suu.

Nessuno dei quattro Paesi ha sostenuto l'operazione russa in Ucraina e, senza criticarla apertamente, tutti hanno manifestato cautela ed appelli alla riconciliazione. Considerati i rapporti di forza tra le parti, è lecito interpretare questo atteggiamento come una ridotta fiducia verso Mosca e il timore d'una ricostituzione imperiale di quello spazio ex sovietico che la dottrina russa definisce 'Estero Vicino' (in russo *Bližnee Zarubež'e*), una locuzione utilizzata per rivendicarlo come propria legittima sfera d'influenza[94].

Il relativo calo di prestigio della Russia all'interno della SCO è stato in qualche modo bilanciato dal recente ingresso di due Paesi 'amici' di Mosca. Nel 2023 l'Iran è divenuto membro permanente dell'organizzazione; nel 2024 è stato il turno della Bielorussia. Questi ingressi – in particolar modo il secondo – sembrano tuttavia snaturare lo spirito con cui era nata l'Organizzazione per la Cooperazione di Shanghai, meno focalizzata sull'effettiva cooperazione regionale e sempre più usata quale 'camera di compensazione' dalla Russia, che rivendica le proprie iniziative militari e di politica estera anche a fronte delle tacite perplessità degli altri membri.

---

[90] SKYLAR-MASTRO O., *Sino-Russian Military Alignment and Its Implications for Global Security*, in «Security Studies» 33 (2024), n. 2, p. 269.

[91] WEITZ, R., *Assessing Chinese-Russian…*op. cit., p. 3.

[92] GAIANI G., *Il vertice della SCO a Samarcanda tra intese, divergenze e riflessi sull'Europa*, in «Analisi Difesa», 20/09/2022, https://www.analisidifesa.it/2022/09/il-vertice-della-sco-a-samarcanda-tra-intese-divergenze-e-riflessi-sulleuropa/

[93] Un buon inquadramento è LARUELLE M. - PEYROUSE S., *Les Russes du Kazakhstan. Identités nationales et nouveaux États dans l'espace post-soviétiques*, Paris 2004; Per l'impatto del conflitto ucraino, cfr. DUMOULIN M., *Steppe Change: How Russia's War on Ukraine is Reshaping Kazakhstan*, Policy Brief ECFR, 13 April 2023, https://ecfr.eu/publication/steppe-change-how-russias-war-on-ukraine-is-reshaping-kazakhstan/

[94] UBAYDULLAEVA, D., GENAUER J., *Shifting Geopolitics of Central Asia: The Regional Impact of the Russia-Ukraine War,* Australian Institute of International Affairs, 20/11/2024, https://www.internationalaffairs.org.au/australianoutlook/shifting-geopolitics-of-central-asia-the-regional-impact-of-the-russia-ukraine-war/.

In parallelo, si è assistito ad una tendenza di segno opposto: il netto rafforzamento, dapprima economico e ultimamente anche militare, dei rapporti bilaterali della Cina con i Paesi SCO. Dal progetto di 'Nuova Via della Seta' ai dati sull'*import-export*, dal settore dell'energia a quello dei trasporti, dai progetti sull'IA sino alle speculazioni su una nuova base militare cinese in Tagikistan, gli esperti sono concordi nel ritenere che l'influenza della Cina e soprattutto la fiducia che essa gode in questi Paesi sia oggi complessivamente superiore a quella della Russia[95]. Non vi è consenso invece sulle evoluzioni future: secondo taluni, la competizione Russia-Cina nella regione è destinata ad aumentare; secondo altri, la politica di *de-confliction* che ha governato gli ultimi vent'anni resterà invece la cifra caratteristica delle relazioni di buon vicinato tra Mosca e Pechino[96]. Il combinato disposto tra l'indebolimento della Russia e il rafforzamento della Cina in Asia centrale non va interpretato, a parer di chi scrive, come una tendenza ineluttabile, bensì come una condizione che può evolvere in un senso o in un altro in presenza di specifiche variabili.

Russia e Cina sono senz'altro pronte a intervenire militarmente in Asia centrale di fronte a eventuali scenari che minacciassero gli interessi di entrambe: ad esempio, un'ipotetica insurrezione islamista degli Uiguri in Xinjiang, che rischi di espandersi oltre i confini cinesi e destabilizzare anche aree di interesse russo; un *golpe* filo-occidentale in un Paese SCO; scontri armati di frontiera tra Stati deboli come Tagikistan e Kirghizistan. A seguito del conflitto in Ucraina, tuttavia, un nuovo tipo di scenario appare oggi sicuramente possibile, benché non ancora molto probabile. Si tratta dell'eventualità in cui uno dei Paesi SCO assuma iniziative percepite come ostili dal Cremlino – ad esempio, chiusura di basi militari russe, oppure misure ritenute discriminatorie verso la popolazione russa – tali da provocare un intervento di Mosca. La Cina, in ragione dell'accresciuto prestigio acquisito, potrebbe in tal caso opporsi a un'iniziativa unilaterale della Russia, generando una crisi, almeno diplomatica, tra le due potenze. Un indicatore efficace di quanto siano divenuti più difficili i rapporti tra il Cremlino e i Paesi ex URSS è la rottura tra Russia e Armenia, uno degli Stati ex sovietici storicamente più legati a Mosca. L'Armenia ha pagato a caro prezzo il mancato sostegno all'operazione russa in Ucraina e un avvicinamento agli Stati Uniti ritenuto eccessivo dal Cremlino. Così, quando nel settembre 2023 l'Azerbaigian ha attaccato e annesso la regione contesa del Nagorno Karabakh, la Russia non è intervenuta in difesa dell'Armenia, che in seguito ha ufficialmente abbandonato il trattato di alleanza militare che la vincolava a Mosca[97]. Un segnale di potenziale disallineamento tra le esigenze di Mosca e gli interessi di Pechino è invece la nuova cooperazione militare tra il Cremlino e la Corea del Nord, sancita prima da un trattato di difesa bilaterale e poi dall'invio di truppe nordcoreane in Ucraina. L'attivismo della Russia nei confronti di uno Stato che la Cina considera un proprio satellite, nonché una pedina strategica fondamentale nei futuri equilibri dell'Indo-Pacifico, sembra non sia stato gradito a Pechino[98]. Ragionevolmente, la Cina può temere che la Corea del Nord offra supporto alla Russia per ottenere da quest'ultima margini di autonomia dalla Cina stessa, specularmente a quanto iniziano a fare – a parti invertite e in modo meno eclatante – gli Stati dell'Asia centrale.

Se l'analisi delle esercitazioni militari ha mostrato una comunità di intenti all'insegna della stabilità regionale, i complessi equilibri in politica estera suggeriscono pertanto un quadro più problematico. Quali sono le altre variabili che potrebbero avvicinare o allontanare Russia e Cina?

La Russia, la Cina e le scelte dell'Occidente

Il rapporto russo-cinese non può essere definito "alleanza" e difficilmente tale diverrà in futuro. Le alleanze sono infatti sancite da un trattato militare e spesso non sono paritetiche,

---

[95] HAMILTON R. E., *China, Russia, and Power Transition in Central Asia*, Foreign Policy Research Institute (FPRI), May 2024, https://www.fpri.org/article/2024/05/china-russia-and-power-transition-in-central-asia/

[96] Uno dei *report* analitici più aggiornati in merito a questo dibattito è attualmente KENDALL-TAYLOR A. - CURTIS L. - JOHNSTON K. - SCHOCHET N., *Russia and China in Central Asia Cooperate, Compete, or De-conflict?*, Center for New American Security (CNAS), November 2024, https://www.cnas.org/publications/reports/russia-and-china-in-central-asia.

[97] Per una ricognizione analitica di questa vicenda mi permetto di rimandare a CITATI D., *Il caso del Nagorno Karabakh. Cosa insegna la vittoria dell'Azerbaigian sugli Armeni?*, in «Rivista Militare» 4 (2024), pp. 34-37.

[98] WINTOU P., *China Unnerved by Russia's Growing Ties With North Korea, Claims US Official*, «The Guardian», 24/11/2024, https://www.theguardian.com/world/2024/nov/24/china-unnerved-russia-growing-ties-north-korea-claims-us-official

poiché contemplano quasi sempre uno Stato egemone e Paesi più deboli che ad esso si affidano per la propria difesa, come nel caso del Patto Atlantico e del Patto di Varsavia. Gli studiosi utilizzano talora il termine 'partenariato', che è sicuramente un termine tecnico più corretto per indicare invece buoni rapporti tra due potenze di livello mondiale come Russia e Cina[99]. Può tale partenariato evolvere in senso propriamente 'strategico', cioè definire un'intesa segnata da una precisa e condivisa visione geopolitica, anche in assenza di un trattato militare di mutua assistenza?

Russia e Cina non hanno mai espresso una dottrina comune e le dichiarazioni in favore di un mondo 'multipolare' sono troppo generiche per assurgere a un livello programmatico[100]. Russia e Cina non hanno mai espresso una dottrina comune, e le dichiarazioni in favore di un mondo 'multipolare' sono, come non di rado le conferenze bilaterali (o multilaterali) partecipate da Mosca e Pechino, troppo generiche per assurgere ad un livello programmatico. La Cina d'altronde ha mantenuto un atteggiamento ambiguo rispetto allo stesso conflitto russo-ucraino, difendendo verbalmente la sovranità dell'Ucraina e allo stesso tempo condannando l'allargamento ad est della NATO, ovvero proponendosi come mediatore ma limitandosi, nei fatti, a dichiarazioni e iniziative diplomatiche molto blande. Certo non ha mai appoggiato, almeno direttamente, lo sforzo bellico della Russia, come hanno fatto invece Iran e Corea del Nord inviando uomini e mezzi.

Particolarmente inadeguate appaiono inoltre le interpretazioni di tipo ideologico, sia da parte degli avversari sia da parte dei sostenitori. Non è in alcun modo provabile l'esistenza di un 'asse delle autocrazie' tra Russia e Cina contro il mondo libero e democratico, né sembrano convincenti le dichiarazioni circa 'l'amicizia senza limiti' su cui sarebbero instradati i due Paesi[101]. Il rapporto tra Russia e Cina è insomma un'intesa flessibile basata sulla *Realpolitik*, su un calcolo ragionato di interessi che può svilupparsi o entrare in crisi in base al verificarsi o meno di eventi concreti.

A tal proposito, nel tentativo di delineare le linee di evoluzione futura del rapporto russo-cinese, una ricercatrice statunitense ha proposto un interessante modello statistico-quantitativo basato su quattro indicatori: 1. Il *procurement* militare; 2. La condivisione di progetti industriali; 3. Il livello di coordinamento istituzionale; 4. La preparazione militare congiunta. Assegnando un punteggio (basso, moderato, alto) a ciascun indicatore, si può cercare di misurare la tenuta di quello che l'autrice definisce il grado di allineamento tra Mosca e Pechino[102]. Questo tipo di analisi predittiva, che pare ispirarsi alle tecniche analitiche strutturate (SATs) della tradizione d'*intelligence* statunitense[103] offre spunti ragguardevoli ma ha il limite di considerare solo parametri interni al rapporto russo-cinese. A questi si potrebbero dunque aggiungere le variabili esterne più importanti: le politiche di USA e alleati nei quadranti geopolitici di interesse per Mosca e Pechino. La Russia considera l'Europa e il Medio Oriente i teatri privilegiati d'azione, come dimostrano le operazioni militari in Siria e Ucraina e l'espansionismo nel Mediterraneo. La Cina concentra i propri interessi nell'Indo-Pacifico e ha apertamente dichiarato la necessità d'una futura riunificazione con Taiwan.

Se ad esempio l'Occidente negoziasse con la Russia una divisione territoriale dell'Ucraina, l'architettura di sicurezza NATO in Europa o la presenza russa in Medio Oriente, Mosca potrebbe avere meno interesse a sostenere Pechino in un eventuale attacco della Cina a Taiwan? O al contrario, un atteggiamento all'insegna del compromesso diplomatico con la Russia costituirebbe per la Cina un incentivo a muovere guerra in Asia, contando anche sul supporto di Mosca? Lo sviluppo di una serie di 'analisi di ipotesi confliggenti' che mettano in correlazione incrociata tutti questi dati (gli indicatori interni del rapporto Russia-Cina; le possibili scelte dell'Occidente; le reazioni di Mosca e di Pechino alle singole ipotesi), costituirebbe forse un utile strumento di lavoro per prevedere l'andamento dell'intesa flessibile tra le due potenze.

---

[99] Per approfondire la distinzione tra partenariato e alleanza, si veda SNYDER, G. H., *The Security Dilemma in Alliance Politics*, «World Politics» 36 (1984), pp. 461-495; ID., *Alliance Politics*, London 1997.

[100] ALEXEEVA O. - LASSERRE F., *The Evolution of Sino-Russian Relations as Seen from Moscow: The Limits of Strategic Rapprochement* in «China Perspective» 3 (2018), pp. 69-77.

[101] Cfr. LO B., *The Sino-Russian Partnership. Assumptions, Myths and Realities*, Institut Français de Relations Internationales (IFRI), January 2023, https://www.ifri.org/en/studies/sino-russian-partnership-assumptions-myths-and-realities .

[102] SKYLAR-MASTRO O., *Sino-Russian Military Alignment…,* op cit., p. 263.

[103] Si veda il classico PHERSON R. H. - HEUER R., *Structured Analytic Techniques for Intelligence Analysis*, Washington DC, 2010.

RENATO MESSINA

Ufficiale dell'Esercito in servizio presso il Comando Forze Operative Terrestri e frequentatore del 27° corso ISSMI. Ha prestato servizio precedentemente al NATO Rapid Deployable Corps – Spain e al 7° reggimento bersaglieri.

COGNITIVE WARFARE, AN URGENT FIX FOR THE ITALIAN DEFINITION

La cognitive warfare (CW) sta emergendo come un nuovo paradigma nei conflitti moderni, attirando crescente attenzione nel dibattito strategico internazionale. Questo studio analizza criticamente il concetto di CW così come definito nel documento "Cognitive Warfare – la competizione nella dimensione cognitiva" (2023) dello Stato Maggiore della Difesa italiano (SMD). Attraverso un'analisi qualitativa, concettuale e testuale basata sulle scienze strategiche, la ricerca mira a valutare la solidità concettuale dell'attuale definizione italiana di CW. I risultati evidenziano alcune carenze riguardo alla natura della CW, al suo rapporto con i principi storici della military deception e alla specificità degli obiettivi. Lo studio propone definizioni alternative e raccomandazioni concrete per affinare e consolidare il concetto italiano di cognitive warfare, contribuendo così al suo sviluppo teorico e operativo. Le implicazioni di questo studio possono allargare lo spazio di discussione in tema di cognitive warfare e favorire il lavoro concettuale dello SMD.

Parole chiave: cognitive warfare, strategia militare, dottrina italiana, analisi concettuale, military deception

ABSTRACT

Cognitive warfare (CW) is emerging as a new paradigm in modern conflicts, attracting increasing attention in international strategic debates. This study critically analyzes the concept of CW as defined in the 2023 document "Cognitive Warfare - Competition in the Cognitive Dimension" by the Italian Defence General Staff (IDGS). Through a qualitative and textual analysis based on strategic sciences, the research aims to evaluate the conceptual solidity of the current Italian definition of CW. The results highlight some deficiencies regarding the nature of CW, its relationship with historical principles of military deception, and the specificity of its objectives. The study proposes alternative definitions and concrete recommendations to refine and consolidate the Italian concept of cognitive warfare, thus contributing to its theoretical and operational development. Implications of this study can enlarge the field of discussion about cognitive warfare and support the IDGS in its conceptual work.

Keywords: cognitive warfare, military strategy, Italian doctrine, conceptual analysis, military deception

Introduction and literature review

With the publication of the document "Cognitive Warfare - Competition in the Cognitive Dimension," the IDGS has positioned itself at the forefront of efforts to provide a structured framework for the emerging concept of CW. Although the cognitive dimension is not a new aspect of war—as Clausewitz clearly states when he describes the ultimate aim of war as the subjugation of the enemy to our will[104]—contemporary and future technologies, new domains, and the widespread connectivity available to much of the population could make the cognitive dimension more decisive than in the past. Traditional propaganda techniques can now leverage artificial intelligence and social networks to influence both adversary and friendly populations, while classic military deception can exploit space and cyber domains to amplify

[104]CLAUSEWITZ, K., *Della Guerra*, Arnoldo Mondadori Editore, Roma 1970.

its effects. The literature on cognitive flaws is extensive, including well-known publications aimed at a general audience. Books such as *Thinking, Fast and Slow* by Daniel Kahneman (2011) and *Noise: A Flaw in Human Judgment* (2021) by Kahneman, Sibony, and Sunstein have brought the topics of cognitive biases and limitations to global attention, by a psychological perspective. Within NATO, work on cognitive issues related to warfare is still ongoing, and a shared definition of the concept is expected shortly. In recent years, the academic sphere has also dedicated itself to the study of this subject as evidenced by the seminal work of Du Cluzel (2021)[105], which defines cognitive warfare as "...the way of using knowledge for a conflicting purpose," and that of Clavarie and Du Cluzel (2022)[106], which began to propose possible definitions and identify areas of development. Mahjoub Eshrat-abadi and Shakuri Moghani (2022)[107] highlight how there is often a risk of falling into fallacies that reduce CW exclusively to the psychological field, "cognitive operations," interference, compromise, military operations, or battlefield application. The debate has gradually been enriched by contributions such as the brilliant critical analysis of Deppe and Schaal (2024)[108], who have proposed their own formulation, attempting to bridge the gap between academic and institutional military definitions. In the same year, Drmotova and Kutej[109] identified three main segments of cognitive warfare: neuroscience, social sciences, and technology. Cambria and Curcio (2024)[110] provided a brilliant definition of the cognitive dimension, both in general and operational terms. The Italian Defence has adopted a transitional definition, reported in the preface of the aforementioned document, which describes cognitive warfare as "... a multi-domain operation (or part thereof) that employs means, actions, and tools across the connections between classical domains (land, air, naval), space and cyber domains, the information environment, and the electromagnetic spectrum, influencing human behaviour and generating effects in the cognitive dimension, with the aim of gaining an advantage over the adversary.". This approach, although certainly useful in establishing a starting point for discussion in the professional sphere, is exposed to potential misunderstandings and difficulties in the application phase.

Methodology

This study employs a qualitative and textual analysis approach rooted in strategic sciences to critically examine the concept of cognitive warfare (CW) as defined by the Italian Defence General Staff (IDGS). The research addresses two primary questions:

1. How can strategic science improve the Italian definition of cognitive warfare?
2. What practical options are available for the evolution of the current definition?

The analysis primarily focuses on the document "Cognitive Warfare - Competition in the Cognitive Dimension" published by the IDGS in 2023. The reason for this choice is that the named document is the only official and public position of the IDGS about CW. The methodology involves a critical examination of the components within the Italian CW definition, comparing it with existing strategic science concepts and military historical evidence. This approach allows for a comprehensive evaluation of the definition's strengths and weaknesses, grounded in established theoretical frameworks and historical precedents. The study proceeds through the detailed analysis of the IDGS definition, the comparison of these components with relevant concepts from strategic sciences and military history, the synthesis of findings to identify conceptual gaps and areas for improvement and the

---

[105] DU CLUZEL, F., *Cognitive Warfare,* NATO ACT Innovation Hub, 2021. Available at https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf, visited on 13th november 2024.

[106] CLAVERIE, B. - DU CLUZEL, F. *The Cognitive Warfare Concept,* NATO ACT Innovation Hub, 2021. Available at https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf, visited on il 13 november, 2024.

[107] MAHJOUB ESHRAT-ABADI, H. - SHAKURI MOGHANI, S., *Modern Cognitive Warfare: From the Application of Cognitive Science and Technology in the Battlefield to the Arena of Cognitive Warfare,* in «Journal of Human Resource Studies», 2022, Spring, Vol. 12, N. 2, pp. 156-180.

[108] DEPPE, C. - SCHAAL, G. S., *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept,* 2024. Available at https://pubmed.ncbi.nlm.nih.gov, visited on 21 november 2024.

[109] DRMOTOVÁ, K. - LIBOR, K. *Cognitive Warfare as a New Dimension of Security. A Fictional Concept or a Real Silent Threat?,* in Vojenskè Rozhledy (Czech Military Review), 2024, available at https://vojenskerozhledy.cz/en/, visited on 21 november 2024.

[110] CAMBRIA, A. – CURCIO, M. *A definition of cognitive dimension and its exploitation in the military affairs*, in «Strategic Leadership Journal», 2024, Vol. III.

formulation of alternative definitions that address the identified shortcomings.

Findings

The findings of the study highlight three key deficiencies in the Italian Defence General Staff's (IDGS) definition of cognitive warfare (CW). Firstly, the current characterization of CW as merely an "operation" is seen as inadequate, failing to encompass its broader strategic implications and transformative potential. Secondly, the definition does not clearly differentiate between cognitive effects and behavioural outcomes, a critical oversight that undermines the practical application and evaluation of CW strategies. Lastly, the stated objective of gaining an advantage over adversaries is too generic because does not provide any specific characterization of the possible competitive advantage provided by CW. These findings underscore the necessity for a revised definition by the IDGS.

Discussion

Only an “operation”?

The definition provided by the IDGS states that cognitive warfare is an operation. Using NATO's definition of operation, which is "a sequence of coordinated actions with a defined purpose"[111], what is called warfare in the name is then defined differently. This does not represent a problem so much for the semantic difference as for the breadth and ambition of CW itself. Indeed, a coordinated sequence of actions presupposes both an available doctrine that allows practical application, a characteristic currently not applicable in the field of CW. If the aspiration is to create a new way of war, the term operations is far too limited. According to Echevarria, a way of war "...implies thinking about conflict holistically, from prewar condition-setting to the final accomplishment of one's strategic objectives"[112]. Referring to Echevarria[113], it is also highlighted how relevant it is to be aware of a structural difference between what could be a *way of war* and a *way of battle*. Echevarria, in fact, although in a different context, highlights how the current American way of war is more a way of battle. Echevarria's critique, writing this article in 2004, points to the fact that American military culture is focused on purely technical military aspects and does not effectively connect success in war with the achievement of political objectives. For our purposes, however, this differentiation can be particularly useful in helping and guiding us in reasoning about CW and its future evolution. The American strategist's reasoning suggests a question that CW theory should answer, namely whether it should be considered (or if one wants to develop it as) a way to win the war or also a solution to "win the peace". A definition of CW according to this canon would, therefore, allow emphasizing its comprehensive approach, assuming a high level of ambition even without already having a fully available doctrine.

Another opportunity is to define CW as a theory of war, as it adequately falls within being a "... epistemology relating to the phenomenon of war, and all its related aspects, that seeks to understand it and its links to wider conflict; and provide a framework for the valid creation and dissemination of knowledge concerning war and warfare"[114]. Considering CW as a theory of war would emphasize the multi-domain character and transversality to the instruments of national power. In this case, the level of ambition would be maximum, aiming to develop a holistic approach in confronting war itself. Moreover, we should consider that Clausewitz, in “On war”, explicitly states that theory should not aim to dictate actions through rigid rules but should instead provide tools for understanding war's nature and dynamics. He writes, "Theory should be study, not doctrine. This point of view makes theory possible and eliminates its conflict with reality"[115]. For Clausewitz, another key requirement for a theory of war is the importance of grounding theory in historical experience. He writes, "The knowledge which is basic to the art of war is empirical"[116] emphasizing that historical examples provide clarity and proof in understanding war's nature. However, he cautions against misusing history by drawing simplistic analogies or applying outdated lessons without considering contemporary

---

[111] NATOTerm database, visited on 20 november 2024.
[112] ECHEVARRIA, A. J., *Toward an American Way of War*, USAWC Press, 01 march 2004.
[113] Ibid.
[114] BOSIO, N. J. *Undestanding war’s theory: what military theory is, where it fits, and who influence it?,* Australian Army Occasional paper, april 2018.
[115] CLAUSEWITZ, K., op. cit.
[116] Ibid.

contexts.
Another way to address this issue is to consider CW a strategic theory. Colin Gray believes that a strategic theory "...educates the mind by providing intellectual organization, defining terms, suggesting connections among apparently disparate matters, and offering speculative consequentialist postulates"[117]. Adopting such an approach would then aspire to provide a solid corpus of ends, ways, and means applicable to the contemporary context, while unleashing the exciting potential of producing cognitive strategies.
If, on the contrary, one aspired to a more limited definition, it might prove opportune to orient oneself towards the observation of the state of the art here and now, using *ad hoc* formulations that capture only and exclusively what is reasonably and predictably possible to insert in this field. Although less appealing, the use of descriptions such as "integrated employment of means and methods...", instead of the term operation, would return a realistic picture of what exists and could reasonably exist, while still leaving room for the possibility of real employment of some of these means and methods, even in the face of a doctrine that is not yet structured. This range of formulations would certainly be less ambitious but would probably respond to more practical needs.

Cognitive Warfare and Multidomain approach
The IDGS definition states clearly that CW is multidomain. This represents a coherent and logical evolution from several perspectives. First, ongoing western doctrines defines themselves as “multidomain”. While it remains debatable whether this is an actual characteristic or merely an aspirational end state, aligning CW with current doctrinal frameworks ensures consistency. Second, military history—particularly in the context of deception—provides valuable insights. A key lesson from the practice of deception is that a ruse directed at an enemy through only one source or channel is often destined to fail, as demonstrated by the works of Barton Whaley[118] about the historical evidence of success and failure in military deception. We can reasonably argue that historical evidence supports the aspiration for CW to be multidomain by design, even if it is not an inherently necessary feature.

The “friendly side of Cognitive Warfare”
The current Italian definition of CW primarily emphasizes its application against adversaries. However, this definition does not explicitly address the role of CW in enhancing the cognitive capabilities of friendly forces, even though such an implication can be inferred from the broader context of the document. The document highlights the importance of leveraging emerging technologies and integrating cognitive strategies across various domains, suggesting that CW is not solely about degrading adversary cognition but also about enhancing one's own. For instance, references to "cognitive enhancement" and the integration of interdisciplinary resources indicate potential applications for improving decision-making, situational awareness, and operational effectiveness within friendly forces. Nevertheless, these aspects remain implicit and are not clearly articulated as part of CW's definition. This omission risks underrepresenting a critical dimension of CW—its potential to strengthen friendly capabilities in addition to countering threats. To fully capture the dual nature of CW, it would be beneficial for the Italian definition to explicitly include its application to the friendly side.

“What do you want the enemy to do?”
A subsequent part of the CW definition by IDGS states "... influencing human behaviour and generating effects in the cognitive dimension...", appropriately highlighting the characteristic elements of this new methodology of confrontation and conflict. The main issue with this part of the definition lies in the fact that the pursuit and achievement of cognitive effects is never sufficient to accomplish anything. There is a substantial difference between possible cognitive effects and actual behaviours. This difference is excellently illustrated by addressing the foundations of military deception and using some solid historical evidence like the one of Col. Dudley Clarke during the II world war. In 1941, Col. Dudley Clarke had already been in

[117] GRAY, C. S. *Modern strategy*, Oxford University Press, Oxford 1999, p. 36.
[118] WHALEY, B., *Practice to deceive – learning curves of military deception planners*, Naval Institute Press, Annapolis 2016 e WHALEY, B., *Tournabout and Deception: crafting the double-cross and the theory of out*, Naval Institute Press, Annapolis 2016.

command of the so-called "A" Force for a year, which was the group of planners based in Cairo responsible for English deception plans for Gen. Archibald Wavell, as part of British operations in Africa. That year, Clarke prepared the deception plan against Italian forces in Ethiopia and found himself addressing the very issue of cognitive effects and expected behaviours. Even though the deception was well executed, the Italians did exactly the opposite of what was expected of them. We can read from his own word the faced challenge from his memoirs: "In the first Deception Plan I ever tackled I learned a lesson of inestimable value. The scene was Abyssinia.... Gen. Wavell wanted the Italians to think he was about to attack them from the south in order to draw of forces from those opposing him on the northern flank. The Deception went well enough-but the result was just the opposite of what Wavell wanted. The Italians drew back in the South, and sent what they could spare from there to the North, which was of course the true British objective. After that it became a creed in "A" Force to ask a General – What do you want the enemy do to? – and never – What do you want him to think?" [119]. Clarke encountered the same type of conceptual difficulty that transpires from the current definition of CW, namely failing to unequivocally clarify that the actual goal is a behaviour experienced by a person or group of people and not just a perception or thought. More recently in 2021, Israeli Defense Forces (IDF) purposedly and successfully deceived Hamas fighters using mass media and social networks. In this case the connection between cognitive effect and actual behaviours worked quite effectively. As described in the words of a New York Times article "The Israeli military abruptly announced after midnight on Friday that its ground forces had begun - attacking in the Gaza Strip - saying it on Twitter, in text messages to journalists, and in on-the-record confirmations by an English-speaking army spokesman. Several international news organizations, including The New York Times, immediately alerted readers worldwide that a Gaza incursion or invasion was underway, a major escalation of Israeli-Palestinian hostilities. Within hours, those reports were all corrected: No invasion had taken place. Rather, ground troops had opened fire at targets in Gaza from inside Israeli territory, while fighters and drones were continuing to attack from the air. A top military spokesman took responsibility, blaming the fog of war. But by Friday evening, several leading Israeli news outlets were reporting that the incorrect announcement was no accident but had actually been part of an elaborate deception. The intent, the media reports said, was to dupe Hamas fighters into thinking that an invasion had begun and to respond in ways that would expose far greater numbers of them to what was being called a devastatingly lethal Israeli attack."[120]. This example shows clearly that the desired strategic or tactical effect needs to be something performed in practical ways.

This "cognitive-behaviours link" remains valid even when it comes to influencing groups of people, political and social leaders, and not just military decision-makers. One always seeks a desired behaviour (even in a negative direction), be it a vote, a *like*, or an operational decision. Consequently, stating that CW performs its function by "influencing behaviour and generating cognitive effects"[121] dangerously places on the same level two effects that are one the consequence of the other. This part of the definition could be corrected by explicating the correct logical sequence of the two parts or by eliciting the part of cognitive effects, safeguarding the purpose that describes the achievement of desirable behavioural effects.

A solution looking for a problem

We thus arrive at the final part of the definition of CW, namely the specification of its purpose. The IDGS writes that CW has "...the objective of gaining an advantage over the adversary."[122] This purpose, drafted in such generic terms, corresponds to the immediate purpose of any competitive activity. The fundamental problem is of a logical nature, as the parties involved in a competitive relationship will necessarily seek an advantage over the adversary. However, the absence of a shared, clear, and qualifying purpose is a symptom and not the problem. CW's potential is hindered by the diverse range of activities and tools associated with it, making it objectively difficult to identify a characterizing purpose. This ensemble, consisting mainly of diversified resources and technologies, struggles to solve a

---

[119] WHALEY, B., *Practice to deceive – learning curves of military deception planners*, Naval Institute Press, Annapolis 2016, p. 33.

[120] HALBFINGER, D., *A press corps deceived, and the Gaza invasion that wasn't*, New York Times, 14/05/2021, visited on 20/02/2025, https://www.nytimes.com/2021/05/14/world/middleeast/israel-gaza-disinformation.html

[121] SMD, *cognitive warfare*, op. cit..

[122] Ibid.

problem more specific than a generic advantage over the adversary. The difficulty is profound because, even if one were to try to introduce a more recognizable purpose, such as the modification of behaviours, one would quickly fall back into the realm of multi-domain and technologically advanced deception, which would still leave out many elements that can currently fall under CW, such as the pharmacological enhancement of cognitive performance. The problem of purpose coincides with the problem of delimiting the field of action, and they can hardly be separated from each other. In this field, C. J. Wylie's interpretation of the main descriptive pattern of war can help us: "...as far as the aggressor is concerned, the pattern of war consists of his attempts to establish and maintain, primarily by military means, a measure of control over the conservator sufficient to force the conservator to conform to whatever may be the aggressor's terms."[123]. Understanding war as an attempt to establish a certain degree of control over the adversary perfectly aligns with the emerging concept of CW, facilitating the linkage of such variety of tools and techniques with a political objective.

Limitations

This study has several limitations, mainly the lack of quantitative analysis and the probable cognitive biases of the qualitative approach. Moreover, approaching the field by the perspective of strategic sciences and military history leaves several points of view not covered. It's also important to note that while the study proposes alternative definitions based on identified flaws, there may be other potential formulations of cognitive warfare that have not been considered. The field's complexity and interdisciplinary nature suggest that further definitions could be derived from different analytical approaches or emerging research in related domains.

Way ahead for the Cognitive Warfare's definition and practical implications

In conclusion, an in-depth analysis of the Italian definition of CW has revealed several conceptual gaps that warrant careful consideration. Firstly, the characterization of CW as a mere "operation" proves inadequate in capturing its true essence and transformative potential. This limited conceptualization risks underestimating the scope and impact of CW, opening an opportunity for a discussion aimed at elevating it to the status of a "way of war" or even a "theory of war". Such a reformulation would allow for the recognition of the holistic and pervasive nature of CW, which transcends the traditional boundaries of military operations. A second critical aspect emerges from the failure to distinguish between cognitive and behavioural effects in the current definition. This omission not only neglects a fundamental principle well-rooted in the practice of military deception but also risks diverting attention from the concrete and measurable objectives of CW. It is essential to recognize that, while cognitive alterations are a crucial means, the true purpose of CW lies in modifying the observable behaviours of our audience or person of interest. This clarification is not merely semantic but has profound implications for planning and evaluating the effectiveness of CW operations. Furthermore, the generality of the stated objective - "to gain an advantage over the adversary" - proves insufficient in capturing the specificity and innovative potential of CW. This vague formulation could apply to any form of conflict or competition, failing to highlight what makes CW unique and potentially revolutionary. Ultimately, given the experimental momentum undertaken by the IDGS in formulating an initial definition of CW, a revision is desirable to create a robust conceptual framework that recognizes CW as an emerging paradigm in the conduct of warfare, capable of integrating cognitive, behavioural, and technological elements into a coherent, albeit transitory and evolving, body of knowledge. The following recommended definitions, based on the level of ambition and comprehensiveness to which one might aspire, provide viable options for the progression of the Italian definition of CW by the Italian Defence:

- Cognitive warfare is a theory of war that considers it essential that the domain of human cognition be enhanced in the friendly part and degraded in the hostile one in order to obtain a certain degree of control over the adversary and, consequently, the desired political objectives (Italian: la *cognitive warfare* è una teoria della guerra che ritiene essenziale che l'ambito della cognizione umana sia potenziato nella parte amica e

[123] WYLIE, J. C. *Military strategy: a general theory of power control,* Naval Institute Press, Annapolis 2014.

degradato in quella ostile al fine di ottenere un certo grado di controllo sull'avversario e, conseguentemente, gli obiettivi politici desiderati).

- Cognitive warfare is a method of warfare that, through the use of interdisciplinary resources and a multi-domain approach, aims to achieve strategic, operational, and tactical objectives, thanks to the achievement of cognitive enhancement of one's own forces and the simultaneous cognitive degradation of those of the adversary (Italian: la *cognitive warfare* è un metodo di guerra che, attraverso l'impiego di risorse interdisciplinari e approccio multidominio, mira ad ottenere obiettivi strategici, operativi e tattici, grazie al potenziamento cognitivo delle proprie forze e al contemporaneo degradamento cognitivo di quelle avversarie).
- Cognitive warfare is the integrated employment of interdisciplinary resources and a multi-domain approach, characterized by the cognitive enhancement of one's own forces and the simultaneous cognitive degradation of those of the adversary in order to contribute to the success of an operation or mission (Italian: la *cognitive warfare* è l'impiego integrato di risorse interdisciplinari e approccio multidomino, caratterizzato dal potenziamento cognitivo delle proprie forze e dal contemporaneo degradamento cognitivo di quelle avversarie al fine di contribuire al successo di un'operazione o missione).

Further scientific research could provide alternative ways to elaborate the definitions, different frameworks and processes for the analysis, new methods to integrate cognitive warfare ways and means as well as comparative approaches could benefit a better understanding of the cognitive warfare.

By a practical perspective, IDGS could take steps to foster a CW culture within the Armed Forces. The more ambitious the chosen definition of CW, the greater the effort required to enhance CW practices, training, and education. The cultural shift needed could be significant and must begin as early as the education phase following personnel recruitment. The most affected groups are likely to be Officers and Non-Commissioned Officers, along with their respective education and training pathways. Specifically, the Armed Forces should:

- introduce basic deception principles and techniques during the early stages of education in military academies;
- by default, incorporate deception planning into training and exercises;
- utilize wargaming as a tool for cognitive warfare experimentation and training;
- offer more advanced cognitive warfare theory (and potentially practical applications) during the Joint Staff Course (Istituto Superiore di Stato Maggiore Interforze, ISSMI).

MARCO MARSILI

Researcher at Cà Foscari University of Venice, specializing in international relations, security, and defense, with a focus on international humanitarial law, human rights, hybrid and cognitive warfare

EMERGING AND DISRUPTIVE TECHNOLOGIES: STRATEGIC IMPLICATIONS AND ETHICAL CHALLENGES OF DUAL-USE INNOVATIONS

ABSTRACT

Emerging and disruptive technologies (EDTs) are at the forefront of global innovation, influencing geopolitics, security, and organizational development. These technologies—spanning artificial intelligence, quantum computing, and autonomous systems—serve dual purposes, with applications in both civilian and military contexts. This dual-use nature poses significant ethical and legal challenges, particularly regarding their potential misuse in conflict settings. This article examines the strategic implications of EDTs, with a focus on their role in reshaping power dynamics and their ethical compliance with international standards. Recommendations are offered to address regulatory gaps and ensure responsible innovation.

Keywords: Autonomous Systems, Artificial intelligence, Dual-use Technologies, Global Governance, International Law.

Introduction

Emerging and disruptive technologies are dramatically reshaping the global security landscape, presenting both substantial opportunities for innovation and significant challenges. These technologies—ranging from artificial intelligence (AI) and robotics to autonomous systems, quantum computing, and biotechnology—have the potential to revolutionize a wide array of sectors, including healthcare, industry, and national security. However, the dual-use nature of many of these technologies, which allows them to serve both civilian and military purposes, creates complex interactions between technological advancement, regulation, and security. This dual-use characteristic raises critical questions about governance, ethical considerations, and the broader implications for global security and stability.

A notable example of dual-use technology is unmanned aerial vehicles (UAVs), commonly referred to as drones. While drones are extensively used in civilian sectors - such as agriculture, logistics, and disaster response - they also have significant military applications, including intelligence gathering, precision strikes, and electronic warfare. As Gettinger (2019) highlights, drones have revolutionized industries such as agriculture by enabling efficient monitoring of crops and logistics by assisting in goods delivery and search-and-rescue operations (p. 136). However, their adaptability for military use presents challenges in regulating technologies that seamlessly transition between civilian and military domains, raising concerns about potential misuse and the complexities of oversight, particularly with regard to non-state actors (p. 138).

The ethical and legal dilemmas surrounding EDTs, particularly lethal autonomous weapons systems (LAWS), are another critical area of concern. These systems, capable of selecting and engaging targets without human intervention, have sparked intense debates about their ethical implications. Crootof (2015) argues that the deployment of autonomous weapons, often referred to as "killer robots", presents significant legal and ethical challenges, particularly regarding accountability, proportionality, and compliance with international humanitarian law (p. 1845). As military technologies become faster and more autonomous, traditional

frameworks for ensuring accountability in armed conflict become increasingly inadequate. Crootof emphasizes that attributing responsibility in situations where systems operate autonomously poses profound challenges, highlighting significant gaps in legal and ethical accountability (p. 1847). These concerns underscore the need for updated legal and ethical frameworks to address the emerging risks of these technologies.

In addition to autonomous weapons, the integration of AI and machine learning into military operations raises new governance challenges. AI's capabilities in real-time data analysis and predictive modeling have become invaluable for enhancing military decision-making and operational efficiency. However, as Marsili (2023) points out, the incorporation of these technologies into military operations must be carefully aligned with international law and ethical standards to avoid misuse (p. 115). While these technologies offer substantial military advantages, Marsili stresses the importance of regulating their use to ensure compliance with humanitarian principles, particularly regarding the protection of civilians and adherence to international human rights law (p. 116). Ensuring the responsible deployment of EDTs requires establishing governance structures that balance technological innovation with the protection of fundamental ethical standards. Additionally, Marsili and Wróblewska-Jachna (2024) emphasize that integrating AI into military strategies should be done with great care to ensure compliance with international norms and human rights protections, ensuring that these advancements do not lead to unintended consequences (p. 25).

Furthermore, the implications of EDTs extend beyond the battlefield, with civilian applications advancing faster than the development of regulatory frameworks. As technologies such as AI, cybersecurity, and biotechnology proliferate in civilian sectors, concerns about their potential misuse by both state and non-state actors grow. These technologies often present vulnerabilities that can be exploited, especially in scenarios that blur the lines between peacetime and conflict. The rapid pace of technological advancement, combined with insufficient regulation, creates a precarious environment where the risk of misuse or malicious application increases significantly. Consequently, the proliferation of EDTs requires a coordinated international response to establish norms, build trust, and prevent misuse. Regulatory bodies and international treaties must evolve to address these emerging threats and ensure that EDTs are used responsibly, both in military and civilian contexts.

This article aims to critically examine the multifaceted impact of EDTs, particularly in the context of dual-use applications, and their implications for global security and governance. It addresses the ethical, legal, and regulatory challenges that arise from the rapid development and deployment of these technologies and advocates for a balanced approach that fosters innovation while mitigating associated risks. Drawing on existing literature and case studies, this study seeks to contribute to the ongoing discourse surrounding the governance of emerging technologies and offer insights into how policymakers can navigate the complexities of EDTs in an increasingly interconnected world.

The Dual-Use Dilemma

The dual-use nature of emerging and disruptive technologies represents a multifaceted and growing challenge in the contemporary security landscape. These technologies, characterized by their potential to be used for both civilian and military purposes, pose profound ethical, legal, and operational dilemmas for states, organizations, and the global community. The rapid pace of technological innovation has not only expanded the range of applications for EDTs but has also blurred the traditional boundaries between civilian and military domains, complicating regulatory efforts and raising the stakes for international security.

Historically, technological advancements have often been dual-use in nature. However, the proliferation of EDTs in the 21st century has amplified this dilemma to unprecedented levels. As Marsili (2023) observes, technologies such as artificial intelligence, unmanned aerial vehicles, and autonomous systems are inherently neutral in design but acquire distinct characteristics based on their application (p. 118). This duality introduces significant risks, as the same technologies that drive economic and social progress can also enable conflict, destabilization, and human rights violations. Marsili further notes that the pace of technological development and the ease with which technologies can be repurposed for military use make regulating their application increasingly difficult (p. 119). Marsili and Wróblewska-Jachna (2024) similarly argue that the evolution of these technologies necessitates a rethinking of governance structures and international norms to ensure they are

used ethically and responsibly in both civilian and military domains (p. 22).

The dual-use dilemma extends beyond drones to foundational debates about regulating disruptive technologies. While the EU's precautionary approach (e.g., AI Act bans on social scoring) prioritizes human rights (European Union, 2024), critics argue that strict rules may hinder innovation. For example, historical parallels like the Papal Bull issued by Innovent II against crossbows in 1139—ignored due to their military utility—highlight the challenges of enforcing bans without verification mechanisms (Keen, 1999). Conversely, proponents of deterrence, such as U.S. initiatives to outpace China in quantum computing (White House, 2022), advocate for technological superiority over regulation. A middle ground lies in the EU's "sandbox" model, allowing controlled testing of high-risk AI under Article 53 of the AI Act.

Similarly, artificial intelligence presents a paradoxical challenge. On one hand, AI-driven innovations hold immense promise for improving quality of life through advancements in healthcare, education, and public administration. On the other hand, these same technologies are at the core of autonomous weapons systems, facial recognition for mass surveillance, and cyber warfare capabilities. The deployment of autonomous systems in conflict scenarios is particularly concerning. As Crootof (2015) argues, such systems disrupt established norms of accountability in warfare, as decisions traditionally made by human operators are now relegated to machines. This shift raises fundamental ethical questions about the delegation of lethal decision-making authority and the erosion of human oversight in life-and-death scenarios (p. 1845).

The dual-use dilemma also extends to emerging areas such as biotechnology and quantum computing. Advances in synthetic biology, for instance, offer unprecedented potential for medical breakthroughs, including personalized medicine and vaccine development. However, the same technologies can be weaponized to engineer bioweapons or manipulate genetic material for nefarious purposes. Quantum computing, while promising to revolutionize fields such as cryptography and material science, also poses significant risks to global security. A state or organization that achieves quantum supremacy could undermine existing encryption standards, threatening the integrity of financial systems, communications, and critical infrastructure (Marsili, 2023, p. 121).

An often-overlooked aspect of the dual-use dilemma is its geopolitical dimension. The competition among states to achieve technological superiority has led to a securitization of innovation, where advancements in dual-use technologies are perceived through the lens of national security. This dynamic is particularly evident in the realm of AI and cyber technologies, where rivalries between major powers such as the United States, China, and Russia drive investments in military applications of EDTs. Such rivalries not only fuel arms races but also complicate international cooperation on issues like arms control and non-proliferation (Marsili, 2022, p. 42).

Moreover, the dual-use dilemma has significant implications for global governance and regulatory frameworks. Existing mechanisms for technology control, such as export controls and international treaties, often struggle to keep pace with the rapid evolution of EDTs. The dual-use nature of these technologies challenges the traditional paradigm of arms control, which relies on clear distinctions between civilian and military applications. As Marsili (2024) highlights, addressing these challenges requires a rethinking of regulatory approaches to ensure compliance with international humanitarian law while fostering innovation (p. 67).

The ethical considerations surrounding dual-use technologies further underscore the complexity of this dilemma. Technologies such as autonomous drones, cyber tools, and AI systems raise questions about proportionality, discrimination, and accountability in their deployment. Marsili (2023) emphasizes the need for robust ethical frameworks to guide the development and use of these technologies, particularly in conflict scenarios. Without such frameworks, the risk of unintended consequences—ranging from civilian casualties to the escalation of conflicts—becomes unacceptably high (p. 120).

In addition to ethical and legal concerns, the economic implications of dual-use technologies must also be considered. The commercialization of EDTs has created lucrative markets, incentivizing private sector investment in areas like AI, robotics, and biotechnology. However, this economic potential is often at odds with security considerations, as private companies prioritize profit over compliance with international norms. Governments must therefore strike a delicate balance between fostering innovation and ensuring that dual-use technologies are

not exploited for harmful purposes.
The dual-use dilemma is not a problem that can be solved in isolation. It requires a coordinated effort involving states, international organizations, academia, and the private sector. Policymakers must develop strategies to manage the risks associated with dual-use technologies while harnessing their potential for societal benefit. This includes investing in research on the ethical implications of EDTs, strengthening regulatory frameworks, and promoting international cooperation to address the dual-use challenge in a holistic manner.

Ethical and Legal Implications of Dual-Use Technologies
The rapid development of emerging and disruptive technologies has raised profound ethical and legal challenges, particularly when considering their dual-use nature. Dual-use technologies are those that can serve both civilian and military purposes, blurring the lines between peaceful innovation and military applications. The dual-use characteristic complicates regulatory efforts and raises questions about the ethical responsibility of developing, deploying, and utilizing these technologies. As such, understanding the ethical and legal implications of dual-use technologies is crucial in addressing the risks they pose to both global security and individual rights.
One of the most contentious ethical issues surrounding dual-use technologies is the potential for misuse. Technologies originally developed for civilian purposes, such as AI, drones, and biotechnology, can easily be repurposed for military applications. This rapid adaptability raises concerns about the intentions behind their use and the consequences of their deployment. The most prominent ethical dilemma involves the development of lethal autonomous weapons systems, often referred to as "killer robots". These systems, capable of selecting and engaging targets without human intervention, are at the forefront of debates regarding technological ethics. The question of whether machines should be given the authority to make life-and-death decisions without human oversight is central to these discussions.
Crootof (2015) underscores that the use of lethal autonomous weapons systems presents significant ethical challenges, particularly concerning accountability, proportionality, and the compliance of such systems with international humanitarian law (IHL). As Crootof argues, the deployment of LAWS raises fundamental questions about who is accountable when these systems cause harm or breach the laws of war. In traditional warfare, the chain of command and human operators ensure accountability, but with autonomous systems, these lines become blurred. Crootof stresses that, in the absence of human decision-making, determining responsibility for violations becomes difficult, leading to a lack of legal and ethical accountability (p. 1847). Additionally, as LAWS become more advanced, the ethical concerns about the proportionality of their actions, especially in complex battlefield environments, become increasingly problematic. In many cases, the swift decision-making and action capabilities of LAWS may be at odds with the principle of proportionality in IHL, where the harm caused must not outweigh the military advantage gained (Crootof, 2015, p. 1849).
Moreover, as the technology behind autonomous weapons evolves, there is a growing concern about the potential for these systems to be used by non-state actors, including terrorists and criminal organizations. The ability to deploy weapons without human oversight could significantly alter the balance of power, creating new threats to international security. The ethical dilemma here lies in the fact that while these technologies could be used for peacekeeping and humanitarian missions, their ease of weaponization and rapid deployment in the wrong hands could escalate conflicts and lead to grave humanitarian crises. The possibility of such technologies being employed by malicious actors emphasizes the need for international governance structures that regulate their development and use, ensuring they do not fall into the wrong hands (Crootof, 2015, p. 1850).
Furthermore, the ethics of human enhancement and the integration of artificial intelligence into warfare and military technologies must also be addressed. The ethics of human enhancement and AI-driven surveillance intersect critically in debates over mass surveillance technologies. For instance, the EU AI Act (Regulation (EU) 2024/1689) prohibits real-time biometric identification in public spaces, citing risks to privacy under Article 8 of the *European Convention on Human Rights* (ECHR; European Union, 2024). However, exemptions for national security—such as Italy's experimental use of SARI Real-Time for counterterrorism—raise concerns about normalized mass surveillance (Garante per la

protezione dei dati personali, 2021). Judicial oversight, as emphasized in *Big Brother Watch and Others v. the United Kingdom* (ECtHR, 2018), remains essential to balance security and fundamental rights.

The legal implications of dual-use technologies are just as complex and pressing. The dual-use nature of many emerging technologies challenges the existing frameworks of international law, particularly in the areas of arms control, disarmament, and the protection of civilians. One of the key issues is the question of how to regulate technologies that are developed for civilian purposes but can easily be adapted for military use. The current legal frameworks often fail to account for the rapid evolution and dual-purpose nature of these technologies, leading to regulatory gaps that can be exploited.

In the case of drones, for instance, their widespread use in civilian applications such as surveillance, transportation, and disaster response contrasts sharply with their military applications in intelligence gathering, precision strikes, and reconnaissance. The dual-use nature of drones raises questions about the adequacy of existing laws to regulate their military use. Gettinger (2019) highlights that drones have become ubiquitous in both military and civilian sectors, and their rapid adaptability means that regulations must evolve continuously to keep pace with new developments. Gettinger argues that the lack of clear and comprehensive regulations governing drone usage increases the risk of misuse, particularly by non-state actors who may deploy drones for nefarious purposes (p. 12).

A particularly significant legal challenge posed by dual-use technologies is their compliance with international humanitarian law and international human rights law (IHRL). In the case of autonomous weapons, the principle of distinction—ensuring that military actions are directed only at legitimate military targets—becomes increasingly difficult to maintain when machines, rather than humans, make targeting decisions. This poses a direct challenge to IHL, which is designed to protect civilians during armed conflict by ensuring that the use of force is both necessary and proportionate (Crootof, 2015, p. 1852). Moreover, as these technologies become more sophisticated, the challenge of ensuring that they adhere to human rights standards, such as the right to life and the protection from arbitrary killing, grows more complicated. Legal scholars argue that new international treaties and mechanisms are necessary to establish clear guidelines for the ethical and legal deployment of autonomous systems in both military and civilian contexts.

In the context of AI, Müller (2023) addresses the ethical and legal challenges posed by artificial intelligence, particularly in relation to decision-making and the use of AI in warfare. He highlights that AI systems, while capable of performing complex tasks, present significant legal and ethical dilemmas regarding transparency, accountability, and the protection of human rights. As AI systems are increasingly integrated into military operations, the challenge lies in ensuring that these systems remain under human control and that their deployment aligns with international norms (Müller, 2023).

The regulatory challenges posed by dual-use technologies are substantial. Existing regulatory frameworks, both national and international, are often ill-equipped to address the complexities of these rapidly advancing technologies. The international community has struggled to develop effective arms control measures for technologies that can be used both for peaceful purposes and for warfare. As a result, there is an urgent need for updated governance structures that can address the unique challenges posed by EDTs.

For example, the proliferation of autonomous systems and AI technologies requires a coordinated international effort to develop norms and standards for their ethical use. Floridi, Taddeo, and Herkert (2020) emphasize that international governance bodies must play a central role in developing frameworks that regulate the use of these technologies while ensuring their responsible deployment (p. 100). They argue that the creation of new treaties or amendments to existing ones, aimed specifically at addressing the risks posed by dual-use technologies, is essential to mitigate their potential for harm. These regulatory bodies must not only enforce compliance with IHL and IHRL but also ensure that the technological development of AI and autonomous systems remains transparent and accountable.

O'Neil (2016) adds an additional layer of concern in her analysis of big data and its potential for misuse, particularly in the context of warfare and surveillance. O'Neil argues that big data, if not properly regulated, can exacerbate inequality and undermine democratic processes by providing powerful actors with unprecedented control over information and decision-making (p. 45). In military contexts, the unregulated use of big data and AI systems could lead to the

manipulation of populations and the escalation of conflicts, making the need for regulatory oversight even more urgent.

One potential solution to these governance challenges is the establishment of international oversight bodies or verification mechanisms that ensure compliance with global norms and ethical standards. The creation of international treaties and conventions that specifically address the dual-use nature of emerging technologies is another necessary step. Such legal frameworks should seek to create clear distinctions between civilian and military applications and establish guidelines for the ethical development and deployment of these technologies.

The ethical and legal implications of dual-use technologies are multifaceted and complex. These technologies present both vast opportunities and significant risks, and their rapid development and dual-use nature demand careful oversight and regulation. The ethical dilemmas surrounding autonomous weapons, AI, and other EDTs underscore the need for international governance frameworks that ensure these technologies are used responsibly, in compliance with international law, and in a manner that upholds fundamental human rights. As the global security landscape continues to evolve, the development of legal and ethical frameworks to govern dual-use technologies will be critical to ensuring that their benefits are maximized while minimizing their potential for harm.

The rapid development of emerging and disruptive technologies has raised critical ethical and legal concerns, particularly regarding dual-use technologies—those that can be used for both civilian and military purposes. While these technologies often originate in civilian sectors, their military applications can lead to unforeseen consequences, requiring urgent attention to the ethical and legal frameworks that govern their use. Understanding these implications is vital, as the line between peaceful innovation and military deployment often becomes blurred.

One of the most pressing ethical dilemmas surrounding dual-use technologies is their potential for misuse. Technologies initially designed for peaceful purposes, such as artificial intelligence, drones, and biotechnology, can be easily adapted for military purposes. This adaptability raises questions about the responsibility of developers, the security of these technologies, and the broader impact on society. For instance, lethal autonomous weapon systems, often referred to as "killer robots", present a major ethical challenge. These systems, which can operate without human intervention, bring into question the morality of entrusting machines with life-and-death decisions. As Floridi and Taddeo (2014) highlight, the development and deployment of such systems raise profound ethical issues concerning accountability, fairness, and the protection of human dignity. The autonomy of these systems complicates the establishment of clear responsibility for their actions and creates legal uncertainties, particularly in combat scenarios where human lives are at risk.

Moreover, LAWS may breach the principle of proportionality, a core tenet of international humanitarian law, which dictates that the harm caused by an attack must not exceed the military advantage gained. As these systems become increasingly sophisticated, their decision-making processes may conflict with the ethical standards of warfare, as rapid autonomous decision-making could lead to disproportionate responses in complex combat environments. The evolving capabilities of such systems necessitate careful scrutiny to ensure they align with international law and ethical standards (Floridi & Taddeo, 2014).

Another ethical issue in the use of dual-use technologies is their potential to exacerbate inequalities. O'Neil (2016**)** discusses how algorithms and big data can increase social inequality and threaten democracy, particularly in the context of predictive policing, surveillance, and decision-making processes that lack transparency. In the military context, similar algorithms could be used to target individuals or groups based on data analytics, leading to biased or unjust outcomes. O'Neil's argument—that algorithms can act as "weapons of math destruction"—is particularly relevant in discussions about the regulation of dual-use technologies, as the unchecked use of such technologies could lead to systemic harm and violations of human rights (O'Neil, 2016).

The legal challenges associated with dual-use technologies are equally complex. Technologies such as drones, which can be used for civilian applications like surveillance and transportation, are also deployed in military operations for reconnaissance and targeted strikes. As Gettinger (2019) notes, drones have become a ubiquitous tool in both civilian and military domains, with their use increasing worldwide. However, their dual-use nature complicates efforts to regulate their military applications. The development of international regulations to address the use of drones and other dual-use technologies is crucial to

preventing misuse by state and non-state actors alike. In this context, Gettinger underscores the need for stronger governance frameworks that can keep pace with the rapid development of drone technologies and ensure that they are used responsibly (Gettinger, 2019).

The integration of AI in military applications is another area of concern. Tigard (2021) explores the legal and ethical challenges posed by AI in warfare, emphasizing the importance of ensuring that autonomous systems adhere to ethical principles such as accountability, fairness, and proportionality. Tigard argues that AI systems, particularly in military contexts, must be designed with robust ethical guidelines to avoid unintended consequences, such as the escalation of conflicts or violations of international law. As AI technology evolves, its potential to influence warfare requires the creation of new legal frameworks that ensure its responsible use while minimizing harm (Tigard, 2021).

Furthermore, Floridi and Taddeo (2014) stress the ethical responsibility of developers and regulators in shaping the future of dual-use technologies. They advocate for an ethical design process that integrates consideration of the broader social implications and potential risks associated with these technologies. By establishing guidelines for the ethical development and use of dual-use technologies, Floridi and Taddeo (2014) argue, we can mitigate their potential for harm while maximizing their benefits.

In addition to addressing ethical concerns, it is essential to consider the legal implications of dual-use technologies. Existing international laws, particularly in the realms of arms control and humanitarian law, are often ill-equipped to deal with the rapid pace of technological development and the dual-use nature of many emerging technologies. As Floridi and Taddeo (2014) and others have pointed out, the use of autonomous systems and other advanced technologies in warfare may outpace existing legal frameworks, creating gaps that could be exploited by those seeking to use them irresponsibly. This highlights the need for updated governance structures that can effectively regulate these technologies while ensuring that they do not violate fundamental human rights or international law.

The regulation of dual-use technologies must also address the challenges posed by non-state actors. As technologies become more accessible and cheaper, there is an increasing risk that non-state actors, including terrorist organizations, will use these technologies for malicious purposes. For example, the use of drones in military operations by groups such as the Islamic State of Iraq and Syria (ISIS) has already demonstrated the potential for misuse of these technologies. Developing international treaties or conventions that specifically address the risks posed by non-state actors and ensure that dual-use technologies are not used for illicit purposes is essential for global security.

The ethical and legal implications of dual-use technologies are profound and far-reaching. The rapid development of AI, drones, and other disruptive technologies presents both significant opportunities and serious risks. Addressing these challenges requires the creation of robust international frameworks that regulate the development and use of these technologies, ensuring that they are used responsibly, ethically, and in accordance with international law. As Floridi and Taddeo (2014) suggest, the future of dual-use technologies must be shaped by ethical considerations that prioritize human dignity, fairness, and accountability, while balancing the potential for technological innovation with the need for legal and moral responsibility.

Regulatory Frameworks and Governance Challenges for Emerging Disruptive Technologies

Emerging technologies, such as artificial intelligence, autonomous systems, drones, and biotechnology, present significant regulatory challenges due to their dual-use nature. These technologies, capable of both civilian and military applications, often evolve more rapidly than existing governance structures. As these technologies become more widespread across various sectors, the lack of clear and robust regulatory frameworks raises concerns regarding their safe and ethical use, particularly in the context of national security, human rights, and global stability.

One of the main challenges in regulating emerging technologies is the speed at which they evolve. As these technologies mature, they often surpass the ability of existing legal and regulatory bodies to implement adequate safeguards. According to Floridi and Taddeo (2014), "The complexity and speed of technological change demand a governance framework that is both flexible and forward-looking" (p. 1). Traditional regulatory models, which tend to be

slow and reactive, struggle to address the new issues posed by emerging technologies such as automated warfare, autonomous weapons, and surveillance systems. This gap between technological development and regulation can lead to unintended consequences, including abuse, human rights violations, and heightened geopolitical tensions.

The increasing use of AI and autonomous systems in military operations highlights the urgent need to update governance structures to address the ethical and legal concerns surrounding these technologies. Lethal autonomous weapons systems, for example, can operate without direct human intervention, raising critical questions about accountability, attribution, and compliance with international humanitarian law. Schmitt (2017) emphasizes this issue, noting that the lack of clear regulations regarding LAWS could lead to a situation where "states may rely on autonomous systems for the use of lethal force without ensuring adequate legal oversight" (p. 195).

Marsili and Wróblewska-Jachna (2024) argue that "the digital revolution, driven by AI, presents both opportunities and risks, requiring new approaches to governance and regulation that address both technological advancements and their implications for human rights and social stability" (p. 22). This dual nature of AI necessitates a regulatory approach that balances innovation with the protection of democratic values and individual rights.

Various international bodies and treaties have attempted to address the governance of emerging technologies, but progress has been slow, and gaps remain in terms of global consensus. The United Nations (UN) and the European Union (EU) have made some strides in developing regulatory frameworks, particularly in the areas of AI and drones, but these efforts are often fragmented and lack effective enforcement mechanisms.

For instance, the EU has adopted the *Artificial Intelligence Act*, which is one of the first comprehensive regulatory frameworks for AI. This regulation, which does not apply to military uses of AI, aims to ensure that AI is developed and used in ways that respect fundamental rights, promote transparency, and prevent discriminatory practices. However, as Müller (2023) notes, the EU's efforts "represent only a first step in the complex process of establishing global standards for AI governance" (para. 6). The challenge lies in harmonizing these regional efforts with global standards and ensuring that the regulations are applicable beyond national borders. While regional frameworks can be tailored to specific political and economic contexts, they often fail to address the global nature of technology and the transboundary implications of technological advancements.

Ethical considerations are increasingly shaped by jurisprudence on mass surveillance. As Nino (2022) notes, courts like the ECtHR and CJEU are redefining the privacy-security balance, rejecting bulk data retention (e.g., *La Quadrature du Net v. France*, 2020) while permitting targeted surveillance under strict proportionality tests. This shift challenges technologies like emotion recognition AI, which the EU AI Act restricts to medical contexts (European Union, 2024).

Müller (2023) emphasizes that AI governance must be rooted in ethical principles that promote transparency, fairness, and accountability. He proposes a framework that includes "clear guidelines for the ethical use of AI, ensuring that AI systems are not only technically secure but also morally acceptable" (para. 8). This includes addressing issues such as algorithmic transparency, the right to explainable AI, and the need for robust oversight to prevent discriminatory practices in automated decision-making.

Ethical considerations regarding emerging technologies are further complicated by their potential military applications. As Schmitt (2017) observes, the use of AI and autonomous systems in warfare raises questions about delegating life-and-death decisions to machines, potentially violating fundamental principles of IHL, such as distinction and proportionality (p. 202). This brings to the forefront the urgent need for updated regulatory frameworks that can address the specific challenges posed by military uses of emerging technologies while safeguarding humanitarian values.

Risks and Ethical Dilemmas of Lethal Autonomous Weapons Systems and Military AI

The introduction of lethal autonomous weapons systems and artificial intelligence in military applications is reshaping the landscape of modern warfare. These technologies promise to revolutionize conflict management, offering enhanced precision, faster decision-making, and reduced risks to human combatants. However, their deployment raises profound ethical, legal, and operational challenges. These challenges are not merely technical but also strike at the

core of international humanitarian law and the principles of accountability and ethical warfare (Crootof, 2015; Sparrow, 2007).

One of the most pressing issues associated with LAWS is the "accountability gap". Traditional military operations are governed by a clear chain of command, where responsibility for decisions can be traced to specific individuals. LAWS disrupt this paradigm by introducing systems capable of autonomous decision-making, often without human intervention. This raises critical questions: Who is responsible when an autonomous system makes a lethal decision that results in civilian casualties or violates IHL? Is accountability to be assigned to the operator, the programmer, the military commander, or the state itself (Asaro, 2012)?

The opacity of AI algorithms, often referred to as the "black-box" problem, exacerbates this issue. Unlike human decision-making, which can be scrutinized and questioned, the internal processes of machine-learning systems are often inscrutable. This lack of transparency hinders not only accountability but also public trust and legal scrutiny (Bhuta et al., 2016). For instance, autonomous drones used for targeted strikes may make decisions based on patterns and datasets not accessible to or understandable by human operators, raising concerns about the predictability and reliability of such systems.

LAWS must operate within the bounds of IHL, which requires adherence to the principles of proportionality, necessity, and distinction. These principles demand that military actions balance the use of force with the need to minimize harm to civilians and ensure that attacks are directed exclusively at legitimate military targets. However, LAWS lack the contextual understanding and moral reasoning required to make nuanced ethical decisions, particularly in complex and dynamic combat environments (Sparrow, 2007; Sharkey, 2019).

For example, consider an autonomous system deployed in an urban area, tasked with neutralizing a high-value target. The presence of civilians, non-combatants, and critical infrastructure creates an intricate ethical landscape that challenges even the most experienced human commanders. An LAWS, operating based on preprogrammed algorithms or real-time data analysis, may fail to accurately assess the proportionality of its actions, leading to unintended harm and violations of IHL.

Furthermore, the absence of human empathy and intuition in LAWS decision-making processes raises moral concerns. While humans can weigh the emotional and ethical dimensions of warfare, machines are inherently amoral and operate solely based on programmed parameters, which may not account for all contingencies (Crootof, 2015).

LAWS have the potential to alter the dynamics of conflict escalation. Their ability to operate at speeds far beyond human capacity introduces risks of rapid escalation, particularly in scenarios involving miscommunication or miscalculation. For instance, an autonomous system might misinterpret a benign action by an adversary as a hostile act, triggering a disproportionate response and escalating tensions into full-scale conflict (Horowitz, 2019).

In addition, the proliferation of LAWS raises concerns about their misuse by state and non-state actors. Terrorist organizations or rogue states could exploit these technologies to carry out precision strikes, sabotage critical infrastructure, or disrupt international stability. The dual-use nature of many AI technologies further complicates regulatory efforts, as civilian AI applications can often be repurposed for military use (Singer, 2009).

The legal frameworks governing LAWS are currently inadequate to address their unique challenges. While IHL provides a foundation for regulating the conduct of hostilities, its application to autonomous systems is fraught with ambiguity. For example, Article 36 of the Additional Protocol I to the *Geneva Conventions* requires states to ensure that new weapons comply with IHL, yet there is no consensus on how this applies to LAWS (Sassòli, 2014).

Efforts to establish international norms and treaties, such as the United Nations' *Convention on Certain Conventional Weapons* (CCW), have faced significant challenges due to differing national interests and strategic priorities. Some states advocate for a complete ban on autonomous weapons, citing ethical and humanitarian concerns, while others emphasize the strategic advantages and deterrent value of such systems (Heyns, 2016).

In addition, the rapid pace of technological innovation outstrips the capacity of legal frameworks to adapt. As LAWS become increasingly sophisticated, regulatory efforts must balance the need for innovation with the imperative to uphold ethical and legal standards in warfare (Bhuta et al., 2016).

To mitigate the risks associated with LAWS, many experts emphasize the importance of maintaining meaningful human control over autonomous systems. This entails ensuring that

humans retain the ability to supervise, intervene, and override the decisions of autonomous systems at critical junctures. Such measures not only enhance accountability but also reinforce compliance with IHL and ethical standards (Asaro, 2012).

For instance, hybrid models that combine autonomous capabilities with human oversight could allow for the advantages of LAWS while minimizing their risks. In this context, humans would serve as a final check on the actions of autonomous systems, ensuring that ethical and legal considerations are upheld.

The deployment of lethal autonomous weapons systems and military AI represents both an opportunity and a challenge for the future of warfare. While these technologies have the potential to revolutionize military operations, their ethical, legal, and operational implications demand careful consideration. By fostering international collaboration, developing robust legal frameworks, and ensuring meaningful human oversight, the risks associated with LAWS can be mitigated, paving the way for their responsible and ethical integration into military strategies.

The Role of International Cooperation in Managing Dual-Use Technologies

Emerging disruptive technologies, particularly those with dual-use capabilities, present complex challenges for international security, regulation, and governance. As technologies such as artificial intelligence, robotics, and biotechnology evolve rapidly, the potential for their use in both civilian and military contexts grows, complicating their management. The dual-use nature of these technologies requires a comprehensive international approach to governance, as technological developments often transcend national borders. The risks associated with these innovations cannot be effectively addressed by individual states alone. Therefore, international cooperation is crucial to ensure that these technologies contribute to global security while minimizing potential misuse.

One of the primary challenges in managing dual-use technologies is the lack of coherent international norms and standards. The rapid pace of technological advancement often outpaces the capacity of international bodies to regulate these developments effectively. As Marsili (2023) emphasizes, global governance frameworks are increasingly inadequate for addressing the challenges posed by EDTs, especially in military contexts (p. 121). The absence of comprehensive international agreements on dual-use technologies results in a fragmented regulatory environment, where some states may adopt stricter controls while others remain less stringent. This uneven regulatory landscape can create vulnerabilities, particularly when technologies are transferred between countries with differing levels of oversight.

To address these challenges, international cooperation is essential. The establishment of binding agreements, such as the Biological and Toxin Weapons Convention (BTWC) or the Wassenaar Arrangement, showcases the potential for global cooperation in regulating specific dual-use technologies. However, as technologies continue to advance, these agreements must be updated and adapted to remain relevant. For instance, AI and autonomous systems are not sufficiently addressed by existing arms control treaties, highlighting the need for new international frameworks tailored to these emerging technologies.

Collaboration among international organizations—such as the UN, NATO, and the EU—is vital for creating consistent standards for the development, transfer, and use of dual-use technologies. These organizations are instrumental in facilitating dialogue among member states, creating legally binding agreements, and promoting transparency and accountability in the development and deployment of EDTs.

Transparency and information-sharing are crucial components of international cooperation on dual-use technologies. Effective regulation relies on the timely exchange of information regarding the development and deployment of emerging technologies. However, the secretive nature of military research and the competitive advantage provided by technological superiority often hinder the flow of information between states and international organizations. Consequently, the risk of both unintentional and intentional misuse of dual-use technologies increases.

Efforts to promote transparency, such as implementing confidence-building measures and establishing international technology monitoring mechanisms, can help mitigate these risks. For example, the EU's European Defence Fund (EDF) encourages cooperation in military technology research and development, while ensuring alignment with ethical guidelines and

international security standards. Similar initiatives at the international level can help ensure responsible sharing of advancements in dual-use technologies, providing states with access to the information necessary to prevent misuse.

International agreements, such as the 1975 International Traffic in Arms Regulations (ITAR), which govern the flow of sensitive technologies, offer guidelines for managing the exchange of research data and technological innovations. When properly enforced, these agreements can help prevent the proliferation of advanced technologies to non-state actors or states with weak regulatory frameworks that may exploit them for destabilizing purposes.

Private sector involvement is also crucial for the effective regulation and management of dual-use technologies. Many of the most significant innovations in AI, robotics, and biotechnology are driven by private companies, often with limited governmental oversight. As Marsili and Wróblewska-Jachna (2024) highlight, private sector actors, particularly in the technology and defense industries, play a key role in shaping the development and deployment of dual-use technologies (p. 122). Given the global nature of the markets these companies operate in, their actions have significant implications for international security.

For international cooperation to succeed, private companies must be integrated into the governance process. This involves creating partnerships between states, international organizations, and industry leaders to develop frameworks that ensure the responsible development and use of dual-use technologies. The private sector can also contribute by adopting self-regulatory mechanisms, such as ethical guidelines and codes of conduct, aligned with international standards.

Public-private partnerships can play a critical role in advancing research while ensuring that ethical considerations are integrated into technological development. By collaborating, the public and private sectors can bridge the gap between innovation and regulation, fostering technological growth that prioritizes security and ethical standards.

Despite the clear need for international cooperation, several challenges hinder effective collaboration in managing dual-use technologies. First, differences in national priorities and political systems complicate efforts to establish unified regulations. For example, states with more aggressive military agendas may prioritize the development of cutting-edge technologies with little regard for international norms, while others may take a more cautious approach. This disparity in national security interests can create tensions and undermine efforts to develop global frameworks.

Second, the rapid pace of technological change presents a significant challenge for international cooperation. While international treaties and agreements typically evolve slowly, emerging technologies develop at an unprecedented rate, making it difficult for policymakers to keep up. As a result, states and international organizations often find themselves reacting to technological developments rather than proactively addressing them. This reactive approach can lead to regulatory gaps that allow the unchecked proliferation of dual-use technologies.

Finally, enforcement remains a significant obstacle to international cooperation. Even when international agreements are reached, there is no guarantee that all parties will adhere to the terms. States may be reluctant to enforce regulations that conflict with their national interests, and the lack of a global regulatory body with enforcement powers complicates the implementation of international agreements.

The role of international cooperation in managing dual-use technologies is more critical than ever as the global landscape continues to evolve. As technologies like AI, robotics, and biotechnology become more pervasive, the need for comprehensive, coordinated regulation is paramount. By fostering greater transparency, encouraging private sector involvement, and strengthening international norms and standards, the global community can work together to mitigate the risks associated with these technologies while promoting their responsible development. The challenges to international cooperation are substantial, but with concerted effort and collaboration, a global framework for managing dual-use technologies can be established to ensure security, ethics, and stability in an increasingly interconnected world.

Technological Risks and Ethical Considerations

Emerging disruptive technologies, such as artificial intelligence, robotics, cyber capabilities, and biotechnology, are rapidly transforming both military operations and civilian infrastructures. These technologies carry significant dual-use potential, which means they can be applied in both beneficial and potentially harmful ways across various sectors. While EDTs

promise advancements in security and operational efficiency, they also pose considerable ethical, legal, and political challenges, particularly in the realm of warfare and global security. The dual-use nature of these technologies introduces risks to human rights, accountability, and international law, and it is crucial to regulate their development and deployment responsibly. This section explores the key ethical issues related to the use of these technologies and proposes frameworks for addressing their potential risks.

A central ethical challenge of integrating autonomous systems into military operations is determining accountability. Lethal autonomous weapons systems, capable of making decisions regarding the selection and engagement of targets without direct human oversight, have raised significant concerns. Although LAWS could enhance operational efficiency and reduce human casualties in some scenarios, they present challenges in terms of moral and legal responsibility.

One of the main dilemmas is who should be held accountable if an autonomous system commits an act that violates international humanitarian law, such as targeting civilians or committing war crimes. The increasing autonomy of these systems creates a legal gray area, as it becomes harder to attribute responsibility for decisions made by machines. Many experts suggest that meaningful human oversight should be maintained in the use of such systems to ensure compliance with ethical standards and legal frameworks (Müller, 2023). At the same time, the complexity and opacity of AI decision-making processes—often characterized by "black box" models—raise further concerns about the transparency and traceability of autonomous actions (O'Neil, 2016).

AI's role in warfare introduces various ethical concerns, particularly regarding the risk of biased decision-making and the potential for exacerbating inequalities. Military AI systems, including those used for target recognition or threat analysis, rely heavily on data. If the data used to train these systems is biased or incomplete, the algorithms can perpetuate systemic inequalities or even discriminate against specific groups. For example, predictive algorithms might disproportionately target certain ethnic or social groups, further entrenching existing societal biases (O'Neil, 2016).

Another major concern is the potential misuse of AI in disinformation campaigns or cyberattacks. AI-driven technologies such as deepfakes can manipulate public perception by creating fake images or videos that appear convincingly real. Such technologies have the potential to disrupt democratic processes, undermine political stability, and escalate conflicts. Given their widespread availability and ease of use, these tools pose a serious threat to both the integrity of information and to global security (Müller, 2023). As AI continues to develop, the ethical implications of its use in military and informational contexts must be carefully regulated to prevent harm and misuse.

The integration of AI into surveillance technologies also raises profound ethical concerns about privacy and civil liberties. As AI enables the widespread monitoring of individuals, both in military and civilian contexts, concerns about data privacy have escalated. Technologies like facial recognition, drones, and data mining can be employed to track individuals and gather vast amounts of personal data. While these systems can enhance national security, they also open the door for intrusive surveillance practices that infringe on citizens' rights to privacy and freedom of expression.

In authoritarian regimes, such surveillance systems are particularly dangerous, as they can be used to monitor, suppress, or persecute political dissidents and marginalized groups. The unchecked use of AI in surveillance without adequate safeguards can result in a major erosion of human rights and democratic freedoms. Ensuring that these technologies are employed in ways that respect privacy and civil rights, particularly in the context of military or counterterrorism operations, is paramount (Müller, 2023).

A growing concern in the age of emerging technologies is the increasing divide between countries that possess advanced technologies and those that do not. The disparity in technological capabilities exacerbates global inequality and could lead to geopolitical instability. For example, nations with access to cutting-edge AI and autonomous systems gain strategic advantages in warfare and security, while others may struggle to protect themselves or leverage similar technologies for economic development.

This technological divide could lead to new forms of power imbalance, with technologically superior countries having the ability to exert dominance over weaker states. Furthermore, the lack of access to disruptive technologies can impede the social and economic progress of

underdeveloped regions. To ensure a more equitable distribution of technological benefits, it is essential for international policies to promote collaboration and responsible sharing of these innovations, preventing their monopolization by a few powerful states (Müller, 2023).

To address the ethical risks associated with disruptive technologies, a robust framework for international cooperation and regulation is necessary. Existing international law is often ill-equipped to handle the rapid development of AI, robotics, and related technologies. This regulatory gap can leave room for exploitation and misuse, particularly in military and surveillance contexts. Therefore, nations must collaborate to create policies that promote the ethical development and deployment of these technologies while ensuring compliance with human rights standards.

International discussions on the regulation of lethal autonomous weapons systems and AI have already begun, but these efforts need to be expanded to cover all aspects of EDTs. Müller (2023) argues that such regulations must be multifaceted, addressing issues of accountability, transparency, and fairness. The ongoing development of AI in military applications underscores the need for international agreements to ensure that these technologies are used responsibly and ethically, with strict oversight to prevent harmful consequences.

Emerging disruptive technologies offer significant potential for improving military and security operations but also introduce substantial ethical, legal, and human rights challenges. Issues such as accountability, bias, privacy violations, and geopolitical instability must be addressed through rigorous international cooperation and regulation. As these technologies continue to evolve, their use in military and civilian contexts must be carefully monitored to ensure that their deployment serves the greater good without compromising ethical standards or international law.

Conclusion and Future Directions

As emerging disruptive technologies continue to reshape the landscape of military and civilian domains, their dual-use nature presents complex challenges, both ethical and security-related. The potential for these technologies to revolutionize industries and societies is undeniable, but so too is their capacity to be misused or cause unintended harm. Navigating these challenges requires an integrated approach that encompasses regulatory frameworks, international cooperation, technological governance, and ethical considerations.

Equally important is the establishment of regulatory frameworks that can guide the development and use of these technologies, ensuring that their benefits are maximized while minimizing their risks. This requires international cooperation and dialogue to create common standards and norms that transcend national borders. As emerging technologies increasingly operate in a globalized world, ensuring that they are used ethically and responsibly demands collective action and commitment to shared values.

While progress in regulating dual-use technologies has been made, much remains to be done. Technological advancements continue to outpace the development of regulatory frameworks, leaving gaps in governance that may expose vulnerable sectors to security risks. In particular, emerging fields like artificial intelligence, quantum computing, and biotechnology require robust international cooperation to establish effective oversight mechanisms. There is a need for adaptive regulatory structures that can keep pace with technological change while ensuring that ethical considerations are integrated into decision-making processes.

Future research should focus on the development of frameworks that balance innovation with ethical responsibility, providing clear guidelines for the responsible use of dual-use technologies. This includes not only creating more comprehensive laws and regulations but also fostering a global culture of accountability in technological development. The participation of diverse stakeholders, including ethicists, policymakers, technologists, and the public, will be essential to address the complex challenges posed by these technologies.

Furthermore, it is essential to prioritize the protection of human rights and security in the face of technological disruptions. As AI and other EDTs become more embedded in critical infrastructure, governance, and military operations, the potential for misuse—whether intentional or unintentional—will grow. To mitigate these risks, ongoing research into the ethical implications of these technologies, their potential impacts on social justice, and their capacity to undermine democracy and global stability will be vital.

The governance of dual-use technologies hinges on resolving a fundamental tension: whether

to prioritize regulatory frameworks or technological deterrence. Historical precedents, such as the Papal Bull against crossbows—which failed due to its unenforceability—and Cold War-era arms control treaties exploited by the USSR to offset U.S. superiority, caution against relying solely on normative approaches. Conversely, unregulated innovation risks normalizing abuses like mass surveillance, as seen in China's social credit system. A balanced path forward must integrate three pillars:

1. Dynamic regulation: Establish agile institutions like the European AI Office (proposed under Article 56 of the EU AI Act) to update standards in real time, addressing gaps in areas like quantum computing and autonomous weapons.
2. Ethical audits: mandate third-party assessments for dual-use AI developers, akin to GDPR's Data Protection Impact Assessments, to ensure compliance with human rights (Nino, 2022).
3. Global collaboration: expand the *Political Declaration on Responsible Military Use of AI and Autonomy*, signed by 52 states, into a binding treaty under UN auspices.

Critics argue that deterrence via technological superiority—such as the U.S. National Security Strategy's focus on outpacing China in AI—offers more immediate security. However, as the ECtHR affirmed in *Big Brother Watch v. UK*, unchecked technological power erodes democracy. The EU's "risk-based" model outilined in the AI Actdemonstrates that innovation and rights can coexist, but only if states prioritize accountability over short-term strategic gains.

References

- ASARO P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, *94*(886), 687–709.
- BHUTA N., BECK S., GEIß R., LIU H.-Y., KREß C. (Eds. 2016). *Autonomous Weapons Systems: Law, Ethics, Policy*. Cambridge University Press. https://doi.org/10.1017/CBO9781316597873.
- CROOTOF R. (2015). The Killer Robots Are Here: Legal and Policy Implications. *Cardozo Law Review, 36*(5), 1837–1915. https://ssrn.com/abstract=2534567.
- EUROPEAN COURT OF THE HUMAN RIGHTS (ECtHR). (2018). *Big Brother Watch and Others v. the United Kingdom* (Application no. 58170/13). https://hudoc.echr.coe.int/eng?i=001-140713.
- FLORIDI L., & TADDEO M. (2014). *The Ethics of Information Warfare*. Springer. https://doi.org/10.1007/978-3-319-04135-3.
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. (2021). *Provvedimento n. 127 del 25 marzo 2021: parere sul sistema Sari Real Time [9575877]*. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877.
- GETTINGER D. (2019). *The Drone Databook*. Center for the Study of the Drone at Bard College. https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf
- HEYNS C. (2016). Autonomous weapons in armed conflict and the right to a dignified life: an African perspective. *South African Journal on Human Rights*, *32*(1), 46–71. https://doi.org/10.1080/02587203.2017.1303903.
- HOROWITZ M.C. (2019). The Ethics and Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons. *Daedalus*, *145*(4), 25–36. https://doi.org/10.1162/DAED_a_00409.
- INNOCENT II. (1139). Canones Concilii Lateranensis II [Decrees of the Second Lateran Council]. In Mansi J. D. (ed.), *Sacrorum Conciliorum Nova et Amplissima Collectio* (Vol. 21, col. 526–527).
- KEEN M. (1999). Medieval Warfare: A History. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198206392.001.0001.
- MARSILI M. (2022). Hybrid warfare: Above or below the threshold of armed conflict? *Honvédségi Szemle - Hungarian Defence Review*, *150*(1-2), 36–48.
- MARSILI M. (2023). Military Emerging Disruptive Technologies: Compliance with International Law and Ethical Standards. In I. Kalpokas & J. Kalpokienė (Eds.), *Intelligent*

and autonomous: Transforming values in the face of technology (pp. 112–134). Cham: Springer. https://doi.org/10.1163/9789004547261_004
- MARSILI M. (2024). Lethal Autonomous Weapon Systems: Ethical Dilemmas and Legal Compliance in the Era of Military Disruptive Technologies. *International Journal of Robotics and Automation Technology*, 11 (May 2024), 63–68. https://doi.org/10.31875/2409-9694.2024.11.05.
- MARSILI M. - WRÓBLEWSKA-JACHNA J. (2024). Digital Revolution and Artificial Intelligence as Challenges for Today/Rewolucja cyfrowa i sztuczna inteligencja jako wyzwania współczesności. *Media i Społeczeństwo*, *20*(1/ Zeszyt 1), 19-30. https://doi.org/10.5604/01.3001.0054.6506.
- MÜLLER V.C. (2023). Ethics of Artificial Intelligence and Robotics. *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). https://plato.stanford.edu/archives/fall2023/entries/ethics-ai/.
- NINO M. (2022). The normalization of mass surveillance in the jurisprudence of the Strasbourg and Luxembourg Courts. *Freedom, Security, Justice: European Legal Studies*, 3, 105–133. https://doi.org/10.1234/fsj.2022.0007.
- O'NEIL C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, NY: Crown Publishing Group.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (*Artificial Intelligence Act*) and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act)*, PE/24/2024/REV/1, *OJ L, 2024/1689, 12.7.2024,* ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
- SASSÒLI M. (2014). Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified. *International Law Studies*, 90, 308–340.
- SCHMITT M.N. (2017). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Pperations*. Cambridge University Press.
- SHARKEY N. (2019). Autonomous weapons systems, killer robots and human dignity. *Ethics and Information Technology*, *21*(2), 75–87. https://doi.org/10.1007/s10676-018-9494-0.
- SINGER P.W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York, NY: Penguin Press.
- SPARROW R. (2007). Killer Robots. *Journal of Applied Philosophy*, *24*(1), 62–77. https://doi.org/10.1111/j.1468-5930.2007.00346.x.
- TIGARD D.W. (2021). Responsible AI and moral responsibility: A common appreciation. *AI Ethics*, 1, 113–117. https://doi.org/10.1007/s43681-020-00009-0.
- U.S. Department of State. (2023). *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, adopted on 9 November 2023. https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/.
- WHITE HOUSE. (2022, 4 May). *National Security Memorandum on Quantum Computing*. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

GIACINTO D'URSO

Ufficiale in servizio presso la Direzione Alta Formazione e Ricerca del CASD. Ha conseguito la Laurea Magistrale in Scienze Politiche, in Scienze Diplomatiche e Internazionali, in Giurisprudenza, in Scienze Strategiche e in Psicologia. È abilitato all'esercizio della professione di psicologo

GIORGIO GIOSAFATTO

U t.ISSMI(E) dell'Esercito Italiano. Dottore in Scienze Economiche ed in Scienze Strategiche e Politico Organizzative. Ha conseguito il Master of Military Art and Science ed il Master of Arts in Military Operation presso il Command and General Staff College (CGSC) dell'US Army

COMANDARE UN'OPERAZIONE MILITARE NELL'EPOCA DELL'INTELLIGENZA ARTIFICIALE. IL RUOLO STRATEGICO DELLA FORMAZIONE PER AFFRONTARE IL DOMINIO SPAZIALE E ALTRI AMBIENTI OPERATIVI COMPLESSI.

ABSTRACT

Lo spazio extra-atmosferico è un ambiente altamente congestionato, conteso e competitivo nel quale molti paesi hanno avviato programmi militari per salvaguardare gli interessi nazionali. Condurre operazioni spaziali militari in un dominio caratterizzato da fluidità, incertezza, ambiguità e da un overflow di dati ed informazioni è molto complesso, anche a causa della narrativa che accompagna la progressiva introduzione dell'intelligenza artificiale (IA) nel settore della Difesa. In tale quadro, preservare la capacità del personale di adattarsi e di assumere decisioni, anche di natura innovativa, per affrontare situazioni mutevoli ed impreviste è da considerare un fattore di successo. Al riguardo, la percezione di autoefficacia, l'intolleranza all'incertezza e all'ambiguità possono assumere un'incidenza importante e sono state, pertanto, ritenute meritevoli di un approfondimento.

Per quanto noto, questo studio rappresenta una delle prime iniziative volte ad osservare un campione di frequentatori di un corso di alta formazione in un Istituto universitario militare italiano (nello specifico il 27° corso ISSMI presso il Centro Alti Studi della Difesa / Scuola Superiore Universitaria) per conoscere la ricorrenza di eventuali fattori di vulnerabilità allo stress, come viene percepita l'introduzione di sistemi intelligenti in ambito civile e militare, in che misura si ritiene di poter svolgere con efficacia il proprio ruolo in un contesto operativo caratterizzato da fluidità, complessità, incertezza, ambiguità e progressiva introduzione di tecnologie/prodotti che utilizzeranno l'IA per funzionare e l'esistenza di un bisogno formativo.

È stato, pertanto, predisposto un questionario con l'ausilio del programma Microsoft Forms che è stato somministrato in presenza il 9 ottobre 2024. I 169 partecipanti hanno potuto aderire all'iniziativa su base volontaria e rispondere al questionario online in modo del tutto anonimo con le apparecchiature informatiche disponibili.

L'analisi statistica è stata condotta per fasi, utilizzando il linguaggio di programmazione Python, con l'ausilio delle librerie Pandas, Scipy, Pingouin e Statsmodels. È stata valutata la normalità delle distribuzioni delle variabili principali utilizzando il test di Shapiro-Wilk mentre la verifica delle ipotesi di ricerca è stata effettuata utilizzando l'analisi di correlazione di Spearman.

Al termine della disamina, è stata rilevata la ricorrenza di condizioni che possono accrescere

la vulnerabilità di un individuo agli effetti dello stress. Inoltre, è risultato che il campione ha un'opinione positiva nei confronti della diffusione dell'IA nella vita di tutti i giorni. L'impiego di questa tecnologia in ambito militare suscita interesse sebbene non sia stato ancora assunto un atteggiamento marcatamente positivo o negativo. Coloro che fanno preso parte alla rilevazione, hanno di massima una buona percezione di autoefficacia e ritengono di poter usare eventuali strumenti dotati di IA nell'ambito delle attività istituzionali a cui sono preposti con un livello capacitivo medio. È stato, conseguentemente, rilevato un bisogno formativo di cui è consigliabile tener conto nelle successive fasi di progettazione di analoghe tipologie di corso.

In conclusione, la formazione è stata identificata come un settore strategico per poter mantenere l'essere umano al centro del cambiamento e per poterlo correttamente "equipaggiare" con gli strumenti necessari ad affrontare con efficienza ed efficacia le sfide future. La possibilità di conoscere e saper utilizzare i nuovi sistemi gestiti dall'IA, di sperimentare stili decisionali flessibili e altamente adattabili, di mettere alla prova le proprie capacità nella gestione di situazioni incerte, ambigue, complesse e in rapido cambiamento sono degli step importanti nella crescita professionale di un comandante. La scelta di investire nella simulazione e sul potenziamento delle capacità creative e cognitive dell'individuo è raccomandabile, al fine di agevolare l'apprendimento e l'applicazione delle conoscenze acquisite nelle successive fasi di impiego operativo.

Parole chiave: Operazioni spaziali militari, Opinione Pubblica, Difesa, Formazione, intelligenza artificiale

ABSTRACT

Outer space is a highly congested, contested, competitive environment in which many countries have initiated military programs to protect national interests.

Conducting military space operations in a domain characterized by fluidity, uncertainty, ambiguity, and an overflow of data and information is also very complex due to the narrative accompanying the gradual introduction of artificial intelligence (AI) in the Defense. Within this framework, maintaining the ability of personnel to adapt and make decisions, including innovative ones, to deal with changing and unforeseen situations should be considered a success factor.

To the best of our knowledge, this study represents one of the first initiatives aimed at observing a sample of higher education course attendees at an Italian military university (specifically, the 27th ISSMI course at the Centre For Higher Defense Studies - School Of Advanced Defense Studies) to learn about the recurrence of any stress vulnerability factors, how they assess the introduction of intelligent systems in civilian and military environments, the extent to which they believe they can effectively perform their role in an operational environment characterized by fluidity, complexity, uncertainty, ambiguity, and the progressive introduction of technologies/products that will use AI to function, and the existence of a training need.

Statistical analysis was performed step by step with Python programming language using the Pandas, Scipy, Pingouin, and Statsmodels libraries. The Shapiro-Wilk test was used to assess the normality of the distributions of the main variables, while Spearman's correlation analysis was used to test the research hypotheses.

At the end of the study, the recurrence of conditions that can increase an individual's vulnerability to the effects of stress was noted. It was also found that the sample has a positive attitude towards using AI in everyday life. There is interest in using this technology in the military, although there is no evident positive or negative attitude. The participants in the survey have a good perception of self-efficacy and believe that they can use any AI-equipped tool in the context of the institutional activities to which they are assigned with an average

level of capacity. Consequently, a training need has been identified that should be considered in the next stages of designing similar courses.

In conclusion, training has been identified as a strategic area to keep people at the center of change and to equip them with the necessary tools to face future challenges efficiently and effectively. The opportunity to learn about and use new AI-driven systems, to experiment with flexible and highly adaptive decision-making styles, and to test one's ability to deal with uncertain, ambiguous, complex, and rapidly changing situations are essential steps in a commander's professional development. The decision to invest in simulation and cognitive enhancement of the individual is recommended to facilitate learning and application of acquired knowledge in subsequent phases of operational deployment.

Key words: Military space operations, Public Opinion, Defense, Training, artificial intelligence

ABSTRACT

1. Introduzione

Lo spazio extra-atmosferico è un ambiente altamente congestionato, conteso e competitivo (Martinez, 2019; Yuan et Jiang, 2023) ove attori pubblici e privati concorrono per accrescere la loro influenza geopolitica e per beneficiare dei vantaggi offerti dalla *space economy*. La proiezione di interessi nazionali nell'orbita terrestre e la crescente dipendenza dai servizi spaziali (ad esempio le comunicazioni satellitari, l'accesso a internet, la navigazione e la geolocalizzazione, ecc.) hanno richiesto a molti paesi di avviare programmi militari nell'orbita terrestre e di dotarsi di uno strumento in grado di impiegare assetti spaziali di protezione/dissuasione con l'obiettivo di contrastare/scoraggiare eventuali azioni ostili da parte dei competitors internazionali.

Condurre operazioni spaziali militari è molto complesso. Esse consistono in un insieme di attività tecnico scientifiche i cui effetti sono visibili a migliaia di chilometri dall'operatore (ad esempio variare il posizionamento di un satellite), risentono di molteplici variabili (ambiente, tempistiche, leggi fisiche ecc.) e hanno bisogno di dati credibili oltre che di precisione di intervento. Inoltre, la carenza di sensori che permettano di sviluppare un quadro affidabile della situazione operativa è fonte di incertezza e ambiguità nella valutazione delle informazioni disponibili, contribuisce alla ricorrenza del fenomeno dei "falsi allarme" (ad esempio l'attivazione per una potenziale minaccia di collisione che poi non determina la necessità di una manovra di evitamento) e aumenta il rischio che si possano verificare imprevisti. La prevenzione e la gestione di tali eventi richiedono un continuo monitoraggio coniugato ad una elevata prontezza operativa e reattività decisionale.

La futura implementazione dell'IA nel processo decisionale di pianificazione militare permetterà di integrare la struttura organizzativa degli staff, di migliorare la qualità dell'analisi di grandi quantità di dati, di potenziare la capacità predittiva dei sistemi di comando e controllo, rendendo la risoluzione dei problemi operativi più rapida ed efficace (Sanchez et al, 2020). L'uso dell'IA in ambito militare è, tuttavia, fonte di grande incertezza e solleva diverse questioni di natura etico-giuridiche (Sebo et Long, 2023; Gaeta, 2023), soprattutto per quanto riguarda il livello di autonomia di cui dotare i nuovi sistemi intelligenti e il bilanciamento nell'interazione essere umano - macchina. In tal senso, una recente indagine condotta su un campione della popolazione italiana di 524 persone ha posto in evidenza che il ricorso a sistemi di IA in ambito militare suscita interesse ma è anche fonte di preoccupazione che ha indotto una netta maggioranza dei partecipanti a preferire che venga mantenuto il controllo umano di queste emergenti tecnologie (D'Urso, 2024).

L'ambiguità e la complessità che caratterizzano le operazioni spaziali militari, nonché l'incertezza e la narrativa che accompagna l'utilizzo dell'IA nel settore della Difesa possono causare stanchezza ed essere un serio fattore di stress che, perdurando nel tempo, deteriora la resilienza del personale (Luthar et al, 2003; Casula, 2011) e logora il suo benessere biopsicosociale. Ciò rende più difficile reagire ad un imprevisto, aumenta la tendenza ad avallare una soluzione elaborata artificialmente (a prescindere dalla sua correttezza) e più

probabile il rischio di un insuccesso.
La resilienza è una competenza essenziale per il personale militare. Essere in grado di resistere e superare le difficoltà è, in effetti, un fattore di crescita dell'autostima che motiva l'individuo a continuare a svolgere bene il proprio lavoro. Allo stesso tempo, il fallimento aumenta la vulnerabilità del personale esponendolo a problemi psicofisici che possono limitarne significativamente la qualità della vita e della prestazione lavorativa (Nindl et al 2018). In queste situazioni, infatti, è ricorrente il mantenimento di uno stato di allerta e di allarme, la manifestazione di preoccupazione e paura che poi possono evolvere in condizioni di ansia e depressione (Guidi et al, 2020).
La combinazione di diversi fattori di stress, ivi inclusi il mantenimento di uno stile di vita non sano (una cattiva alimentazione, la carenza di sonno, una limitata attività fisica, ecc.) e la percezione di non essere pronto a far fronte ad una specifica prestazione o alla gestione di un evento, sono un'ulteriore causa di alterazione fisiologica da cui possono derivare malfunzionamenti che rendono più difficile l'identificazione di un problema, la gestione di un imprevisto e l'assunzione di una decisione. In una condizione di pericolo, infatti, tutte le risorse disponibili vengono impiegate per potenziare le reti e gli apparati cerebrali preposti a garantire la sopravvivenza, a scapito dei neurocircuiti che si occupano delle attività cognitive di ordine superiore (Vartanian et al, 2020). Inoltre, la continua esposizione a situazioni stressanti può incidere sul metabolismo del triptofano, che contribuisce alla produzione della serotonina (ormone che contribuisce alla regolazione del sonno, dell'appetito e delle emozioni) e dei derivati dalla chinurenina. Il perdurare di una risposta fisiologica a stimoli giudicati pericolosi può indurre uno stato infiammatorio che determina "uno spostamento" verso la "via della chinurenina", limitando la produzione di serotonina (Marazziti et al, 2013). La maggiore prevalenza dell'acido chinolinico, un metabolita neurotossico della chinurenina (Meier et al, 2018), può inibire la sintesi del fattore neurotrofico derivato dal cervello che riveste un ruolo molto importante nei processi di neurogenesi e di sinaptogenesi, determinando anomalie funzionali e strutturali nelle aree del cervello direttamente coinvolte, ad esempio, nella regolazione dell'umore (Marx et al, 2020), nell'immagazzinamento di tracce di memoria (Hasan et al, 2019), nella definizione degli stati di allertamento o di cessazione delle situazioni di pericolo (VanElzakker et al, 2018; Egan et al, 2024), nelle funzioni cognitive ed esecutive (Alvarez et Emory, 2006; Pocivavsek et al, 2017) oltre che nei network che contribuiscono al processo decisionale e alla risoluzione di problematiche che richiedono una soluzione creativa (Beaty et al, 2017; Bendetowicz et al, 2018).
In un ambiente operativo caratterizzato da complessità, fluidità e crescente innovazione digitale appare, quindi, assolutamente necessario preservare la capacità del personale di assumere decisioni, anche di natura innovativa, per affrontare situazioni impreviste, incerte e ambigue. In tale quadro, la percezione di autoefficacia, l'intolleranza all'incertezza e all'ambiguità possono assumere un ruolo importante e meritevole di un approfondimento.

2. Background teorico

2.1. Autoefficacia

L'autoefficacia riguarda l'insieme delle convinzioni che una persona possiede circa le proprie capacità di agire attivamente in un ambiente, compiendo le azioni necessarie ad assolvere un compito con una performance di livello soddisfacente. La convinzione di poter essere "all'altezza della situazione" consente di sostenere la motivazione, di alimentare l'impegno con cui si affrontano nuove sfide e di ridurre l'impatto che lo stress ha sul benessere psicosociale dell'individuo (Bandura, 1977; Bandura, 1997; Amiri et al., 2019; Barbara et al, 2021; Liu et al 2024).
Nel corso di un imprevisto, l'essere umano può trovarsi nelle condizioni di non poter sempre prevedere gli ostacoli da superare e di non essere certo degli obiettivi o delle tempistiche entro cui vanno conseguiti, delle risorse e dell'impegno richiesti, delle modalità di coordinamento attraverso cui ricevere eventuali feedback sulla qualità delle prestazioni e poter conseguentemente adottare i correttivi eventualmente ritenuti necessari (Bandura et Cervone, 1983). In una simile contingenza, la regolazione cognitiva dell'azione e della motivazione possono risultare compromesse da forme di pregiudizi che contribuiscono a far emergere nell'individuo una maggiore o minore fiducia in sé stesso e

la convinzione di avere o meno tutte le risorse necessarie (conoscenze, competenze e abilità) per svolgere le proprie mansioni e risolvere le problematiche ad esse correlate. L'idea di non essere in grado di svolgere una specifica attività sostiene il convincimento che sia possibile un insuccesso, riduce le *chance* di poter adeguare l'impegno ed il comportamento al senso di autoefficacia e aumenta il rischio che siano commessi errori o assunte decisioni sbagliate a causa di forme eccessive di sicurezza, di maggiore cautela (Cervone, 1989) e/o di inerzia. In tale quadro, Cook et al (2013) ritengono che l'organizzazione possa svolgere un ruolo determinante per instaurare un virtuoso processo di scambio sociale attraverso cui sostenere l'autoefficacia e la qualità delle prestazioni dei lavoratori. Nello specifico, quando le organizzazioni forniscono supporto in termini di risorse (formazione, strumentazione, equipaggiamento, ecc), informazioni e opportunità di crescita professionale, instaurano un sentimento di soddisfazione che solitamente induce i dipendenti a sentirsi in obbligo e a ricambiare con un maggior impegno professionale.

2.2. Intolleranza all'incertezza e all'ambiguità

L'intolleranza all'incertezza è la tendenza di un individuo a ritenere insostenibile l'idea che, a causa della carenza di un adeguato set informativo e dell'incapacità di attuare misure risolutive o di prevenzione ritenute efficaci (Bottesi et al, 2019; Bahadir et Dundar, 2024), possa verificarsi in futuro un imprevisto o un evento infausto (Carleton, et al 2007; Carleton et al 2016 (a); Carleton et al 2016 (b); Lauriola et al, 2016). Lo stato di insofferenza causato da una irrisolta condizione di intolleranza all'incertezza ha un impatto negativo sul benessere psicofisico dell'individuo che tende progressivamente ad aggravarsi (El Khoury-Malhame, et al, 2024), determinando la manifestazione di comportamenti disadattivi come ad esempio forme di evitamento e fuga da situazioni potenzialmente incerte (Pawluk et Koerner, 2013) oltre che uno stile decisionale irrazionale, impulsivo (Bottesi et al, 2019; Páez Gallego et al, 2020; Danışman et İspir, 2024) o rischioso (Jensen et al, 2014).

L'intolleranza all'ambiguità è, invece, la propensione di una persona a percepire situazioni non ben definite o caratterizzate da novità, complessità e insolubilità come una potenziale fonte di minaccia (Iannello et al, 2017; Petrocchi et al, 2021). Interagire con un evento giudicato ambiguo determina un'esperienza di disagio emotivo (Pierro et al, 1995) a causa della preoccupazione di non riuscire a mantenerne il controllo (Endler et al., 2000), a prevedere le difficoltà da superare ed il livello della prestazione necessaria a far fronte ai compiti richiesti. Ciò determina reazioni cognitive e comportamentali caratterizzate rispettivamente da rigidità e dalla tendenza a non accettare alcuna forma di rischio.

L'intolleranza all'ambiguità e all'incertezza sono entrambe delle forme di vulnerabilità dell'individuo caratterizzate dalla tendenza ad esaminare l'ambiente circostante, a sovrastimare la possibilità di essere esposto ad un rischio e a rispondere agli stimoli giudicati minacciosi con una serie di reazioni cognitive, emotive e comportamentali volte all'autoprotezione (Grenier et al, 2005). Tale modalità comportamentale rievoca, ad esempio, la continua ricerca di informazioni tipica dell'infodemia (propagazione di una quantità eccessiva di notizie di cui non è possibile rintracciare e vagliare con accuratezza la fonte) e della cybercondria (termine coniato per descrivere l'ansia e la paura causata dalla ricerca di informazioni sanitarie online) che hanno caratterizzato la pandemia di COVID 19 (McKinnon et al, 2020, Zakar et al, 2021, World Health Organization, 2022). Inoltre, queste tipologie di fragilità si associano, spesso, ad un una condizione di stress (Sowan et Baziliansky, 2024; Ghorbanalipour et al, 2024), ulteriormente aggravata dalla limitata percezione di autoefficacia (Endres et al, 2009; Iannello et al, 2017; Kagan, 2021; Kestler-Peleg et al, 2023).

Il fattore che concorre a diversificare queste forme di fragilità è il tempo in cui viene collocata la minaccia. Infatti, gli individui intolleranti all'ambiguità non sono in grado di sopportare una situazione ambigua che si verifichi "qui e ora" mentre quelli intolleranti all'incertezza considerano inaccettabile che un evento futuro possa verificarsi con esiti negativi, indipendentemente dalla probabilità che esso accada (Dugas et al, 2001).

3. La ricerca in ambito militare

I numerosi studi condotti sull'applicazione dell'autoefficacia in un contesto militare ne hanno

ampiamente dimostrato l'importanza per la definizione di strategie di coping che consentano di rafforzare la resilienza dei soldati sottoposti a forti stress e traumi durante il loro impiego operativo (Koning-Eikenhout et al, 2024; Schwarzer, 2024). È, infatti, utile evidenziare che è proprio la percezione di essere incapaci di affrontare una situazione difficile e potenzialmente rischiosa ad incidere sulla qualità della performance, sulla capacità di adattamento ad un nuovo contesto e complessivamente sul benessere individuale (Kokun, 2024). L'autoefficacia ha, inoltre, un ruolo centrale anche nei contesti formativi. Al riguardo, Kanapeckaitė et al (2022) hanno rilevato che essa svolge un ruolo di mediazione tra il livello di resilienza del personale militare e la percezione della qualità dei risultati da loro conseguiti, aumentandone la prontezza operativa. Infatti, la convinzione di essere capaci di organizzare e di intraprendere una linea d'azione per raggiungere specifici obiettivi risulta determinante per rendere un soldato motivato ad aumentare la propria competenza professionale (Buch et al, 2015) nel corso della carriera (*lifelong learning*) ed essere sempre pronto all'impiego (Johnsen et al, 2017). Infine, Gasaway (2024) ritiene che l'autoefficacia sia uno degli ingredienti essenziali per poter decidere in ambienti caratterizzati da forte stress, alto rischio, tempi compressi e condizioni in rapido cambiamento. In questa tipologia di scenario, l'autoefficacia attribuisce al decisore/comandante maggiore contezza della qualità delle conoscenze e competenze possedute e la ragionevole certezza di poterle impiegare correttamente, al fine di mantenere il controllo dell'ambiente in cui opera. Un comandante sprovvisto di questa peculiare caratteristica potrebbe risultare sopraffatto dai dubbi e probabilmente ritardare l'assunzione di decisioni critiche, determinando la diffusione di incertezza nel suo staff e, conseguentemente, un calo dell'efficienza.

L'impatto dell'intolleranza all'incertezza e all'ambiguità sullo stato di salute del personale militare e sulla qualità del processo decisionale in contesti critici ha incominciato ad essere da poco tempo oggetto di interesse. Bardeen et al. (2017) hanno rilevato che l'intolleranza all'incertezza è l'unica condizione che consente di formulare una previsione su come una persona interpreta un evento come stressante. Satici et al (2020) e Paluszek et al (2021) hanno osservato una correlazione inversa fra il livello di incertezza/ambiguità e la capacità di resilienza mentre Hmilar et Cherevychnyi (2020), monitorando un campione di 85 ufficiali-tirocinanti Ucraini, hanno constatato che l'incertezza, causata principalmente dalla complessità della situazione geopolitica, ingenerava uno stato emotivo negativo e stress.

La percezione di non essere in grado di affrontare una determinata situazione contribuisce a far sviluppare l'idea che essa sia difficile, spiacevole e inquietante. In tale quadro, Raines et al. (2019), Hromova H. M. (2022) e Badawi et al, (2022) hanno evidenziato l'esistenza di una correlazione fra l'intolleranza all'incertezza e il Disturbo da Stress Post Traumatico (PTSD)[124], in un campione di veterani e militari. Nello specifico, la diminuzione dei valori di intolleranza all'incertezza si associava a diminuzioni della gravità del PTSD.

In una condizione di intolleranza all'incertezza, il comandante militare può, quindi, risultare vittima del suo stato mentale, finendo per incappare in un ciclo vizioso di errori e adottare uno stile decisionale che, basato sulle esperienze precedenti, facilita la scelta di soluzioni potenzialmente non adatte a perseguire la piena risoluzione del problema in atto. Questo aspetto è stato approfondito da Laycock et al (2024) i quali hanno sottolineato che la percezione di un rischio nel corso del processo decisionale può spingere il decisore ad optare per soluzioni che portano a benefici nel breve termine piuttosto che per decisioni in grado di produrre effetti nel tempo.

Adams-White et al (2018) hanno messo in risalto che, nel corso di una simulazione in cui era stato chiesto ad un campione di persone di assumere decisioni in un set ambientato in una sala operativa di una nave militare, gli individui con una minore tolleranza all'ambiguità erano meno precisi nel loro processo decisionale. Per questo motivo, Oreshkin et al (2019) hanno sostenuto che la tolleranza all'ambiguità sia uno dei tratti personali più importanti da ricercare nel profilo dei comandanti militari. Ciò facilita il mantenimento di una adeguata capacità di adattamento, elevati standard decisionali e consente di intervenire in situazioni operative incerte, dinamiche e mutevoli con un'elevata prontezza operativa (Belin et al, 2020).

[124] Patologia psichiatrica complessa che ha come agente eziologico il trauma, un evento che si pone "al di là delle esperienze umane abituali", includendo anche le vicende la cui traumaticità è in relazione a sentimenti di paura, di impotenza e di orrore.

Infine, Rydmark et al (2021) hanno rilevato che l'avversione o l'intolleranza all'ambiguità richiede un efficace gestione della comunicazione nel corso del processo decisionale. Nello specifico, inquadrare l'ambiguità o l'incertezza nel contesto dei potenziali rischi di una operazione può indurre il decisore a richiedere ulteriori informazioni e a ritardare la propria scelta anche in un contesto critico nel quale la carenza di tempestività può determinare perdite e rendere un intervento svantaggioso in termini di costo-efficacia.

3.1 Scopo della ricerca

Scopo della presente ricerca è di osservare i frequentatori del 27° corso ISSMI presso il Centro Alti Studi della Difesa / Scuola Superiore Universitaria per conoscere:

- la ricorrenza di eventuali fattori di vulnerabilità allo stress;
- come valutano l'introduzione di sistemi intelligenti in ambito civile e militare;
- in che misura ritengono di poter svolgere con efficacia il proprio ruolo in un contesto operativo caratterizzato da fluidità, complessità, incertezza, ambiguità e progressiva introduzione di tecnologie/prodotti che utilizzeranno l'IA per funzionare;
- l'esistenza di un bisogno formativo nello specifico campo.

In tale quadro, sono state formulate anche le seguenti domande di ricerca:

- a quali fattori è correlata un'opinione positiva verso l'IA nel settore difesa?
- esiste una correlazione fra i livelli di intolleranza all'incertezza/intolleranza all'ambiguità e la percezione di autoefficacia nella gestione di problemi operativi complessi?
- esiste una correlazione fra i livelli di intolleranza all'incertezza/intolleranza all'ambiguità e la percezione di autoefficacia nell'uso di tecnologie/prodotti che utilizzano l'IA per funzionare?
- a quali fattori può essere correlata la percezione di un bisogno formativo per quanto attiene all'utilizzo di sistemi dotati di IA?

4. Metodologia

4.1 Partecipanti

Il campione esaminato è costituito dai frequentatori del 27° corso ISSMI, un bacino di personale altamente qualificato che per essere ammesso alla frequenza della predetta attività formativa è stato sottoposto ad una fase di selezione e valutazione da parte dell'organizzazione di appartenenza. Questi frequentatori costituiscono un bacino di risorse pregiate che include anche coloro che assumeranno ruoli di alta dirigenza e leadership nell'ambito della Difesa.

4.2 Materiali

È stato predisposto un questionario con l'ausilio del programma Microsoft Forms. Le domande/affermazioni incluse nel documento sono state articolate in otto sezioni.

La prima sezione (comprensiva di venticinque domande) ha avuto l'obiettivo di caratterizzare il bacino dei partecipanti, acquisendo informazioni di carattere generale (genere, età, residenza, titolo di studio, ecc.), sullo stile di vita (tempo dedicato allo sport, pendolarismo, ore di sonno, ecc.) e sui bisogni formativi percepiti come necessari per colmare eventuali gap capacitivi, tenuto conto dei cambiamenti che l'introduzione dell'IA e delle nuove tecnologie potranno determinare nella professione militare. Al riguardo, è stato chiesto di rispondere esprimendo un parere su scala Likert a 5 punti (1=totalmente in disaccordo, 5=totalmente d'accordo) alle seguenti affermazioni:

- conoscere il funzionamento delle tecnologie che utilizzano l'intelligenza artificiale, consentirà di valutare eventuali rischi con maggiore consapevolezza;
- esercitarmi ad operare e a decidere in uno staff dotato di sistemi che utilizzano l'IA mi aiuterebbe a svolgere il mio incarico con maggiore efficienza, efficacia e consapevolezza;
- le continue innovazioni tecnologiche che riguardano i processi di *problem-solving* e di *decision-making* richiedono il potenziamento delle abilità e competenze di cui sono in possesso;
- in una fase di rivoluzione tecnologica e digitale è necessario acquisire una mentalità nuova;

- vivere in un periodo di cambiamenti richiede di essere pronti ad assumersi nuovi impegni e responsabilità;

La seconda sezione (comprensiva di quattro affermazioni) ha avuto l'obiettivo di valutare l'utilità percepita, il potenziale impatto dell'IA sulla società (benefici e rischi) e l'intenzione di avvalersi di questa nuova tecnologia nella vita di tutti i giorni. A tal scopo, si è fatto ricorso all'Artificial intelligence attitude scale (AIAS – 4 – Grassini, 2023), uno strumento a quattro item per i quali viene chiesto di indicare il livello di concordanza attraverso una scala Linkert a 10 punti (1 = totalmente in disaccordo, 10 = totalmente d'accordo).

La terza sezione (comprensiva di 15 affermazioni) è stata dedicata alla valutazione degli atteggiamenti dei partecipanti nei confronti dell'utilizzo dell'IA in ambito militare. In tale quadro, si è fatto ricorso all'Attitudes toward AI in defense scale (AAID - Hadlington et al, 2023), uno strumento composto da 15 item ripartiti in due sottoscale che rappresentano rispettivamente atteggiamenti positivi (9 item) e negativi (6 item) per i quali viene richiesto di esprimere il livello di concordanza attraverso una scala Linkert a 5 punti (1=totalmente in disaccordo, 5= totalmente in accordo).

La quarta sezione (comprensiva di dieci affermazioni) è stata finalizzata a cogliere la convinzione dei partecipanti di poter svolgere con efficacia il proprio ruolo nell'ambito dell'organizzazione di appartenenza. Tale misurazione è stata effettuata attraverso la versione italiana della Scala di autoefficacia generalizzata (Sibilia et al, 1995), composta da 10 item per i quali viene richiesto di esprimere una risposta mediante una scala Likert a 4 punti (1= non vera, 4= totalmente vera). I punteggi finali inferiori a 2, compresi tra 2 e 3 e superiori a 3 indicano rispettivamente un livello basso, medio e alto di autoefficacia (Liu et al, 2024).

La quinta Sezione (comprensiva di ventidue affermazioni) è stata impiegata per conoscere l'autoefficacia percepita dai partecipanti rispetto all'uso di tecnologie/prodotti di IA in ambito militare. Tale rilevazione è stata effettuata attraverso l'utilizzo dell'Artificial intelligence self-efficacy Scale (AISE – Wang et al, 2024) che consente di indagare quattro dimensioni: assistenza (la percezione dell'IA come utile per i compiti assegnati), interazione antropomorfa (antropomorfismo percepito nel corso dell'iterazione con le tecnologie/prodotti che utilizzano l'IA per funzionare), comfort con l'IA (consapevolezza emotiva di un individuo nel corso di una interazione con prodotti di IA) e competenze tecnologiche (livello di conoscenza e di confidenza nell'utilizzo di prodotti di IA). Lo strumento prevede un sistema di risposta tipo Likert a 7 punti (1= totalmente in disaccordo, 7= totalmente d'accordo). Ai fini del presente studio, i punteggi inferiori a 3, compresi tra 3 e 5 e superiori a 5 indicano rispettivamente un livello basso, medio e alto di AISE. Gli individui con livello complessivo di AISE basso possono percepire l'utilizzo di tecnologie/prodotti di IA come un fattore di stress. Le persone che hanno un alto livello di AISE possono, invece, avere una maggiore motivazione all'apprendimento e dovrebbero impegnarsi in azioni di autoregolazione per poter migliorare la qualità delle loro conoscenze e abilità relative all'utilizzo dell'IA. Un buon livello di AISE coniugato ad una efficace capacità di gestione emotiva nel corso dell'interazione con prodotti artificialmente intelligenti lascia presagire una maggiore capacità di adattamento ad un ambiente nel quale l'IA sia uno strumento di uso comune.

La sesta sezione (comprensiva di ventiquattro affermazioni) è stata dedicata alla misurazione della convinzione di autoefficacia dei partecipanti nella gestione di problemi operativi complessi attraverso la Scala elaborata da Farnese et al (2007) che consente di esaminare 4 dimensioni: la maturità emotiva (convinzioni riguardo le proprie capacità di gestire situazioni stressanti e di affrontare imprevisti), finalizzazione dell'azione (convinzioni circa le proprie capacità di porsi obiettivi concreti e realizzabili e di perseguirli), fluidità relazionale (convinzioni circa le proprie capacità di interagire con gli altri e di mantenere buone relazioni sociali), analisi del contesto (convinzioni circa le proprie capacità di comprensione e di adattamento al contesto lavorativo di riferimento). Lo strumento prevede una modalità di risposta tipo Likert a 5 punti (1=per nulla capace, 5= del tutto capace). Ai fini del presente studio, i punteggi inferiori a 3, compresi tra 3 e 4 e superiori a 4 indicano rispettivamente un livello basso, medio e alto di autoefficacia.

La settima Sezione (comprensiva di dodici affermazioni) ha avuto l'obiettivo di valutare

l'intolleranza all'incertezza dei partecipanti attraverso la versione italiana dell' Intollerance of Uncertainty Scale (IUS-12) sviluppata Lauriola et al (2016). Lo strumento utilizza un formato di risposta di tipo Likert a 5 punti (1=Per niente caratteristico di me, 5= Esattamente caratteristico di me). Ai fini della presente ricerca, i punteggi inferiori a 3, compresi fra 3 e 4 e superiori a 4 descrivono rispettivamente un livello basso, medio e alto di intolleranza all'incertezza.
L'ottava Sezione (comprensiva di sette item) ha avuto l'obiettivo di misurare il livello di intolleranza all'ambiguità dei partecipanti attraverso il ricorso alla versione italiana della scala di ambiguità del questionario Need for Closure (Pierro et al., 1995). Tale strumento utilizza un formato di risposta di tipo likert a 6 punti (1=totalmente in disaccordo, 6= totalmente d'accordo). Ai fini della presente ricerca, i punteggi inferiori a 3 compresi fra 3 e 4 e superiori a 4 descrivono rispettivamente un livello basso, medio e alto di intolleranza all'ambiguità.

4.3 Procedura somministrazione
Il 9 ottobre 2024 il questionario è stato presentato ai partecipanti che hanno potuto aderire all'iniziativa in modo volontario e anonimo. La somministrazione è avvenuta in presenza, prevedendo la compilazione del documento in modalità online utilizzando le apparecchiature informatiche disponibili (personal computer, tablet, smartphone, ecc.). Le impostazioni utilizzate per organizzare la raccolta delle risposte hanno consentito di escludere automaticamente la possibilità di partecipare più volte alla compilazione. Coloro che hanno preso parte all'iniziativa sono stati preventivamente informati sullo scopo dello studio[125] ed hanno espresso il consenso alla loro partecipazione e al trattamento dei dati, selezionando l'opzione pertinente nelle fasi iniziali del sondaggio. È stata, inoltre, fornita una definizione di IA, al fine di fornire un inquadramento che permettesse al partecipante di comprendere le domande/affermazioni proposte e di individuare la risposta più adatta a descrivere la sua opinione.

4.4 Analisi Statistica
Per rispondere alle domande di ricerca e verificare le ipotesi formulate, è stata adottata una metodologia statistica basata sulle seguenti cinque fasi:

- Analisi descrittiva
  Le caratteristiche demografiche e comportamentali dei partecipanti sono state analizzate attraverso statistiche descrittive (media, deviazione standard, mediana e range). Sono stati generati istogrammi e distribuzioni per valutare la variabilità dei dati e individuare eventuali valori anomali.
- Valutazione dell'affidabilità degli strumenti
  La coerenza interna delle scale è stata valutata attraverso il calcolo di Cronbach's Alpha. Questo indicatore ha permesso di verificare l'affidabilità delle misure e la consistenza delle sottoscale utilizzate per valutare il bisogno di formazione in tema di IA. Per quanto riguarda le altre dimensioni analizzate, ciò non è stato necessario in ragione della già consolidata affidabilità delle scale utilizzate.
- Test di normalità
  È stato eseguito il test di Shapiro-Wilk per determinare se i punteggi delle variabili chiave seguissero una distribuzione normale. In caso di deviazioni significative dalla normalità, sono state adottate analisi non parametriche.
- Analisi delle correlazioni
  Le relazioni tra le variabili principali sono state esplorate attraverso analisi di correlazione. È stata calcolata la matrice di correlazione utilizzando il coefficiente di Spearman. I risultati generati sono stati rappresentati visivamente tramite *heatmap*. In particolare, sono state analizzate le correlazioni tra:
  - opinione positiva verso l'IA nel settore difesa e altre dimensioni misurate;

[125] Nella Sezione del questionario in cui è stata descritta la finalità della ricerca è stato precisato che le domande/ affermazioni proposte erano riconducibili ad un progetto relativo all'utilizzo dell'IA nell'ambito delle attività di uno staff militare e nel processo decisionale del Comandante operanti nel settore spaziale.

- livelli di intolleranza all'ambiguità / all'incertezza e percezione di autoefficacia nella gestione di problemi complessi;
- livelli di intolleranza all'ambiguità e all'incertezza e percezione di autoefficacia nell'uso di tecnologie e prodotti con IA;
- bisogno di formazione e altre dimensioni misurate.

− Verifica delle ipotesi

Per ciascuna ipotesi, sono stati esaminati i dati e sono stati riportati gli effetti statisticamente significativi, con particolare attenzione al valore di p (<0,05) e all'ampiezza della correlazione. Le correlazioni significative sono state classificate in base alla loro forza (debole, moderata, forte).

L'analisi è stata condotta utilizzando il linguaggio di programmazione Python, con l'ausilio delle librerie Pandas, Scipy, Pingouin e Statsmodels, per garantire una gestione rigorosa e trasparente dei dati. I risultati sono stati successivamente verificati attraverso visualizzazioni grafiche e tabelle sintetiche.

5. Risultati

5.1 Caratteristiche del campione

Al termine delle attività di somministrazione, hanno aderito all'iniziativa e compilato correttamente il questionario 169 persone di cui 157 uomini (93%) e 12 donne (7%). Tutti i partecipanti risultano in possesso di un titolo di laurea[126] (n. 109 pari al 64%) o di una formazione post-laurea (n. 60 pari al 36%). I restanti dati statici relativi ai partecipanti sono riepilogati nelle tabelle I - II.

Età	**Dimensione**		**Residenza**	**Dimensione**		**Stato civile**	**Dimensione**	
	N	%		N	%		**N**	**%**
meno di 32	12	7	**Nord Italia**	24	14	**Coniugato - Coniugata**	114	68
32-34	4	2	**Centro Italia**	105	62	**Single**	26	15
35-37	25	15	**Sud Italia**	23	14	**Convivente**	20	12
38-40	80	47	**Isole**	5	3	**Separato - Separata Divorziato - Divorziata**	9	5
41-43	35	21	**Estero**	12	7			
maggiore di 43	13	8						

Tab. I – Ripartizione del campione in relazione all'età, residenza e stato civile

[126] Requisito richiesto per l'ammissione al corso.

Ultimo settore d'impiego	Dimensione	
	N	%
Operativo	62	37
Logistico	15	9
Giuridico	11	6
Economico-finanziario	7	4
Formazione - Addestramento	8	5
Organi di Vertice della Difesa	44	26
Amministrazione -Commissariato	5	3
Infrastrutture	1	1
Cyber	7	4
Spazio	2	1
Università - Altro Impiego	7	4

Tab. II – Ripartizione del campione in relazione all'ultimo settore d'impiego

Nell'ambito del campione esaminato, il 20% dei partecipanti non pratica alcuna attività sportiva, l'11% dorme 4-5 ore a notte nel corso della settimana lavorativa ed il 66% viaggia quotidianamente per raggiungere la sede di servizio, il 18% fuma ed il 28% beve alcolici. Nessun partecipante presenta contestualmente tutte le condizioni summenzionate. Un numero di ore limitato di sonno si associa al pendolarismo quotidiano nell'11% dei casi, mentre il fumo e l'uso di alcolici si riscontrano contestualmente nel 15% degli intervistati.

5.2 Atteggiamento ed opinione nei confronti dell'IA in ambito civile e militare

Il calcolo del punteggio dell'AIAS-4 ha posto in evidenza che i partecipanti hanno complessivamente un atteggiamento ed una opinione di massima positivi sull'utilizzo dell'IA nella vita di tutti i giorni. Il 9% di coloro che hanno compilato il questionario hanno, invece, palesato una posizione neutrale o negativa, esprimendo una valutazione minore o uguale a 5 (Fig. 1).

Il punteggio riportato dal campione nelle due sottoscale dell'AAID evidenzia che non è stato ancora assunto un atteggiamento marcatamente positivo nei confronti dell'utilizzo dell'IA in ambito militare e che coesistono in egual misura idee o convincimenti positivi e negativi (Fig. 2).

Inoltre, l'89% del campione si aspetta che l'IA militare sia sottoposta al controllo dell'essere umano. Per questo motivo, viene ritenuto che il personale militare svolgerà in prospettiva un ruolo sempre più importante (64% dei partecipanti). È condivisa, altresì, l'idea che le nuove tecnologie renderanno più attendibili gli output prodotti durante il processo decisionale (53% dei partecipanti), ma accresceranno il livello di responsabilità del Comandante e del suo staff (63% dei partecipanti). Infine, il 45% degli intervistati

ritiene improbabile che l'utilizzo dell'IA in ambito militare possa determinare un impoverimento dei valori militari condivisi, mentre il 41% del campione ha preferito assumere una posizione neutrale al riguardo.

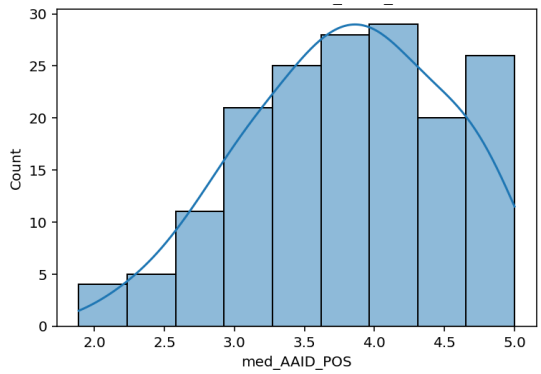


Fig. 1 – Distribuzione della media dei punteggi AIAS-4

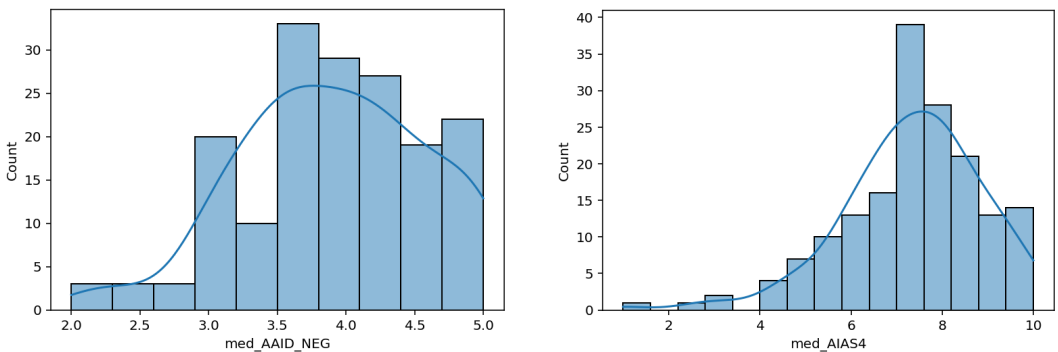


Fig. 2 – Distribuzione della media dei punteggi delle sottoscale AAID

5.3 Bisogno formativo

Il set di domande volte a misurare il bisogno formativo ha conseguito uno *score* per il coefficiente Alpha di Cronbach pari a 0.759 che consente di sostenerne l'affidabilità.

Il 44% del campione ritiene di non essere in possesso di una preparazione adeguata ad assumere un incarico di staff o di comando in una Unità in cui è previsto l'impiego di sistemi che utilizzano l'IA per funzionare (il 34% dei partecipanti ha mantenuto una posizione neutrale). In un simile scenario, viene ritenuto necessario acquisire un nuovo mindset (89% dei partecipanti), il potenziamento delle competenze già disponibili (82% dei partecipanti) ed una formazione etico-giuridica che permetta di interagire con i sistemi artificialmente intelligenti con una maggiore competenza (87% dei partecipanti). Esercitarsi ad operare nell'ambito di uno staff in cui è previsto l'utilizzo di sistemi dotati di IA (77% dei partecipanti) e la conoscenza delle loro modalità di funzionamento (89% dei partecipanti) vengono ritenute misure atte ad aumentare la capacità di valutare eventuali rischi e di poter svolgere l'incarico assegnato con maggiore efficienza ed efficacia.

5.4 Percezione di Autoefficacia

Le risposte attribuite dai partecipanti nell'ambito degli item della General Self Efficacy Scale (GSE) evidenziano che il campione ritiene di poter svolgere il proprio ruolo nell'ambito dell'organizzazione di appartenenza con un livello di efficacia medio / alto (Fig. 3).

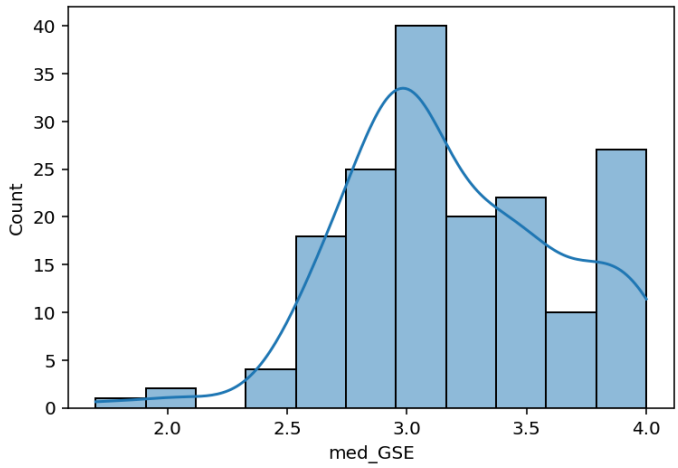


Fig. 3 – Distribuzione della media dei punteggi GSE

I partecipanti ritengono, invece, di poter affrontare un problema complesso con un livello alto di efficacia (Fig. 4). L'analisi delle dimensioni apprezzabili attraverso il ricorso alla Scala elaborata da Farnese et al, (2007) ha consentito di rilevare, altresì, che in questa fase di trasformazione digitale il 14% del campione è dell'avviso di poter gestire le relazioni sociali, le situazioni stressanti ed eventuali imprevisti con un livello medio basso di efficacia mentre il 7% crede di avere una capacità medio bassa di adattamento e comprensione del contesto lavorativo.

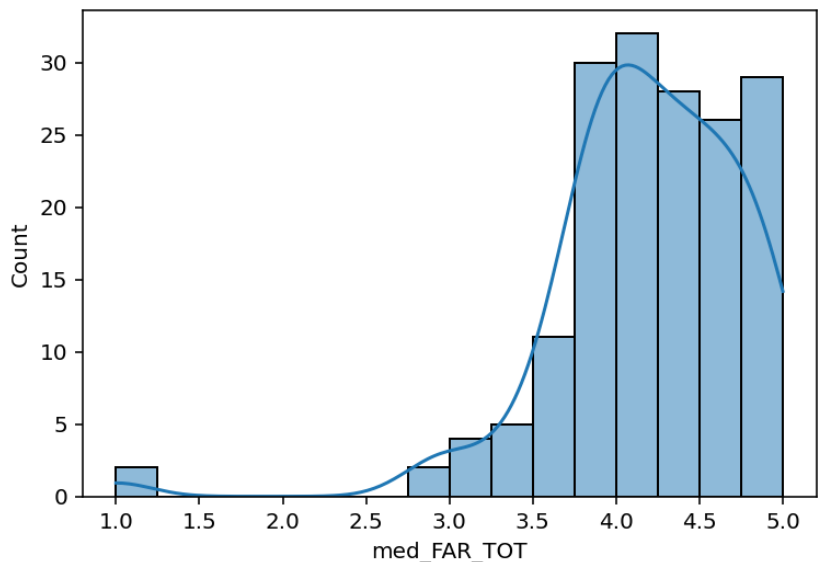


Fig. 4 – Distribuzione della media dei punteggi autoefficacia gestione problemi complessi

Per quanto attiene all'analisi dell'AISE (Fig. 5), la media dei punteggi attribuiti dai partecipanti evidenzia che il campione è dell'avviso di poter usare eventuali strumenti dotati di IA con un livello medio di efficacia. Tale convincimento si attesta ad un livello alto di efficacia nel 47% dei partecipanti mentre per il 15% la valutazione attribuita è di livello medio basso.

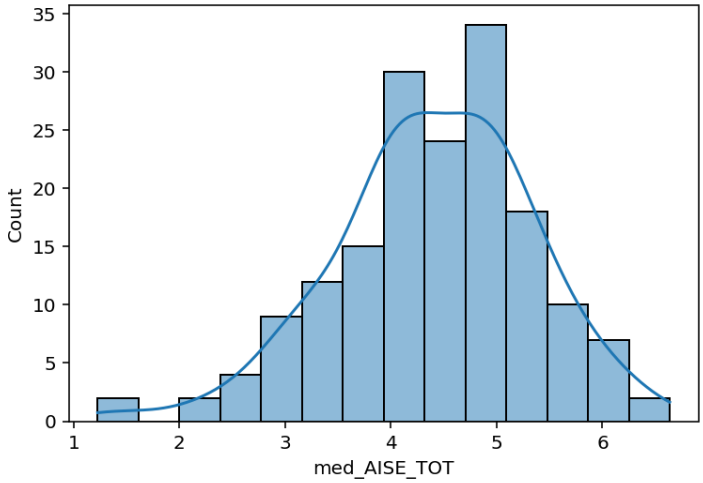


Fig. 5 – Distribuzione della media dei punteggi AISE

L'analisi di dettaglio delle sottoscale di cui è composta l'AISE ha posto in evidenza che il campione crede che nell'ambito dei compiti assegnati possa interagire con le tecnologie dotate di IA con un livello medio alto di utilità e di consapevolezza emotiva. La percezione che si possa interagire con un sistema dotato di IA con le stesse modalità con cui si agisca con un essere umano (antropomorfismo) si attesta ad un livello medio basso mentre il livello di conoscenza e di confidenza sono ritenuti di livello medio.
Il 44% dei partecipanti ha un buon livello di AISE coniugato ad una efficace capacità di gestione emotiva nel corso dell'interazione con prodotti artificialmente intelligenti, qualità che lasciano presagire una maggiore capacità di adattamento ad un ambiente nel quale l'IA sia uno strumento di uso comune. Diversamente, il 12% del personale ha un ridotto livello di AISE e una limitata capacità di gestione emotiva nel corso dell'interazione con l'IA, che descrivono una situazione in cui è possibile la manifestazione di stress, ansia e/o preoccupazione.

5.5 Intolleranza all'ambiguità e all'incertezza

La media dei punteggi attribuiti dai partecipanti evidenzia che nell'ambito del campione vi è un livello basso di intolleranza all'incertezza che, tuttavia, si attesta ad un livello medio / alto nell'11% dei partecipanti (Fig. 6).
La media dei punteggi attribuiti dai partecipanti evidenzia che nell'ambito del campione vi è un livello medio di intolleranza all'ambiguità, che, tuttavia, si attesta ad un livello medio / alto nel 47% dei partecipanti (Fig. 7).

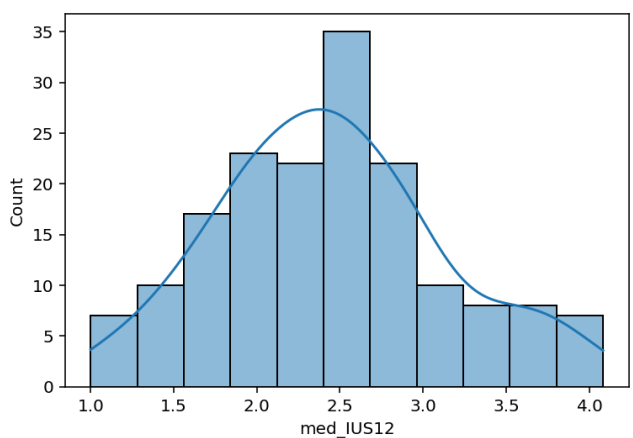


Fig. 6 - Distribuzione della media dei punteggi relativi all'intolleranza all'incertezza

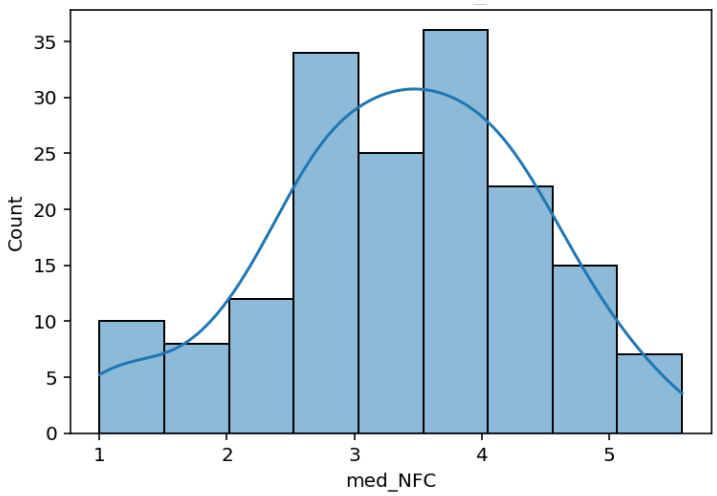


Fig. 7 - Distribuzione della media dei punteggi relativi all'intolleranza all'ambiguità

5.6 Verifica delle domande di ricerca

Prima di procedere con la verifica delle domande di ricerca, è stata valutata la normalità delle distribuzioni delle variabili principali utilizzando il test di Shapiro-Wilk. I risultati (riepilogati in tabella III) indicano che la maggior parte delle variabili non segue una distribuzione normale, con p-value inferiori a 0.05. In particolare, variabili come AIAS - 4 ($p = 0.00007$) e FARNESE ($p < 0.00001$) evidenziano deviazioni significative dalla normalità in tutte le dimensioni. Tuttavia, alcune eccezioni, come AISE Tot. ($p = 0.1184$) e IUS12 ($p = 0.0515$), indicano una conformità alla normalità.

Alla luce di questi risultati, sono stati adottati metodi statistici non parametrici per analizzare le relazioni tra le variabili. Questo approccio si è rivelato più adatto per garantire la robustezza dell'analisi, dato il mancato rispetto dell'assunzione di normalità per la maggior parte delle variabili.

Variabile	p-value	Distribuzione Normale
AISE Tot.	0,11837426	Sì
IUS12	0,05147036	Sì
NFC	0,04884550	No
AISE TS	0,02224411	No
AAID Pos.	0,01277032	No
AAID Neg.	0,00122446	No
AISE CF	0,00022481	No
GSE	0,00015954	No
NFT	0,00014808	No
AIAS4	0,00007042	No
AISE AI	0,00002743	No
AISE AS	0,00000327	No
FARNESE ME	0,00000002	No
FARNESE FR	0,00000000	No
FARNESE Tot.	0,00000000	No
FARNESE AC	0,00000000	No
FARNESE FA	0,00000000	No

Tab. III – Risultati test Shapiro-Wilk

La fase di verifica è stata effettuata utilizzando l'analisi di correlazione di Spearman, in considerazione dell'assenza di normalità, per valutare le relazioni tra le variabili considerate e rispondere alle domande di ricerca. Di seguito sono presentati i risultati per ciascuna ipotesi,

con una sintesi approfondita delle evidenze emerse.

Ipotesi 1: Fattori correlati all'attitudine/opinione positiva verso l'IA nel settore difesa
L'opinione positiva verso l'IA nel settore difesa (misurata con l'AAID) è risultata correlata moderatamente (r = 0.60, p < 0.001) con **l'opinione generale verso l'IA** (misurata con l'AIAS-4), suggerendo una relazione significativa tra la percezione dell'IA nella vita di tutti i giorni e il suo utilizzo in contesti militari. Inoltre:

- la correlazione con la **percezione di autoefficacia nell'uso di tecnologie/prodotti con IA (AISE - assistenza)** è moderata (r = 0.52, p < 0.001), evidenziando che chi percepisce l'IA come uno strumento utile tende a sviluppare un atteggiamento positivo verso la sua applicazione in ambito difesa.
- sono state osservate correlazioni deboli con la stessa **percezione di autoefficacia** (AISE) nelle dimensioni del **comfort** (r = 0.32, p < 0.001) e delle **competenze tecnologiche** (r = 0.22, p = 0.004), indicando che anche la componente emotiva e le competenze tecniche contribuiscono all'attitudine positiva, sebbene in misura minore.

Questi risultati suggeriscono che l'attitudine verso l'IA nel settore difesa è strettamente connessa alla percezione generale dell'IA e alla fiducia nell'utilizzo di tecnologie IA per attività di livello pratico o tecnico.

Ipotesi 2: Correlazione tra intolleranza all'incertezza e percezione di autoefficacia nella gestione di problemi complessi
L'**intolleranza all'incertezza** mostra correlazioni negative deboli ma significative con la **percezione di autoefficacia nella gestione di problemi complessi** (r = -0.29, p < 0.001). Nello specifico:

- la correlazione con la **maturità emotiva** è leggermente più pronunciata (r = -0.37, p < 0.001), evidenziando che una maggiore intolleranza all'incertezza è associata a una riduzione della capacità percepita di gestire emozioni e situazioni stressanti.
- la correlazione con la **fluidità relazionale** è debole (r = -0.29, p < 0.001), indicando un impatto minore ma comunque significativo sui rapporti interpersonali in situazioni complesse.

Questi risultati evidenziano che l'intolleranza all'incertezza rappresenta un fattore di vulnerabilità per la risoluzione di problemi complessi con particolare riferimento alle dinamiche legate alla gestione delle emozioni e delle relazioni.

Ipotesi 3: Correlazione tra intolleranza all'ambiguità e percezione di autoefficacia nella gestione di problemi complessi
L'**intolleranza all'ambiguità** è correlata negativamente e debolmente con la maturità emotiva (r = -0.24, p = 0.002). Non emergono correlazioni significative con altre dimensioni dell'autoefficacia nella gestione di problemi complessi, suggerendo un impatto limitato rispetto all'intolleranza all'incertezza.

Ipotesi 4: Correlazione tra intolleranza all'incertezza/all'ambiguità e percezione di autoefficacia nell'uso di tecnologie/prodotti con IA:
Non si rilevano correlazioni significative tra l'intolleranza all'incertezza o all'ambiguità e la percezione di autoefficacia nell'uso di tecnologie/prodotti con IA (misurata con l'AISE), indicando che questi fattori non influenzano direttamente la fiducia nell'uso di tali strumenti.

Ipotesi 5: Fattori legati alla percezione di bisogno di formazione per l'utilizzo di IA
La **percezione di autoefficacia nell'uso di tecnologie/prodotti con IA** (AISE - assistenza) mostra una correlazione moderata con il **bisogno di formazione per l'utilizzo di IA** (r = 0.51, p < 0.001). Altre correlazioni significative includono:

- una correlazione moderata con l'**opinione positiva verso l'IA nel settore difesa** (r = 0.49, p < 0.001);
- correlazioni deboli con il comfort (r = 0.30, p < 0.001), **le competenze tecnologiche** (r = 0.21, p = 0.006) e le dimensioni dell'**autoefficacia nella gestione di problemi complessi** (r da 0.21 a 0.32, p < 0.01).

Questi risultati evidenziano che il bisogno di formazione è principalmente legato alla percezione dell'utilità dell'IA e alla fiducia nei propri mezzi per utilizzarla, ma è influenzato anche dall'opinione generale verso l'IA (misurata tramite l'AIAS-4) e da competenze

trasversali.

Ipotesi 6: Correlazione tra percezione di autoefficacia nell'uso di tecnologie/prodotti con IA e gestione di problemi complessi

Sono state rilevate correlazioni deboli ma significative tra la percezione di **autoefficacia nell'uso di tecnologie/prodotti con IA** (misurata con l'AISE) e la **percezione di autoefficacia nella gestione di problemi complessi** per quanto attiene alle dimensioni della **fluidità relazionale** ($r = 0.27$, $p < 0.001$), della **maturità emotiva** ($r = 0.24$, $p = 0.001$) e dell'analisi del contesto ($r = 0.23$, $p = 0.003$).

Questi risultati indicano che la fiducia nell'uso di tecnologie IA è associata alla capacità percepita di gestire problemi complessi, sebbene il legame sia relativamente debole.

In sintesi, l'analisi delle ipotesi di ricerca ha evidenziato che:

- l'opinione positiva verso l'IA nel settore difesa (misurata con l'AAID) è fortemente influenzata dall'opinione generale verso l'IA (misurata con l'AIAS-4) e dalla percezione di autoefficacia (misurata con l'AISE) nelle dimensioni di assistenza e comfort;
- l'intolleranza all'incertezza è un fattore critico che riduce la percezione di autoefficacia, in particolare nella gestione di problemi complessi e nelle dimensioni di maturità emotiva e fluidità relazionale;
- il bisogno di formazione nel settore dell'IA è guidato dalla percezione della sua utilità, dall'opinione positiva del suo utilizzo in ambito militare e dalle competenze tecnologiche disponibili, suggerendo l'importanza di programmi di formazione specifici e mirati.
- le relazioni tra la percezione di autoefficacia nell'uso di tecnologie IA e la gestione di problemi complessi evidenziano che la fiducia nelle tecnologie è un aspetto chiave per migliorare le capacità decisionali in contesti operativi complessi.

6. Discussione

Nel corso di una operazione militare moderna la capacità di decidere in tempi brevi, in scenari caratterizzati da rapidi cambiamenti e in condizioni di alto stress o di forte rischio, rappresenta un importante fattore di successo. Lo stress, in particolare, è risultato un argomento rilevante nel corso della presente ricerca poiché lo stato di iperattivazione dell'organismo determinato dalla percezione di una minaccia (anche eventuale) e dal timore di non saperla o di non poterla affrontare accresce la vulnerabilità all'incertezza e all'ambiguità e può essere causa di un blackout cognitivo che rende difficoltoso, se non addirittura impossibile, affrontare e adottare i provvedimenti necessari a risolvere un problema.

In tale quadro, i dati raccolti attraverso il questionario somministrato ai frequentatori del 27° corso ISSMI del Centro Alti Studi della Difesa / Scuola Superiore Universitaria hanno consentito di dare una risposta alle seguenti domande:

- **Esistono fattori di vulnerabilità allo stress?**

  È stato rilevato che nell'ambito del campione esiste la ricorrenza di condizioni che possono accrescere la vulnerabilità di un individuo agli effetti dello stress. Una parte dei partecipanti ha, infatti, uno stile di vita caratterizzato da carenza di sonno, mancanza di attività sportiva, uso di alcol e abitudine al fumo che sono comportamenti molto spesso associati ad un alto rischio di carico allostatico (McEwen et Stellar, 1993; Guidi et al, 2020). Quest' ultimo è un concetto molto utilizzato in letteratura per descrivere l'usura dei sistemi (incluso il cervello) a cui l'organismo va incontro a causa del protrarsi delle risposte neurali e neuroendocrine agli stressor ambientali. Quando lo stato di attivazione fisiologica si protrae nel tempo, il corpo arriva in una condizione di sovraccarico in cui, esaurite le risorse psicofisiche disponibili, non è più in grado di sostenere un'ulteriore fase di adattamento al cambiamento e di ripristinare una condizione di equilibrio (omeostasi). Ciò può causare la manifestazione di una vasta gamma di patologie e compromettere il benessere psicosociale dell'individuo (Beese et al, 2022; Calabrò et al, 2024; Gostoli et al, 2024). Il sonno, in particolare, svolge una importante funzione omeostatica che ha positive ricadute sul corretto funzionamento dei network preposti alle funzioni cognitive di ordine superiore, alla regolazione delle emozioni e del tono dell'umore, alla valutazione degli stati di allertamento e della cessazione di una situazione di pericolo. Inoltre, dormire poco inficia i processi di rielaborazione di un evento e ingenera malfunzionamenti nell'ambito dei neuro-circuiti che permettono di svolgere le attività di *decision making* e *problem solving*, accrescendo il rischio che venga adottato uno stile decisionale disadattivo o che si

manifesti una propensione all'impulsività nel corso di un imprevisto o di un'emergenza. Infine, il sonno ha un ruolo importante nei processi di formazione della memoria che risultano determinanti per l'elaborazione di idee innovative qualora si debba affrontare un evento nuovo e impossibile da prevedere (Harrison et Horne, 2000; Killgore et al, 2017; Ficca et Fabbri, 2019).

La decisione di non praticare alcuna attività sportiva (o l'impossibilità di poterla svolgere) può avere negative ricadute sulla qualità della performance lavorativa. Secondo una recente revisione, infatti, l'attività sportiva migliora la neurogenesi e la funzione sinaptica nelle regioni cerebrali che concorrono al funzionamento della memoria e ai processi di apprendimento (Martín-Rodríguez, 2024). Inoltre, l'attività fisica è un fattore di crescita dell'autostima, concorre alla percezione di autoefficacia (Pekmezi et al, 2009) e fornisce agli individui gli strumenti necessari per affrontare efficacemente le avversità della vita e per adattarsi con successo ai cambiamenti (Anderson et Shivakumar, 2013; Sarkar et Fletcher, 2014). Per questo motivo, le linee guida dell'Organizzazione Mondiale della Sanità (OMS) indicano che tutti gli adulti dovrebbero svolgere settimanalmente circa 150-300 minuti di attività fisica di intensità moderata o 75-150 minuti di attività fisica più intensa o optare per una combinazione di tali modalità. Secondo l'OMS, peraltro, mantenere l'abitudine a condurre una regolare e adeguata attività sportiva, anche in condizione di particolare impegno lavorativo, consente di accrescere il livello di benessere psicofisico, di migliorare il tono dell'umore e di mitigare il rischio di malattie, ivi incluse quelle causate dallo stress e dalla sedentarietà (WHO, 2020).

Chaiton et al (2024) descrivono il fumo come uno stressor psicobiologico che ha effetti dannosi sul sistema nervoso e sulla qualità della salute mentale. L'astinenza da nicotina provoca ansia, agitazione, irrequietezza e difficoltà di concentrazione che in particolari condizioni possono limitare la performance cognitiva di un decisore. L'utilizzo della sigaretta elettronica può anch'essa ingenerare una forma di dipendenza che contribuisce alla manifestazione dei sintomi della depressione anche tra giovani e giovani adulti che non hanno mai fumato sigarette. L'uso di alcol è, infine, un amplificatore degli effetti che lo stress può ingenerare sulla qualità del funzionamento del sistema cognitivo. Al riguardo, Seemiller et al (2024) hanno sottolineato che la combinazione di stress con un uso eccessivo di alcol altera il funzionamento della corteccia prefrontale, del nucleo accumbens e dell'ippocampo, creando le condizioni che favoriscono l'eziologia della malattia di Alzheimer. Inoltre, l'uso di alcol può deteriorare la qualità del microbioma intestinale e facilitare la produzione di metaboliti che hanno un ruolo nei processi di neuroinfiammazione e, conseguentemente, un impatto sulla qualità del tono dell'umore e sui processi decisionali (Koutromanos et al, 2024).

- **Come viene valutata l'introduzione di sistemi intelligenti in ambito civile e militare? È emerso un bisogno formativo?**

  Il campione ha un atteggiamento positivo nei confronti dell'utilizzo dell'IA nella vita di tutti i giorni. L'impiego dell'IA in ambito militare suscita interesse sebbene i partecipanti non abbiano ancora assunto un atteggiamento marcatamente positivo o negativo. Queste informazioni confermano la tendenza già rilevata in un campione dell'opinione pubblica italiana durante una rilevazione condotta nel periodo fra dicembre 2023 e gennaio 2024 (D'Urso, 2024). Inoltre, la verifica delle domande di ricerca ha evidenziato che una favorevole predisposizione verso l'IA nel settore difesa è fortemente influenzata dall'opinione generale verso l'IA (misurata con l'AIAS-4) e dalla percezione di autoefficacia (misurata con l'AISE) nelle dimensioni di assistenza e comfort.

  Uno degli elementi su cui è interessante soffermarsi è il livello di consapevolezza emersa dalle risposte fornite dai partecipanti. Questi ultimi, infatti, sono apparsi consci dell'inevitabilità del cambiamento in atto e dei vantaggi o degli svantaggi che accompagnano l'introduzione dell'IA nel proprio contesto lavorativo. In effetti, il Capo di Stato Maggiore dell'Esercito Italiano ha recentemente sottolineato che l'innovazione rappresenta la chiave di volta per il successo. Secondo l'Alto Ufficiale sarà molto importante sapersi adattare al presente mentre ci si trasforma per il futuro, avendo chiara l'idea che un'organizzazione che non si innova non sopravvive in un'epoca in cui l'IA sarà pervasiva e determinante in ogni combinazione di tecnologia su cui si baseranno i

nuovi sistemi d'arma (Masiello, 2024). Una chiara visione degli obiettivi organizzativi e delle tempistiche entro cui vanno conseguiti (entro i prossimi tre anni), delle risorse e dell'impegno richiesti aiuta a comprendere le ragioni per cui nell'ambito del campione è emersa una condivisa esigenza formativa e l'interesse ad acquisire nuove conoscenze, competenze e abilità. Abbiamo, infatti, rilevato che il bisogno di formazione nel settore dell'IA è guidato dalla percezione della sua utilità in ambito militare e dalle competenze tecnologiche disponibili. In tale quadro, possedere un *mindset* digitale e avere la possibilità di potersi mettere alla prova in un contesto in cui l'IA è una componente del processo di pianificazione sono stati ritenuti dai partecipanti, ad esempio, delle tappe formative importanti per essere pronti a svolgere adeguatamente le future mansioni dirigenziali nelle rispettive organizzazioni.

Questo risultato è coerente con i livelli di autoefficacia rilevati e con gli esti degli studi riportati nel paragrafo 3. Infatti, la chiarezza del proprio ruolo e del livello di performance richiesto dall'organizzazione è un fattore importante di resilienza che, oltre a sostenere l'adattamento, motiva l'individuo a migliorare la propria formazione per poter essere sempre pronto all'impiego. Inoltre, Garg et Dhar (2017), Al-Hamdan et Bani Issa (2022) e Park et Kim (2023) hanno posto in evidenzia l'importanza del supporto che l'organizzazione è in grado concretamente di fornire alla propria componente umana. Questi studi hanno, infatti, constatato una correlazione positiva fra i livelli di supporto percepito dal personale e la qualità delle loro prestazioni e della loro motivazione, oltre che una migliore predisposizione all'autoformazione e una maggiore soddisfazione lavorativa (Rhoades et Eisenberger, 2002). È, quindi, molto importante che l'organizzazione sappia cogliere questa richiesta di supporto e offrire gli strumenti necessari per facilitare l'adattamento al cambiamento e per poter affrontare le nuove sfide, utilizzando l'innovazione tecnologica come un ausilio per poter meglio gestire la complessità, l'incertezza e l'ambiguità tipiche dei contesti in cui la Difesa è chiamata ad operare.

- **Il campione ritiene di poter svolgere con efficacia il proprio ruolo in un contesto operativo caratterizzato da fluidità, complessità, incertezza, ambiguità e progressiva introduzione di tecnologie/prodotti che utilizzeranno l'IA per funzionare?**

  I dati raccolti attraverso l'utilizzo delle scale di autoefficacia impiegate nel presente studio evidenziano che il campione ha di massima una buona percezione di efficacia ed è dell'avviso di poter usare eventuali strumenti dotati di IA nell'ambito delle attività istituzionali a cui sono preposti con un livello capacitivo medio. I livelli di AISE riscontrati suggeriscono che il personale possa tentare di ricercare in autonomia informazioni sulla specifica materia. È opportuno, quindi, che l'organizzazione garantisca l'accesso ad una formazione di elevata qualità nel settore dell'IA, al fine di prevenire e/o antagonizzare l'effetto del contagio emotivo che potrebbe essere causato da azioni di *cognitive warfare* o dalla mera circolazione di narrazioni distopiche della realtà in questa fase in cui è più forte la diffusione dell'IA nel tessuto sociale ed in ambito militare. Questa misura è quanto mai necessaria per sostenere la fiducia nelle nuove tecnologie e per evitare di incappare in un circolo vizioso che, in carenza di un efficace supporto organizzativo, potrebbe limitare la percezione di autoefficacia e trasformare la cattiva informazione "nell'agente eziologico" dell'intolleranza all'ambiguità e all'incertezza (fig. 8). Quest'ultima, in particolare, è risultata un fattore critico per un comandante poiché si associa ad un decadimento della percezione di autoefficacia nella gestione di problemi complessi oltre che della capacità di regolare l'emotività e di comprendere le modalità più adatte per relazionarsi con gli altri. L'esperienza del COVID-19 ha, infatti, portato prepotentemente alla ribalta l'importanza di garantire l'accesso a notizie certe e documentate soprattutto quando le persone affrontano situazioni di incertezza e di pericolo anche potenziale. In tali circostanze, la preoccupazione facilita la concatenazione di pensieri persistenti e ripetitivi che spingono l'individuo a cercare rassicurazioni, nuove informazioni o distrazioni che impediscono il normale processo di autocontrollo (Luo et al, 2021) e alimentano continuamente un forte senso di incertezza, favorendo la formazione di convincimenti o condotte irrazionali (Fernández-Luque et Bau, 2015).

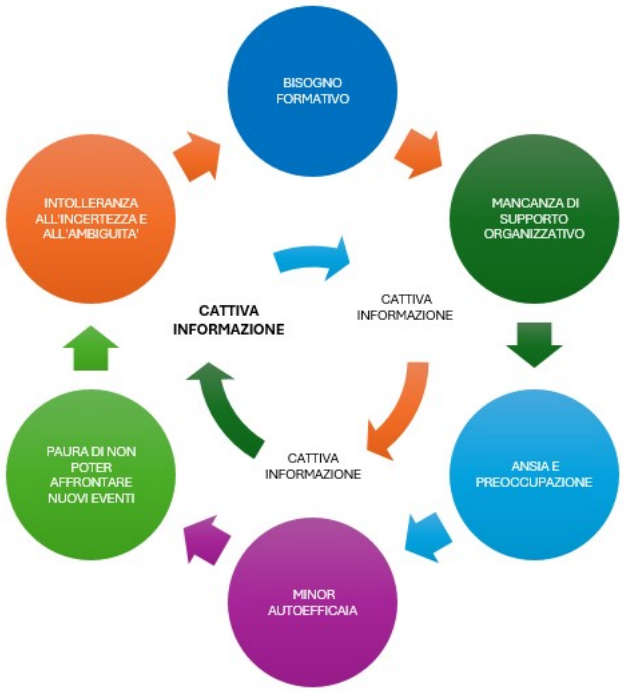


Figura 8 - Ruolo della cattiva informazione nell'eziologia dell'Intolleranza all'incertezza e all'ambiguità

- **Qual è la possibile *way ahead*?**

  L'IA è uno strumento che può agevolare l'assunzione di decisioni consapevoli ed informate in un ambiente operativo complesso (come lo è appunto il settore spaziale) poiché soggetto a continue evoluzioni alimentate da ambiguità ed incertezza. Tuttavia, l'interazione con queste tecnologie non è scevra da problematiche e può risentire di pregiudizi che possono avere un'origine umana o artificiale. In una logica di *conflict continuum,* non può essere escluso che l'avversario riesca a neutralizzare le tecnologie disponibili o a limitarne gli standard qualitativi di funzionamento, lasciando l'individuo a dover subire gli effetti degli errori commessi e a fronteggiare le sue fragilità.

  È necessario, quindi, mantenere l'essere umano al centro del cambiamento e investire sulla sua formazione cercando di renderla adeguata all'evoluzione dei tempi. La conoscenza è il rimedio per prevenire l'ansia e la preoccupazione ma è anche l'ingrediente principale per costruire la fiducia nei confronti delle nuove tecnologie. Per questo motivo, è necessario consentire ai leader di:

  - migliorare periodicamente il bagaglio di esperienze e conoscenze acquisite nel tempo (con particolare riferimento alle competenze trasversali e digitali) e di poterle mettere alla prova in ambienti protetti. Al riguardo, sviluppare capacità di ascolto attivo e di intelligenza emotiva potrebbe risultare utile per poter gestire con efficacia la propria emotività e le relazioni con gli altri;
  - essere consapevole della qualità degli strumenti tecnologici disponibili e dei vantaggi/svantaggi correlati al loro utilizzo nonché della sua capacità di saper cogliere le *chance* più propizie, individuando i tempi e le modalità più adatte per l'azione;
  - comprendere la situazione da affrontare attraverso l'impiego di tutte le informazioni utilizzabili;
  - saper apprendere dagli errori, rimanendo motivati anche nelle avversità e nell'insuccesso.

  In tale quadro, è emergente l'idea che i processi decisionali e di pianificazione debbano essere più flessibili per potersi meglio adattare alle nuove esigenze operative (che possono richiedere anche capacità decisionali in tempo reale) e al *battle rhythm* che le caratterizza

(Sottilare, 2024). Kumar et Taneja, (2023), Gasaway, (2024), Fattoum et al (2024) e Wallin (2024) hanno sottolineato la crescente importanza che viene riconosciuta all'intuizione e alla creatività (Wrigley et Simons, 2025) nell'ambito del processo decisionale dei leader moderni.

Montefusco et Angeli (2024) evidenziano che l'intuizione svolge un ruolo importante nel processo di attribuzione di significato all'insieme di variabili e di dati che in un sistema adattivo complesso si manifestano con modalità diversificate rispetto a quanto accadrebbe in una routine ordinaria. Secondo gli autori, la fluidità e l'ambiguità di una situazione complessa possono essere affrontate acquisendo una preparazione dinamica che, anche attraverso il ricorso all'intuizione, permetta di regolare con continuità e tempestività l'azione in atto e, al contempo, di acquisire nuovi schemi mentali. Il processo che ne deriva ha positive ricadute sulla resilienza organizzativa, sulla qualità delle decisioni e delle risposte fornite a situazioni inaspettate oltre che sulle possibilità di individuare, testare e implementare nuove soluzioni, anche di natura creativa.

Wrigley et Simons (2025) hanno posto in evidenza che i tradizionali sistemi di comando e controllo, incentrati su metodologie riduzionistiche e orientate alla semplificazione dell'ambiente operativo, non si prestano più all'analisi dei nuovi scenari in cui la miscela fra tecnologia, complessità e la diffusione di grandi quantità di dati eccedono la capacità cognitiva degli staff preposti alla pianificazione, anche di livello strategico. Per questo motivo, propongono l'idea di una pianificazione adattiva che, attraverso un approccio innovativo e riflessivo, consenta dinamicamente la creazione di senso, la comprensione dell'ambiente e, conseguentemente, l'identificazione degli adeguamenti da apportare all'azione militare per mantenerne l'efficacia e la reattività all'evoluzione di situazioni molto complesse oltre che per poter sviluppare un processo operativo che consenta di attuare cambiamenti che incidono concretamente sulle parti interessate.

L'efficacia delle decisioni intuitive e creative è determinata dalla qualità del bagaglio di esperienze, conoscenze, capacità e abilità possedute dall'individuo e dalla sua attitudine a individuare adeguate associazioni fra le informazioni immagazzinate nella propria memoria e quelle riconosciute in una specifica situazione o apprese durante lo svolgimento di un compito. Tale processo richiede il coinvolgimento di grandi reti cerebrali (rete predefinita, rete di controllo esecutivo e rete di salienza) che attraverso un funzionamento perfettamente coordinato consentono all'individuo di riflettere e sviluppare nuove idee, di procedere al controllo cognitivo e di individuare la soluzione più appropriata al problema oltre che di allocare le risorse attentive disponibili in relazione al compito da svolgere (Bourgeois-Bougrine, 2020; Raffaelli et al, 2020).

L'intuizione e la creatività non sono qualità innate e possono essere addestrate. Recentemente, Abdulmohdi et McVicar (2024) hanno posto in evidenza che la simulazione aumenta la capacità di assumere decisioni in situazione ad alto rischio come nel caso delle professioni sanitarie. Secondo gli autori una simulazione caratterizzata da standard elevati di qualità e di autenticità può consentire un'esperienza immersiva che facilita il trasferimento delle conoscenze, il livello di apprendimento e la capacità di applicazione della teoria nelle attività pratiche. Affrontare con successo situazioni complesse in un ambiente protetto è un'opportunità che permette di prendere atto dell'utilità dei contenuti appresi e degli strumenti disponibili, è un fattore di crescita dell'autostima che incentiva la consapevolezza che si ha di sé, migliora la percezione di autoefficacia ed incoraggia un approccio proattivo alla risoluzione di un problema. Contestualmente, l'errore fornisce un'ulteriore occasione di apprendimento e rappresenta un ottimo mezzo per accrescere la consapevolezza sulle conseguenze cagionate da eventuali pregiudizi cognitivi e sulle misure da porre in essere per contrastarne gli effetti oltre che per veicolare strategie di:

- gestione dell'incertezza e dell'ambiguità o per individuare, condividere o negoziare la soluzione ritenuta più adatta ad una specifica esigenza o problematica;
- coping per mantenere saldo il livello di resilienza.

La possibilità di sperimentare stili decisionali differenti è molto utile per far maturare al leader la flessibilità cognitiva necessaria a poter scegliere consapevolmente la tipologia di performance decisionale più adotta alla situazione (Bakken et al, 2024). Questa considerazione appare in linea con le conclusioni a cui sono giunti Angeli et Montefusco (2020) per i quali l'accettazione di un approccio decisionale flessibile e altamente adattabile

può risultare utile in situazioni complesse e in rapido cambiamento, al fine di evitare l'effetto paralizzante causato dalla scelta di perseguire scelte pienamente informate che sono, sovente, cognitivamente gravose.

7. Limitazioni e direzione futura per la ricerca

Per quanto noto, questo studio rappresenta una delle prime iniziative volte a comprendere come un campione di frequentatori di un corso di alta formazione in un Istituto universitario militare italiano valuta l'introduzione di sistemi intelligenti in ambito civile e militare (in particolare nel settore spaziale), in che misura ritengono di poter svolgere con efficacia il proprio ruolo nell'attuale contesto operativo, la ricorrenza di eventuali fattori di vulnerabilità allo stress e l'esistenza di un bisogno formativo. Tuttavia, lo strumento utilizzato era di tipo "self report" vi è, dunque, la possibilità che le risposte fornite descrivano lo stato d'animo del momento o corrispondano all'esigenza dei partecipanti di conformarsi e risultare socialmente accettabili. Inoltre, non sono stati utilizzati elementi volti a misurare la motivazione del campione a rispondere al questionario che, comprendendo 120 domande/affermazioni, potrebbe essere risultato lungo e, quindi, noioso da completare. Inoltre, il campione rappresenta un *elite* di personale selezionato dalle rispettive organizzazioni, il numero di persone di genere femminile non risulta adeguatamente rappresentato ed è, pertanto, da evidenziare che ciò non ha consentito di prendere in esame il parere di coloro che hanno intrapreso un differente percorso di carriera. È auspicabile, dunque, che studi futuri utilizzino sistemi di reclutamento che permettano di ottenere un campione più ampio e rappresentativo, al fine di poter intercettare con maggiore precisione il parere della popolazione oggetto d'indagine.

Inoltre, ulteriori percorsi di ricerca potranno essere rivolti ad approfondire le esigenze qui rilevate e individuare strumenti o modelli formativi che consentano di promuovere il necessario cambiamento organizzativo.

8. Conclusioni

Condurre una operazione spaziale militare è molto complesso e può richiedere ad un comandante di dover decidere (anche in tempo reale) in situazioni caratterizzate da volatilità, incertezza, ambiguità e di carenza di informazioni, al fine di prevenire eventuali minacce, contribuire alla gestione di una crisi e per far fronte ad una emergenza o ad un imprevisto.

In queste condizioni, l'individuazione di possibili corsi d'azione e l'assunzione di una decisione possono essere ostacolati dalle ristrette tempistiche a disposizione per lo sviluppo di un processo decisionale consapevole, mirato e razionale, ma anche dal malfunzionamento delle aree del cervello proposte a sostenere questo impegno psicofisico a causa degli effetti collaterali causati da un prolungato stato di attivazione fisiologica.

L'innovazione è un processo inevitabile per poter mantenere la competitività del Paese in un contesto di *conflict continuum*. L'utilizzo dell'IA può rendere il processo decisionale più rapido ed efficace ma l'interazione fra essere umano e macchina può risentire di pregiudizi o di problematiche che potrebbero rendere probabile un insuccesso.

L'analisi e la discussione dei dati raccolti nella presente ricerca hanno permesso, in sintesi, di:

- ritenere auspicabile che nell'ambito della formazione sia posto l'accento sulla necessità di acquisire e mantenere uno stile di vita sano e un'accurata igiene del sonno per poter limitare la vulnerabilità agli effetti che lo stress potrebbe causare alle aree del cervello preposte alle funzioni cognitive;
- rilevare che il campione ha un atteggiamento positivo nei confronti dell'utilizzo dell'IA nella vita di tutti i giorni. L'impiego dell'IA in ambito militare suscita interesse, sebbene i partecipanti non abbiano ancora assunto un atteggiamento marcatamente positivo o negativo. Buona parte del campione ritiene di poter svolgere le proprie mansioni nella rispettiva organizzazione e di poter interagire con un livello medio di efficacia con sistemi gestiti dall'IA. Al riguardo, è, tuttavia, emerso un bisogno formativo di cui è auspicabile tenere conto per il futuro nell'ambito della progettazione di analoga tipologia di corsi, al fine di sostenerne la motivazione, di rafforzarne la percezione di autoefficacia del personale e di garantirne la prontezza operativa.

La formazione rappresenta, in conclusione, un settore strategico per poter mantenere l'essere umano al centro del cambiamento e per poterlo correttamente "equipaggiare" delle

conoscenze, competenze e abilità necessarie a gestire le sfide future e ad accrescere la fiducia nei confronti delle nuove tecnologie. In tale quadro, la possibilità di conoscere e saper utilizzare i nuovi sistemi basati sull'IA, di sperimentare stili decisionali flessibili e altamente adattabili, di mettere alla prova le proprie capacità nella gestione di situazioni incerte, ambigue, complesse e in rapido cambiamento sono step importanti nella crescita professionale di un comandante. La scelta di investire sulla simulazione e sul potenziamento delle competenze trasversali e delle capacità creative e intuitive dell'individuo è raccomandabile, al fine di agevolare l'apprendimento e l'applicazione delle conoscenze acquisite durante l'impiego operativo.

Ringraziamenti

Si ringrazia il Dott. Michael Romei de Socio per la consulenza fornita nell'analisi statistica dei dati raccolti e nella produzione dei prodotti grafici utilizzati nel presente studio

Riferimenti

- ABDULMOHDI, N., & MCVICAR, A. (2024). Student Nurses' Perceptions of the Role of High-Fidelity Simulation in Developing Decision-Making Skills for Clinical Practice: A Qualitative Research Study. SAGE Open Nursing, 10, 23779608241255299.
- ADAMS-WHITE, J. E., WHEATCROFT, J. M., & JUMP, M. (2018). Measuring decision accuracy and confidence of mock air defence operators. Journal of applied research in memory and cognition, 7(1), 60-69. https://doi.org/10.1016/j.jarmac.2018.01.005.
- AL-HAMDAN, Z., and BANI ISSA, H. (2022). The role of organizational support and self-efficacy on work engagement among registered nurses in Jordan: a descriptive study. J. Nurs. Manag. 30, 2154–2164. doi: 10.1111/jonm.13456.
- ALVAREZ, J. A., & EMORY, E. (2006). Executive function and the frontal lobes: a meta-analytic review. Neuropsychology review, 16, 17-42.
- AMIRI, M., VAHEDI, H., MIRHOSEINI, S. R., EGHTESADI, A. R., KHOSRAVI, A. (2019). Study of the relationship between self-efficacy, general health and burnout among Iranian heath workers. Osong Public health and Research Perspectives, 10(6), 359-367.
- Anderson, E., & Shivakumar, G. (2013). Effects of exercise and physical activity on anxiety. Frontiers in psychiatry, 4, 27.
- ANGELI, F., & MONTEFUSCO, A. (2020). Sensemaking and learning during the Covid-19 pandemic: A complex adaptive systems perspective on policy decision-making. World Development, 136, 105106. https://doi.org/10.1016/j.worlddev.2020.105106
- BAHADIR, O., & DUNDAR, C. (2024). The impact of online health information source preference on intolerance to uncertainty and cyberchondria in a youthful generation. Indian Journal of Psychiatry, 66(4), 360-366.
- BADAWI, A., STEEL, Z., HARB, M., MAHONEY, C., & BERLE, D. (2022). Changes in intolerance of uncertainty over the course of treatment predict posttraumatic stress disorder symptoms in an inpatient sample. Clinical psychology & psychotherapy, 29(1), 230-239.
- BAKKEN, B. T., HANSSON, M., & HÆREM, T. (2024). Challenging the doctrine of "non-discerning" decision-making: Investigating the interaction effects of cognitive styles. Journal of Occupational and Organizational Psychology, 97(1), 209-232.
- BANDURA, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. Psychological review, 84(2), 191.
- BANDURA, A., & CERVONE, D. (1983). Self-evaluative and self-efficacy mechanisms governing the motivational effects of goal systems. Journal of personality and social psychology, 45(5), 1017.
- BANDURA, A. (1997). Self-efficacy: the exercise of control, vol. 13. New York: W. H. Freeman.

- BARBARA, F., LUCÀ, Y., CENTO, L., & MANGIOLA, G. (2021). Il ruolo dell'autoefficacia percepita nella relazione tra perfezionismo e burnout. Cognitivismo Clinico, (2).
- BARDEEN, J. R., FERGUS, T. A., & ORCUTT, H. K. (2017). Examining the specific dimensions of distress tolerance that prospectively predict perceived stress. Cognitive Behaviour Therapy, 46, 211–223. 10.1080/16506073.2016.1233454.
- BEATY, R. E., CHRISTENSEN, A. P., BENEDEK, M., SILVIA, P. J., and SCHACTER, D. L. (2017). Creative constraints: brain activity and network dynamics underlying semantic interference during idea production. NeuroImage 148, 189–196. doi: 10.1016/j.neuroimage.2017.01.012.
- BEESE, S., POSTMA, J., & GRAVES, J. M. (2022). Allostatic load measurement: A systematic review of reviews, database inventory, and considerations for neighborhood research. International journal of environmental research and public health, 19(24), 17006.
- BELIN, A. V., BERENDEEV, M. P., MIKERIN, A. A., KOTOV, P. F., KOSTIKOVA, L. P., & BELOGUROV, A. Y. (2020, March). Adaptability issues in professional training of the military. In 4th International Conference on Culture, Education and Economic Development of Modern Society (ICCESE 2020) (pp. 660-663). Atlantis Press.
- BENDETOWICZ, D., URBANSKI, M., GARCIN, B., FOULON, C., LEVY, R., BRÉCHEMIER, M. L., ... & VOLLE, E. (2018). Two critical brain networks for generation and combination of remote associations. Brain, 141(1), 217-233.
- BOTTESI, G., NOVENTA, S., FREESTON, M. H., & GHISI, M. (2019). Seeking certainty about Intolerance of Uncertainty: Addressing old and new issues through the Intolerance of Uncertainty Scale-Revised. PloS one, 14(2), e0211929.
- BOURGEOIS-BOUGRINE, S. (2020). What does creativity mean in safety-critical environments?. Frontiers in Psychology, 11, 565884.
- Buch, R., Säfvenbom, R., & Boe, O. (2015). The relationships between academic self-efficacy, intrinsic motivation, and perceived competence. Journal of Military Studies, 6(1), 19-35.
- CALABRÒ, C., DI TILLO, E., PENSATO, U., ZENESINI, C., FAVONI, V., FONTANA, C., ... & PIERANGELI, G. (2024). Migraine chronification as an allostatic disorder: a proof-of-concept study. Neurological Sciences, 1-8.
- CARLETON, R. N., NORTON, M. P. J., & ASMUNDSON, G. J. (2007). Fearing the unknown: A short version of the Intolerance of Uncertainty Scale. Journal of anxiety disorders, 21(1), 105-117. https://doi.org/10.1016/j.janxdis.2006.03.014.
- CARLETON, R. N. (2016 - a). Into the unknown: A review and synthesis of contemporary models involving uncertainty. Journal of Anxiety Disorders, 39, 30-43. doi:10.1016/j.janxdis.2016.02.007.
- CARLETON, R. N. (2016 - b). Fear of the unknown: One fear to rule them all? Journal of Anxiety Disorders, 41, 5-21. doi:10.1016/j.janxdis.2016.03.011.
- CASULA, C. (2011). La forza della vulnerabilità. Utilizzare la resilienza per superare le avversità: Utilizzare la resilienza per superare le avversità [The power of vulnerability. Using resilience to overcome adversity: Using resilience to overcome adversity]. FrancoAngeli.
- CHAITON, M., FAN, J., BONDY, S. J., COHEN, J. E., DUBRAY, J., EISSENBERG, T., ... & SCHWARTZ, R. (2024). E-cigarette dependence and depressive symptoms among youth. American journal of preventive medicine, 66(1), 104-111.
- CERVONE, D. (1989). Effects of envisioning future activities on self-efficacy judgments and motivation: An availability heuristic interpretation. Cognitive Therapy and Research, 13, 247-261.
- CrONBACH, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297–334. https://doi.org/10.1007/BF02310555.
- COOK, K. S., CHESHIRE, C., RICE, E. R., AND NAKAGAWA, S. (2013). "Social exchange theory" in Handbook of social psychology. (Eds.) J. DeLamater and A. Ward (Springer: Science + Business Media), 61–88.
- DANIŞMAN, M., & İSPIR, G. Z. (2024). Decision-making styles, magical thinking, and intolerance of uncertainty in opioid use disorder. Indian Journal of Psychiatry, 66(1), 545-552. DOI: 10.4103/indianjpsychiatry.indianjpsychiatry_630_23.

- DUGAS, M. J., GOSSELIN, P., & LADOUCEUR, R. (2001). Intolerance of uncertainty and worry: Investigating specificity in a nonclinical sample. Cognitive therapy and Research, 25, 551-558.
- D'URSO, G. (2024). Percezione Pubblica dell'Intelligenza Artificiale militare in Italia [Public perception of military artificial intelligence in Italy]. Strategic Leadership Journal, Vol. 2, 25-57.
- EGAN, L. A., PARK, H. R., & GATT, J. M. (2024). Resilience to stress and trauma: a narrative review of neuroimaging research. Current Opinion in Behavioral Sciences, 58, 101408. https://doi.org/10.1016/j.cobeha.2024.101408.
- EL KHOURY-MALHAME, M., BOU MALHAB, S., CHAAYA, R., SFEIR, M. and EL KHOURY, S. (2024). Coping during socio-political uncertainty. Front. Psychiatry. 14:1267603. doi: 10.3389/fpsyt.2023.1267603.
- ENDLER, N. S., MACRODIMITRIS, S. D., & KOCOVSKI, N. L. (2000). Depression: The complexity of self-report measures. Journal of Applied Biobehavioral Research. https://doi.org/10.1111/j.1751-9861.2000.tb00062.x, 5, 26, 46.
- ENDRES, M. L., CHOWDHURY, S., & MILNER, M. (2009). Ambiguity tolerance and accurate assessment of self-efficacy in a complex decision task. Journal of Management & Organization, 15(1), 31-46.
- FARNESE, M. L., AVALLONE, F., PEPE, S., PORCELLI, R. (2007). Scala di autoefficacia percepita nella ricerca del lavoro. Bisogni, valori e autoefficacia nella scelta del lavoro, 172-177.
- FATTOUM, A., CHARI, S., & SHAW, D. (2024). Configuring systems to be viable in a crisis: The role of intuitive decision-making. European Journal of Operational Research, 317(1), 205-218.
- FICCA, G., & FABBRi, M. (2019). Psicologia del sonno (pp. 1-508). Maggioli editore.
- GAETA, P. (2023). Who Acts When Autonomous Weapons Strike? The Act Requirement for Individual Criminal Responsibility and State Responsibility. Journal of International Criminal Justice, 21(5), 1033-1055.
- GARG, S., and DHAR, R. (2017). Employee service innovative behavior: the roles of leader-member exchange (Lmx), work engagement, and job autonomy. Int. J. Manpow. 38, 242–258. doi: 10.1108/IJM-04-2015-0060.
- GASAWAY, R. B. (2024, May). How smart health leaders make intuitive decisions. In Healthcare Management Forum (Vol. 37, No. 3, pp. 168-172). Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/08404704231212781.
- GHORBANALIPOUR, M., ALILOU, S., BABALOU, K., & AKBARLOU, N. (2024). Depression, perfectionism, and hypertension in the elderly: a path analysis examining worry, ambiguity tolerance, and problem-solving. Elderly Health Journal, 10(1), 70-75.
- GOSTOLI, S., RAIMONDI, G., RAFANELLI, C., & GREMIGNI, P. (2024, May). Attention-Deficit/Hyperactivity Disorder and Unhealthy Lifestyle in Adolescence: Unforeseen Role of Allostatic Overload and Psychological Well-Being. In Healthcare (Vol. 12, No. 10, p. 956). MDPI.
- GRASSINI, S. (2023). Development and validation of the AI attitude scale (AIAS-4): a brief measure of general attitude toward artificial intelligence. Frontiers in psychology, 14, 1191628. doi: 10.3389/fpsyg.2023.1191628.
- GRENIER, S., BARRETTE, A. M., & LADOUCEUR, R. (2005). Intolerance of uncertainty and intolerance of ambiguity: Similarities and differences. Personality and individual differences, 39(3), 593-600. https://doi.org/10.1016/j.paid.2005.02.014.
- GUIDI, J., LUCENTE, M., SONINO, N., & FAVA, G. A. (2020). Allostatic load and its impact on health: a systematic review. Psychotherapy and psychosomatics, 90(1), 11-27. https://doi.org/10.1159/000510696.
- HADLINGTON, L., BINDER, J., GARDNER, S., KARANIKA-MURRAY, M. and KNIGHT, S. (2023). The use of artificial intelligence in a military context: development of the attitudes toward AI in defense (AAID) scale. Front. Psychol. 14:1164810. doi: 10.3389/fpsyg.2023.1164810.
- HARRISON, Y., & HORNE, J. A. (2000). The impact of sleep deprivation on decision making: a review. Journal of experimental psychology: Applied, 6(3), 236.

- HMILAR, O., & CHEREVYCHNYI, S. (2020). Uncertainty tolerance in the process of commander's decision-making. Psycological Journal , 6(2), 75-83.
- HROMOVA H. M. (2022). Interrelation between intolerance of uncertainty and the time perspective profile in the military. Current issues in personality psychology, 10(4), 321–332. https://doi.org/10.5114/cipp.2021.111984
- HASAN, M. T., ALTHAMMER, F., DA GOUVEIA, M. S., GOYON, S., ELIAVA, M., LEFEVRE, A., ... & GRINEVICH, V. (2019). A fear memory engram and its plasticity in the hypothalamic oxytocin system. Neuron, 103(1), 133-146.
- KAGAN, M. (2021). Social support moderates the relationship between death anxiety and psychological distress among israeli nurses. Psychological reports, 124(4), 1502–1514. https://doi.org/10.1177/0033294120945593.
- KANAPECKAITĖ, R., BEKESIENE, S., & BAGDŽIŪNIENĖ, D. (2022). Reserve soldiers' psychological resilience impact to sustainable military competences: on the mediating role of psychological skills (effort, self-efficacy, proactivity). Sustainability, 14(11), 6810.
- KESTLER-PELEG, M., MAHAT-SHAMIR, M., PITCHO-PRELORENTZOS, S., & KAGAN, M. (2023). Intolerance to uncertainty and self-efficacy as mediators between personality traits and adjustment disorder in the face of the COVID-19 pandemic. Current Psychology, 42(10), 8504-8514.
- KILLGORE, W. D., BALKIN, T. J., YARNELL, A. M., & CAPALDI II, V. F. (2017). Sleep deprivation impairs recognition of specific emotions. Neurobiology of sleep and circadian rhythms, 3, 10-16.
- KOKUN, O. (2024). The stability of mental health during war: Survey data from Ukraine. Journal of Loss and Trauma, 1-22. https://doi.org/10.1080/15325024.2024.2328649.
- KONING-EIKENHOUT, L. M., DELAHAIJ, R., KAMPHUIS, W., HULSHOF, I. L., & VAN RUYSSEVELDT, J. (2024). A Loss Cycle of Burnout Symptoms and Reduced Coping Self-Efficacy: A Latent Change Score Modelling Approach. Chronic Stress, 8, 24705470241286948.
- KOUTROMANOS, I., LEGAKI, E., GAZOULI, M., VASILOPOULOS, E., KOUZOUPIS, A., & TZAVELLAS, E. (2024). Gut microbiome in alcohol use disorder: Implications for health outcomes and therapeutic strategies-a literature review. World journal of methodology, 14(1), 88519. https://doi.org/10.5662/wjm.v14.i1.88519.
- KUMAR, N., & TANEJA, A. (2023). Using Intuition to Strengthen Administrative Decision-Making. Indian Journal of Public Administration, 69(1), 59-71.
- IANNELLO, P., MOTTINI, A., TIRELLI, S., RIVA, S., & ANTONIETTI, A. (2017). Ambiguity and uncertainty tolerance, need for cognition, and their association with stress. A study among Italian practicing physicians. Medical education online, 22(1), 1270009.
- JENSEN, D., KIND, A. J., MORRISON, A. S., & HEIMBERG, R. G. (2014). Intolerance of uncertainty and immediate decision-making in high-risk situations. Journal of Experimental Psychopathology, 5(2), 178-190.
- JOHNSEN, B. H., ESPEVIK, R., SAUS, E. R., SANDEN, S., OLSEN, O. K., & HYSTAD, S. W. (2017). Hardiness as a moderator and motivation for operational duties as mediator: The relation between operational self-efficacy, performance satisfaction, and perceived strain in a simulated police training scenario. Journal of police and Criminal Psychology, 32, 331-339.
- LAURIOLA, M., MOSCA, O., & CARLETON, R. N. (2016). Hierarchical factor structure of the Intolerance of Uncertainty Scale short form (IUS-12) in the Italian version. Disponible online: https://www.tpmap.org/wp-content/uploads/2016/09/Vol-23-n.3-articolo-8.pdf
- LAYCOCK, A., SCHOFIELD, G., & MCCALL, C. (2024). The effects of threat on complex decision-making: evidence from a virtual environment. Scientific Reports, 14(1), 22637.
- LIU, A., WANG, D., XU, S., ZHOU, Y., ZHENG, Y., CHEN, J. and HAN, B. (2024). Correlation between organizational support, self-efficacy, and core competencies among long-term care assistants: a structural equation model. Front. Psychol. 15:1411679. doi: 10.3389/fpsyg.2024.1411679.

- LUO, J., WANG, P., LI, Z., CAO, W., LIU, H., MENG, L., & SUN, J. (2021). Health anxiety and its correlates in the general Chinese population during the COVID-19 epidemic. Frontiers in psychiatry, 12, 743409.
- LUTHAR, S. S., CICCHETTI, D., & BECKER, B. (2003). The construct of resilience: A critical evaluation and guidelines for future work. Child development, 71(3), 543-562.
- MARAZZITI, D., BARONI, S., PICCHETTI, M., PICCINNI, A., SILVESTRI, S., & DELL'OSSO, L. (2013). Nuovi sviluppi dell'ipotesi serotoninergica della depressione: shunt del triptofano. Rivista di psichiatria, 48(1), 23-34.
- MARTÍN-RODRÍGUEZ, A., GOSTIAN-ROPOTIN, L. A., Beltrán-Velasco, A. I., Belando-Pedreño, N., Simón, J. A., López-Mora, C., ... & Clemente-Suárez, V. J. (2024). Sporting Mind: The Interplay of Physical Activity and Psychological Health. Sports, 12(1), 37.
- MARTINEZ, L.F. (2019). Legal regime sustainability in outer space: theory and practice. Global sustainability, 2, e26. doi:10.1017/sus.2019.21.
- MARX, W., MCGUINNESS, A.J., ROCKS, T. et al. (2020). The kynurenine pathway in major depressive disorder, bipolar disorder, and schizophrenia: a meta-analysis of 101 studies. Mol Psychiatry. https://doi.org/10.1038/s41380-020-00951-9
- MASIELLO, C. (2024). L'Esercito nei prossimi 3 anni. La visione del Capo di Stato Maggiore dell'Esercito. Disponibile online: https://www.esercito.difesa.it/Documents/A4_VISION_RGB.pdf (consultato il 13 dicembre 2024).
- MCEWEN, B. S., & STELLAR, E. (1993). Stress and the individual: Mechanisms leading to disease. Archives of internal medicine, 153(18), 2093-2101.
- MCKINNON, K. A., HY CALDWELL, P., & SCOTT, K. M. (2020). How adolescent patients search for and appraise online health information: A pilot study. Journal of paediatrics and child health, 56(8), 1270-1276.
- MEIER, T. B., DREVETS, W. C., TEAGUE, T. K., WURFEL, B. E., MUELLER, S. C., BODURKA, J., ... & SAVITZ, J. (2018). Kynurenic acid is reduced in females and oral contraceptive users: Implications for depression. Brain, behavior, and immunity, 67, 59-64.
- MONTEFUSCO, A., & ANGELI, F. (2024). Turning complexity into a Delight to the Mind: An integrative framework for teaching and learning complex reasoning. Management Learning, 13505076241258932.
- NINDL, B. C., BILLING, D. C., DRAIN, J. R., BECKNER, M. E., GREEVES, J., GROELLER, H., TEIEN, H. K., MARCORA, S., MOFFITT, A., REILLY, T., TAYLOR, N. A. S., YOUNG, A. J., & FRIEDL, K. E. (2018). Perspectives on resilience for military readiness and preparedness: Report of an international military physiology roundtable. Journal of science and medicine in sport, 21(11), 1116–1124. https://doi.org/10.1016/j.jsams.2018.05.005.
- ORESHKIN, N. B., SHLYKOV, Y. N., SHEVCHENKO, B. A., KOSTIKOVA, L. P., & BELOGUROV, A. Y. (2019, April). Tolerance of Ambiguity of Cadets in the Military School. In 3rd International Conference on Culture, Education and Economic Development of Modern Society (ICCESE 2019) (pp. 837-841). Atlantis Press.
- PARK, H. J., and KIM, S. (2023). Relationship between super-leadership and self-directed learning ability in online nursing education: the mediating effects of self-leadership and self-efficacy perceptions. Heliyon 9:e17416. doi: 10.1016/j.heliyon.2023.e17416.
- PEKMEZI, D., JENNINGS, E., & MARCUS, B. H. (2009). Evaluating and enhancing self-efficacy for physical activity. ACSM's health & fitness journal, 13(2), 16-21.
- POCIVAVSEK, A., BARATTA, A.M., MONG, J. A., VIECHWEG, S.S. (2017). Acute Kynurenine Challenge Disrupts Sleep-Wake Architecture and Impairs Contextual Memory in Adult Rats, Sleep, Volume 40, Issue 11, November 2017, zsx141, https: // doi. org / 10.1093 / sleep / zsx141.
- PÁEZ GALLEGO, J., DE-JUANAS OLIVA, Á., GARCÍA-CASTILLA, F. J., & MUELAS, Á. (2020). Relationship between basic human values and decision-making styles in adolescents. International journal of environmental research and public health, 17(22), 8315.

- PALUSZEK, M. M., ASMUNDSON, A. J. N., LANDRY, C. A., MCKAY, D., TAYLOR, S., & ASMUNDSON, G. J. G. (2021). Effects of anxiety sensitivity, disgust, and intolerance of uncertainty on the COVID stress syndrome: a longitudinal assessment of transdiagnostic constructs and the behavioural immune system. Cognitive Behaviour Therapy, 50, 191–203. 10.1080/16506073.2021.1877339.
- PAWLUK, E. J., & KOERNER, N. (2013). A preliminary investigation of impulsivity in generalized anxiety disorder. Personality and Individual Differences, 54(6), 732-737.
- Petrocchi, S., Iannello, P., Ongaro, G. et al. The interplay between risk and protective factors during the initial height of the COVID-19 crisis in Italy: The role of risk aversion and intolerance of ambiguity on distress. Curr Psychol 41, 437–448 (2022). https://doi.org/10.1007/s12144-021-01601-1.
- PIERRO, A., MANNETTI, L., GARSIA, V., MIGLIETTA, A., CONVERSO, D., RAVENNA, M., & RUBINI, M. (1995). Caratteristiche strutturali della versione italiana della Scala di Bisogno di Chiusura (di Webster & Kruglanski). TPM. Testing Psicometria Metodologia, 2(3-4), 125-141.
- RAFFAELLI, Q., WILCOX, R., & ANDREWS-HANNA, J. (2020). 21 The Neuroscience of Imaginative Thought: An Integrative Framework. The Cambridge handbook of the imagination, 332.
- RAINES, A. M., OGLESBY, M. E., WALTON, J. L., TRUE, G., & FRANKLIN, C. L. (2019). Intolerance of uncertainty and DSM-5 PTSD symptoms: Associations among a treatment seeking veteran sample. Journal of Anxiety Disorders, 62, 61-67.
- RHOADES, L., and EISENBERGER, R. (2002). Perceived organizational support: a review of the literature. J. Appl. Psychol. 87:698. doi: 10.1037/0021-9010.87.4.698.
- RYDMARK, J., KUYLENSTIERNA, J., & TEHLER, H. (2021). Communicating uncertainty in risk descriptions: the consequences of presenting imprecise probabilities in time critical decision-making situations. Journal of Risk Research, 24(5), 629-644.
- SANCHEZ, L., VASILE, M., MINISCI, E. (2020). AI and Space Safety: Collision Risk Assessment. In: Schrogl, KU. (eds) Handbook of Space Security. Springer, Cham. https://doi.org/10.1007/978-3-030-23210-8_136.
- SARKAR, M., & FLETCHER, D. (2014). Ordinary magic, extraordinary performance: Psychological resilience and thriving in high achievers. Sport, Exercise, and Performance Psychology, 3(1), 46.
- SATICI, B., SARICALI, M., SATICI, S. A., & GRIFFITHS, M. D. (2020). Intolerance of uncertainty and mental well-being: Serial mediation by rumination and fear of COVID-19. International Journal of Mental Health and Addiction. 10.1007/s11469-020-00305-0
- SCHWARZER, R. (2024). Stress, resilience, and coping resources in the context of war, terror, and migration. Current Opinion in Behavioral Sciences, 57, 101393. https://doi.org/10.1016/j.cobeha.2024.101393
- SEBO, J., LONG, R. (2023). Moral consideration for AI systems by 2030. AI Ethics. https://doi.org/10.1007/s43681-023-00379-1.
- SIBILIA, L., SCHWARZER, R., & JERUSALEM, M. (1995). Italian adaptation of the General Self-Efficacy Scale: self-efficacy generalized. Procedia-Social and Behavioral Sciences.
- SEEMILLER, L. R., FLORES-CUADRA, J., GRIFFITH, K. R., SMITH, G. C., & CROWLEY, N. A. (2024). Alcohol and stress exposure across the lifespan are key risk factors for Alzheimer's Disease and cognitive decline. Neurobiology of stress, 100605.
- SOTTILARE, R.A. (2024). Examining the Role of Knowledge Management in Adaptive Military Training Systems. In: Sottilare, R.A., Schwarz, J. (eds) Adaptive Instructional Systems. HCII 2024. Lecture Notes in Computer Science, vol 14727. Springer, Cham. https://doi.org/10.1007/978-3-031-60609-0_22.
- SOWAN, W., & BAZILIANSKY, S. (2024). Acute Stress Symptoms, Intolerance of Uncertainty and Coping Strategies in Reaction to the October 7 War. Clinical Psychology & Psychotherapy, 31(3), e3021.
- VANELZAKKER, M. B., STAPLES-BRADLEY, L. K., & SHIN, L. M. (2018). The neurocircuitry of fear and PTSD. Sleep and combat-related post traumatic stress disorder, 111-125.

- VARTANIAN, O., SAINT, S. A., HERZ, N., & SUEDFELD, P. (2020). The creative brain under stress: Considerations for performance in extreme environments. Frontiers in Psychology, 11, 585969.
- WALLIN, M. (2024). Rethinking Military Planning for Modern Warfare. THE ROYAL SWEDISH ACADEMY OF WAR SCIENCES, 104.
- WANG, Y. Y., & CHUANG, Y. W. (2024). Artificial intelligence self-efficacy: Scale development and validation. Education and Information Technologies, 29(4), 4785-4808.
- World Health Organization (2020). WHO guidelines on physical activity and sedentary behaviour. Geneva: World Health Organization, 1-582.
- World Health Organization, Let's flatten the infodemic curve Available Online at: https://www.who.int/news-room/spotlight/let-s-flatten-the-infodemic-curve (accessed 22 september 2024).
- WRIGLEY, C., & SIMONS, M. (2025). Creativity in Military Complexity: Design, Disruptors and Defence Forces. Taylor & Francis. https://library.oapen.org/handle/20.500.12657/95787.
- YUAN, L., JIANG, T.T. (2023). Review on intelligent autonomous control for spacecraft confronting orbital threats. Acta Automatica Sinica, 49(2): 229−245 doi: 10.16383/j.aas.c211027.
- ZAKAR, R., IQBAL, S., ZAKAR, M. Z., & FISCHER, F. (2021). COVID-19 and health information seeking behavior: digital health literacy survey amongst university students in Pakistan. International Journal of Environmental Research and Public Health, 18(8), 4009.

FOOD FOR THOUGHT

FERDINANDO SANFELICE DI MONTEFORTE

Presidente di Mediterranean Insecurity

LA LEADERSHIP DEBOLE OVVERO COME GESTIRE I SUPERIORI

Centinaia di libri sono stati scritti sulla Leadership, segno dell'interesse che l'argomento incontra, non tanto nel grande pubblico, quanto presso i responsabili della gestione di istituzioni, aziende e imprese, alla ricerca continua di una guida per svolgere al meglio i loro compiti o per istruire i diretti collaboratori.

Come nel caso della Strategia, la leadership è una disciplina empirica, metà arte e metà scienza, nata nell'ambiente militare. Anche in questo caso, a partire dal XX secolo, il mondo dell'economia e finanza e quello dell'industria l'hanno mutuata, adattandola alle esigenze specifiche dei rispettivi settori. Ovviamente, è stato necessario cambiarle il nome, dato che i militari usavano intitolarla "Arte del Comando". Siccome questa operazione di adattamento è iniziata nel mondo anglo-americano, è stato usato il termine "Leadership", rimasto poi invariato anche quando i Paesi con radici linguistiche diverse hanno adottato lo stesso approccio.

In effetti, le Forze Armate avevano avvertito, fin da tempi remoti, l'assoluta necessità di una guida per consentire ai giovani leader di comandare uomini e mezzi, pur non avendo ancora l'abilità che deriva, oltre che da predisposizioni innate, soprattutto dall'esperienza. Quest'ultima, purtroppo, se non accompagnata da una guida comportamentale, si costruisce solo al prezzo di numerosi errori. Come in altri campi, quindi, la scienza interviene per compensare la mancanza di esperienza.

Una frase attribuita, anni fa, all'Ammiraglio Cavagnari, infatti, dice che "Comandare non è come portare". Se è vero, come è vero che agire da soli è difficile, talvolta pericoloso e richiede tanta bravura e un notevole coraggio e decisione, è ancora più vero che far agire un gruppo di dipendenti all'unisono, specie in un ambiente complesso e pericoloso come un campo di battaglia o come una competizione economica o industriale, sorpassa di gran lunga queste difficoltà: il capo, infatti, non deve agire, se non per dare l'esempio, ma deve soprattutto conseguire (o conquistare) un obiettivo per mezzo delle azioni concertare di più persone a lui subordinate.

Il motivo per il quale, in campo militare, non ci si può permettere errori fu indicato, secoli fa, da Sun Tzu, che affermò "La guerra è di vitale importanza per lo Stato. È materia di vita o di morte: è una scelta che può condurre alla salvezza o alla rovina" . Non c'è quindi tempo per consentire a giovani apprendisti al comando di commettere sbagli che potrebbero compromettere l'esito di un intero conflitto.

Naturalmente, lo stesso avviene, sia pure in modo meno cruento, nel mondo economico e finanziario, dove, anziché la salvezza e la prosperità di una Nazione si ricerca, più modestamente, il bene dell'Azienda di cui si è dirigenti. Sia in campo militare, sia in quello civile, però, le situazioni difficili sono sempre all'ordine del giorno, per cui disporre di leader in grado di gestire la dura realtà con efficacia è essenziale.

Quando si parla di leadership, però, ci si dimentica che ogni capo ha un suo superiore, vicino o lontano: il capitano deve rispondere al colonnello, questi al generale, il manager alla proprietà e così via. Anche ogni statista, incluso il livello di Capo di Stato, è soggetto

alle pressioni combinate dei propri capi politici, dei Paesi più potenti, e soprattutto del proprio elettorato.
Si pone allora un problema: se è giusto parlare di rapporti tra il leader e i propri sottoposti – argomento essenziale per i giovani da educare – è altrettanto importante analizzare i rapporti che il leader deve mantenere verso l'alto, sapendo che si troverà sempre in posizione di debolezza, se non altro per il fatto che il suo superiore potrà sempre destituirlo, se lo riterrà necessario.
In conclusione, parlare di "Leadership debole" non è altro che il riconoscimento di una situazione di difficoltà che va tenuta presente, anche quando un militare o un funzionario rivestono incarichi di alto livello, persino se raggiungono livelli di vertice. Ogni posizione comporta che chi la occupa debba gestire dei superiori, o quantomeno figure o entità capaci di condizionarne la condotta, direttamente o indirettamente.
Questa situazione di grave debolezza non è sfuggita agli studiosi più accorti, fin da tempi molto lontani, e merita una pur breve riflessione, anche perché, negli ultimi decenni, è passata un po' in secondo piano, rispetto allo studio dei rapporti del leader con i propri dipendenti.

Il problema della fiducia e della fedeltà

Come viene scelto un leader tra i vari concorrenti a una posizione di comando? Il primo studioso ad analizzare il problema è stato il cinese Sun Bin , oltre 2.400 anni fa. È indicativa la sua affermazione: "Colui che non ottiene la fiducia del sovrano non può essere un generale. Uno la fiducia, due la lealtà, tre il coraggio. Lealtà verso chi? Verso il re. Fiducia verso chi? Verso il sistema di ricompense. Coraggio di che? Coraggio di cacciare coloro che non sono eccellenti. Non si può prendere il rischio di utilizzare le truppe di colui il quale non è leale verso il re" . Il leader, quindi, secondo la visione del superiore, è sostanzialmente un agente, il cui compito è di conseguire gli obiettivi che quest'ultimo gli ha assegnato.
In pratica, però, non sempre il leader viene scelto per le sue comprovate capacità, soprattutto in quei campi, come la Strategia, nei quali siano scarse le occasioni di metterle in mostra. Il politico, quindi, dovendo scegliere tra più individui che, indubbiamente, sono di alto livello qualitativo, preferisce spesso colui il quale gli ha dato prova di fedeltà.
Da un lato, questo è un bene, perché in questi casi si può ritenere che il leader abbia facile accesso al superiore politico e possa metterlo al corrente dei problemi, suggerendo le soluzioni; dall'altro, il politico, nel privilegiare la fedeltà alle altre doti necessarie, nella scelta di un leader a lui subordinato, si sottopone a tre rischi.
Il primo è quello di favorire la "politicizzazione" di aspiranti leader, la cui ambizione supera talvolta le capacità, ma che si mettono in mostra e prevalgono rispetto a colleghi di qualità maggiore. Il secondo è che il politico nel prescegliere un leader a lui fedele, si allontana, più o meno inconsciamente, dal mettere l'uomo giusto al posto giusto: non tutti i candidati, infatti, sono la scelta migliore per svolgere un determinato incarico, mentre invece in un'altra posizione eccellerebbero.
Il terzo rischio, ancora più grave, è che il leader prescelto, per eccesso di fedeltà, accetti situazioni insostenibili o utilizzi senza limiti i propri dipendenti, mettendo in pericolo il conseguimento del fine politico e, talvolta, l'esito stesso di un conflitto o di una competizione.
Si racconta, a tal proposito, che Talleyrand, quando era Ministro degli Esteri di Napoleone, raccomandasse ai giovani diplomatici di nuova nomina "Surtout pas trop de zèle" (soprattutto, non troppo zelo). L'eccesso di zelo, infatti, è un atteggiamento che spesso provoca disastri difficili da gestire. L'esempio classico è dato dall'atteggiamento

dell'Ambasciatore francese a Berlino nel 1870, il cui eccesso di zelo provocò la guerra franco-prussiana, che finì con la completa umiliazione dei Francesi.
In caso di insuccesso, nella migliore delle ipotesi, il leader finirà per essere sacrificato dallo stesso potente che lo aveva prescelto, utilizzandolo come capro espiatorio.
Un esempio classico ci è dato dalle conseguenze del disaccordo tra gli Alleati dell'Intesa, all'inizio del 1918, a riguardo del fronte francese. Come racconta lo storico Liddell Hart, "la situazione fu resa ancor più precaria dall'ostinazione con cui Clemenceau (il Primo Ministro francese) insisteva perché gli Inglesi estendessero il loro fronte a sud, fino al fiume Oise, e cioè di altri 22 chilometri. Per la V Armata britannica del generale Gough ciò significò estendere pericolosamente il proprio fronte e attestarsi in posizioni difensive inadeguate proprio nel settore in cui Ludendorff stava per sferrare il suo colpo" .
Dalla Gran Bretagna, per aggravare la situazione, non arrivarono rinforzi, per compensare la debolezza del fronte, non solo perché il Primo Ministro Lloyd George aveva in mente piani offensivi in altri teatri di guerra, ma soprattutto perché voleva evitare di alienarsi ancora una volta l'opinione pubblica interna, già sconvolta per le pesanti perdite che il Corpo di Spedizione britannico aveva subito fino ad allora sul fronte francese.
Fortunatamente per l'Intesa, i Tedeschi presero la decisione di attaccare più settori contemporaneamente, senza avere le risorse per sfruttare il successo, laddove si fosse verificato uno sfondamento. Ma in quei primi mesi del 1918, l'offensiva di Ludendorff giunse a un passo dal conseguire la vittoria.
Inutile dire che il generale Gough, che aveva accettato questa situazione precaria, e non era riuscito ad impedire ai Tedeschi di sfondare il fronte tenuto dalla sua Armata, venne regolarmente rimosso dal comando, malgrado avesse gestito la crisi con calma ed efficacia.
Eppure, fino ad allora non c'era stato un generale britannico più "ammanigliato" di lui. Egli, infatti, era il favorito del Comandante in Capo britannico, il generale Haig, che lo aveva fatto promuovere in due anni da comandante di una Brigata fino al comando in capo della V Armata, suscitando le comprensibili gelosie degli altri generali in sottordine.
Churchill, che invece nutriva dubbi sul personaggio, scrisse su di lui che "non risparmiò mai né sé stesso né le sue truppe in costosi e disorganizzati attacchi e la tragedia di Paschendaele (la sanguinosa offensiva dell'estate/autunno 1917 nelle Fiandre) fu causa di molto risentimento contro di lui da parte dei suoi subordinati" .
In definitiva, essere il pupillo di un uomo potente porta all'obbedienza cieca, a un punto tale che il primo farà di tutto per soddisfare il secondo, trascinando interi reparti alla rovina e mettendoli in situazione tale da compromettere lo stesso conseguimento del fine che il potente si prefiggeva.

Il problema del rapporto con i Superiori

Gestire un potente non è per nulla semplice, e questo è noto da tempi immemorabili. Il già citato Sun Bin, a questo proposito, ci ha lasciato una frase memorabile, anche se apparentemente ambigua: "Gli ordini del sovrano non devono varcare le porte del campo, cosa che assicura la longevità del generale. Se gli ordini varcano la porta del campo, il generale non sopravvive a lungo e l'armata non può mantenere la propria esistenza" . In parole povere, secondo l'autore, se i soldati (e/o gli impiegati) sapessero tutto ciò che accade nelle stanze del potere, si ammutinerebbero.
In effetti, coloro che si trovano al di sopra del leader commettono spesso alcuni errori gravi, o presentano alcuni difetti comportamentali che non devono essere conosciuti dai gradi più bassi, ma che il leader deve saper gestire, minimizzandoli, per il bene dei propri sottoposti e, in generale, del buon esito dell'operazione.

Il primo errore è l'impazienza o, meglio, l'insofferenza verso le situazioni che non evolvono nel senso desiderato e creano effetti che vanno molto al di là del livello tecnico-operativo, causando talvolta un vero e proprio terremoto politico. Quando, infatti, l'avversario riesce a frenare, se non a bloccare, le iniziative delle forze cui appartiene il leader, i vertici temono, non sempre a torto, che questo stallo metta in pericolo l'esito finale e la stessa stabilità della compagine governativa.
Sun Tzu ha descritto bene il timore dei vertici in questo caso che non riguarda solo le operazioni militari, ma anche quelle economiche o finanziarie: "Quando le armi sono spuntate, l'ardore spento, lo sforzo esaurito, le finanze esauste, è facile che pretendenti al poter appaiano (da ogni parte) per trarre vantaggio dalla difficile situazione (del sovrano). Allora nessuno, per quanto saggio, sarà capace di evitare l'inevitabile" .
Le due Guerre Mondiali sono il classico esempio di come un'aggressione che si intendeva violenta e di breve durata possa tramutarsi in una guerra di logoramento capace di dissanguare ambedue i contendenti, fino a causare il crollo dei rispettivi regimi.
Ma anche le cosiddette "Operazioni di Stabilizzazione" spesso rientrano in questa tipologia, e quanto più si trascinano senza esito, coinvolgendo sforzi e perdite in termini di uomini, mezzi e finanze, più mettono in pericolo l'esistenza stessa di una Nazione o di un'Alleanza. Il Vietnam e l'Afghanistan sono solo due degli esempi più recenti di quanto una tale situazione possa diventare pericolosa.
Appare quindi ovvio che i vertici siano impazienti di risolvere al più presto il conflitto, spesso da loro scatenato, e biasimano la prudenza dei leader che hanno cura di non esporre il Paese o la coalizione a un tracollo rovinoso. Una frase, attribuita a Churchill rende bene l'idea di quanto impazienti siano i vertici, a fronte dei loro sottoposti: "Prendete il più valoroso marinaio, il più intrepido aviatore, o il soldato più audace, metteteli a un tavolo insieme e cosa otterrete? La somma totale delle loro paure" .
Il secondo, grave errore dei vertici è il loro interesse eccessivo per i dettagli. Questa attenzione a volte ossessiva da parte dei vertici, per le minuzie, è pericolosa in quanto rischia di far perdere loro di vista il quadro generale, ed è controproducente, in quanto deresponsabilizza il leader, il quale potrebbe rifugiarsi nella intellettualmente comoda posizione di perfetto sottordine, oppure è costretto a opporsi al suo superiore.
Questo vizio ricorrente dei vertici viene ben descritto, in modo sintetico, dal temine inglese "Micromanagement" (letteralmente "micro-gestione"). La sua causa, secondo alcuni studi, è l'eccessiva centralizzazione delle funzioni "che ha i suoi problemi, in quanto le complessità delle moderne questioni della difesa sono troppo grandi perché un piccolo gruppo di decisori possa gestirle da solo" .
L'esempio classico di questo problema, delle sue origini e delle sue conseguenze ci è dato dalla crisi dei missili a Cuba dell'ottobre 1962. In questa situazione di grave tensione, come riferito dai compilatori di uno studio sull'organizzazione della Difesa USA, "il Presidente USA, espresse la sua preoccupazione che la Marina potesse commettere un errore e causare un incidente. Per calmare le paure del Presidente, (il Segretario alla Difesa) McNamara decise di esplorare le procedure organizzative e le regole di routine per condurre la prima intercettazione (di mercantili sovietici). Facendo visita al Capo di Stato Maggiore (Ammiraglio Anderson) nella Sala Operativa della Marina, McNamara iniziò a fare domande in tono brusco, sulle procedure, nei minimi dettagli. (La discussione divenne in breve sgradevole, tanto che) l'Ammiraglio prese il Manuale dei Regolamenti Navali e sventolandolo in faccia a McNamara, gridò (che) era tutto lì dentro. McNamara rispose (che) non gli importava nulla di cosa avrebbe fatto John Paul Jones , (ma che voleva) sapere cosa farete voi. L'incontro si concluse con l'osservazione dell'Ammiraglio Anderson che disse al Segretario: se Lei e il Suo vice tornate nei vostri uffici, la Marina gestirà il blocco" .

Inutile dire che il giorno dopo l'Ammiraglio fu rimosso dal suo incarico. La foto di lui che esce dall'edificio della Marina tra due ali di personale plaudente è rimasta famosa: quel giorno iniziò la perdita di consensi di McNamara nell'ambito del governo. Fortunatamente, anche se si seppe dopo che un sommergibile sovietico arrivò quasi al punto di lanciare un siluro con testata nucleare, il governo di Mosca diede ordine ai mercantili con i missili a bordo di invertire la rotta e tornare in Patria, prima che fossero intercettati dalle unità della US Navy.
Un Ministro come McNamara che indaga, azione durante, sulle procedure di dettaglio – che peraltro, nel caso specifico, erano state spiegate in precedenza in sede di Consiglio Nazionale di Sicurezza – oltretutto usando un tono inquisitorio, mostra uno scarso rispetto verso i leader preposti a dirigere l'operazione, ne svaluta il ruolo, crea confusione e oltretutto perde tempo prezioso nell'addentrarsi in questioni che non domina a sufficienza.
Ma anche l'Ammiraglio Anderson aveva violato una regola aurea della leadership: come consigliava uno dei primi studiosi della materia, André Gavet, "allorché un superiore interviene nel dominio dell'inferiore, questi lascia fare e dire perché vi è obbligato; appena il superiore è sparito riprende con rassegnazione l'interrotto lavoro, cancellando nei limiti del possibile l'azione estranea" .
L'autore, in sintesi, raccomanda ai leader di aver pazienza nei confronti dei vertici, che sono spesso sottoposti a pressioni ben maggiori di quelle cui i primi sono soggetti.
Il terzo, ancor più grave problema è dato dagli effetti che può esercitare un'opinione pubblica fortemente emotiva, specie se spaventata da una possibile sciagura. La pressione dei media, in questo caso, può spingere persino i vertici a prendere decisioni pericolose.
Anche qui un esempio renderà l'idea del problema. All'inizio della guerra ispano-americana del 1898, mentre il Commodoro Dewey con un'azione fulminea era penetrato nella baia di Manila e aveva distrutto le navi spagnole presenti nelle Filippine, il governo di Washington seppe che una piccola squadra spagnola, composta da quattro incrociatori corazzati, era salpata dalle isole di Capo Verde per ignota destinazione, e temette un possibile colpo di mano contro la costa americana.
Quel che è peggio, non appena la notizia si diffuse, come racconta Mahan, "la nostra costa era in una condizione di panico irrazionale, e insistette per avere piccole squadriglie sparpagliate lungo la sua lunghezza, ovunque, in accordo con la teoria di difesa sempre favorita dallo stupido terrore. La stupidità, stando a ogni esperienza militare, era assoluta e ingiustificata, ma il Ministero della Marina riuscì a opporsi al terrore – l'effetto morale – con un compromesso sulla Squadriglia Volante (gli incrociatori protetti veloci)" che fu trattenuta in acque nazionali, a scapito del principio della concentrazione delle forze.
Come si seppe poco dopo, il panico era totalmente ingiustificato. Gli incrociatori spagnoli erano in pessime condizioni di efficienza, e il loro Ammiraglio, Josè Cervera Pery, si preoccupò solo di raggiungere Cuba, per poi rinchiudersi nella munita rada di Santiago.
Ma il fatto che l'opinione pubblica americana fosse riuscita a condizionare le scelte operative della US Navy è passato alla storia, come primo esempio noto del potere che l'opinione pubblica possiede nel condizionare i decisori politici e non solo.
È di questi giorni la notizia di quanto stia avvenendo in Corea del Sud, dove la popolazione è scesa in piazza per contestare la decisione del Presidente della Repubblica di proclamare lo stato di assedio. Nessuno, neanche un Capo di Stato, è esentato dal dover rispondere delle proprie decisioni!

Come gestire il superiore

Come si può notare, la condizione di debolezza del leader lo costringe a gestire il superiore – sia esso una persona o un'entità come l'opinione pubblica – con cautela ed efficacia,

ricordandosi che si tratta di un'opera, pur faticosa e per certi versi umiliante, compiuta per il bene della missione a lui assegnata.
La storia ci presenta tre modelli di comportamento classici, profondamente diversi l'uno dall'altro, ma che non sono necessariamente antitetici, potendo essere seguiti in sequenza da uno stesso leader al mutare delle circostanze; anzi, in alcuni casi è possibile mescolarli per raggiungere un onorevole compromesso, che vada comunque a beneficio del buon esito della missione.
Il primo modello è quello classico della "Obbedienza cieca". Come affermava lo stesso Gavet, "la natura delle relazioni con il vostro capo non ha bisogno di lunghe spiegazioni. La situazione vostra di fronte a lui non è che la situazione dei vostri inferiori rispetto a voi. Siete perciò obbligato ad agire come collaboratore sottomesso e leale, in nome del dovere comune" .
Un altro autore, l'Ammiraglio Fioravanzo, però, aggiungeva una considerazione: "i galloni danno il diritto di dare degli ordini, non d'imporre delle idee" , anche se precisava di "eseguire gli ordini, senza obiezioni anche se si abbiano idee dissenzienti, perché non siamo più nel campo delle idee ma nel campo dell'azione. Non si vuole con ciò intendere che l'inferiore non debba rendere note al superiore le sue obiezioni, derivanti non già da spirito di critica, ma fondate su dati di fatto o su induzioni logiche. Si deve bensì intendere che l'ordine, una volta perfezionato, non deve più essere discusso" .
Questa affermazione, riguardante l'aspetto critico, ma importantissimo, della "collaborazione di pensiero" veniva temperata dall'avvertenza che, comunque, il giovane leader avrebbe dovuto attenersi alla "coscienziosa esecuzione degli ordini e illuminata interpretazione delle direttive (che) costituiscono imprescindibile dovere dell'inferiore" .
Ma l'Ammiraglio aggiungeva: "nella fase di elaborazione delle decisioni mostra senso di responsabilità ascendente chi prospetta al (proprio) superiore circostanze e previsioni che possono essergli sfuggite. Se l'inferiore lo fa con tatto e deferenza e con palese sentimento del dovere, e non già per sottrarsi alla responsabilità esecutiva, non ci sarà il pericolo che si senta dire (di) non fare obiezioni" .
L'importanza della collaborazione di pensiero introduce il secondo modello, quello detto del "Dialogo ineguale", che costituisce un'estensione del concetto precedente, nel senso di rendere permanente lo scambio di idee tra il leader e il suo superiore. Riferendosi a una serie di casi storici, uno studioso americano notava che "ciò che avvenne tra il presidente o il primo ministro e il generale era un dialogo ineguale – un dialogo nel quale le due parti esprimevano i loro punti di vista senza mezzi termini, talvolta in modo offensivo, e non una volta ma ripetutamente. Lungi dalle semplicistiche convenzioni della teoria normale dei rapporti civili/militari, che sembra confinare il dialogo solo all'inizio e alla fine di una guerra, la pratica di questi uomini era l'integrazione attraverso un conflitto (di idee)" .
Le accese discussioni, durante la Seconda Guerra Mondiale, tra Churchill e il Capo di Stato Maggiore della Difesa, Sir Alan Francis Brooke (poi Lord Alanbrooke) furono memorabili, e sono riportate nelle rispettive autobiografie senza mezzi termini. L'aspetto più importante, però, è che ambedue i resoconti di questo dibattito mostrano l'esistenza di un profondo senso di reciproco rispetto che animava i due uomini. Questa è la condizione sine qua non di questo modello di collaborazione dinamica e un po' eterodossa, ma che la storia mostra essere la più efficace di tutte.
Il leader, sia egli civile o militare, non deve dimenticare, infatti, che il superiore, specie il politico, deve "integrare un vasto amalgama di dati in costante mutazione, multicolori, evanescenti, in sovrapposizione tra loro, (e che sono) troppi, velocemente variabili, troppo interconnessi per essere presi, sistemati ed etichettati come delle farfalle" .
Il leader, invece, rappresenta un singolo, ben definito settore, e non ha necessariamente la visione completa della situazione, nelle sue mille sfaccettature, come viene giustamente

notato dal professor Cohen nella frase appena citata. Ma quello che non sarà ripetuto mai abbastanza è che l'applicazione di questo modello comportamentale è strettamente condizionata dall'esistenza di un profondo, reciproco rispetto tra le parti in causa, rispetto che implica il fatto che ognuno dei due interlocutori non entri a gamba tesa nel campo di competenza dell'altro.

Il terzo modello, piuttosto controverso, è quello della "Disobbedienza apparente", reso celebre da Nelson, durante la battaglia di Copenaghen. Egli era in sottordine a Sir Hyde Parker, un Ammiraglio anziano, dai modi spiacevoli e dal carattere accentratore. La missione affidata al suo sottordine era quella di aggirare da sud la capitale danese, e impegnare le batterie galleggianti che la proteggevano.

I Danesi, infatti, rendendosi conto di non poter combattere ad armi pari la flotta britannica in mare aperto, avevano schierato i loro vascelli, dopo averli disalberati, in modo che questi formassero una linea compatta di batterie, in modo da contrastare ogni tentativo di bombardamento o di sbarco dal mare.

La missione era difficile, ma Nelson l'affrontò con la sua consueta determinazione. Ne seguì uno scontro durissimo, con gravi danni dalle due parti, tanto che Sir Parker, che era rimasto al largo con il grosso della flotta, a un certo punto diede a Nelson l'ordine di ritirarsi.

L'ordine dato era però impossibile da eseguire, in quanto il vento impediva alle navi di Nelson di tornare attraverso gli stretti canali percorsi per aggirare le difese danesi. Quindi, per ritirarsi, la squadriglia di Nelson avrebbe dovuto defilare davanti alle batterie che stava impegnando duramente, prima della loro eventuale resa. In definitiva, la squadriglia di Nelson ne sarebbe uscita distrutta, o quantomeno con perdite gravissime.

Alla ricezione del segnale, Nelson "chiese al suo Aiutante di Bandiera cosa fosse il segnale alzato a bordo della nave del Comandante in Capo. Alla risposta, 'interrompete l'azione', disse, scrollando le spalle, 'non lo farò mai'. Poi osservò, rivolto al comandante Foley (comandante della nave ammiraglia), "Sappia, Foley, che ho un solo occhio, e ho diritto a essere talvolta cieco". Quindi, con una malizia tipica del suo carattere, mise il canocchiale davanti al suo occhio mancante e disse "veramente io non vedo il segnale" .

Inutile dire che, dopo poco, i Danesi alzarono bandiera bianca e Nelson poté ricongiungersi al resto della flotta, fiero del suo successo. Sir Hyde Parker, che sapeva apprezzare i valorosi, non si adombrò per la disobbedienza del suo Ammiraglio in sottordine, anzi lo raccomandò per una promozione.

Questo modello comportamentale non è raccomandato per la maggioranza delle situazioni. Vale solo quando viene dato un ordine impossibile da eseguire, e chi lo riceve sa con assoluta certezza che, per conseguire l'obiettivo assegnato, bisogna agire diversamente.

Per attenersi, comunque, bisogna possedere un livello non comune di autostima, un coraggio morale senza pari e una conoscenza approfondita della situazione, a livello ben maggiore di quanto non l'abbia il superiore che ha dato l'ordine ineseguibile. Come notava il già citato Ammiraglio Fioravanzo, "di Nelson non ne nascono molti, e ad ogni modo si tratta di coraggio della responsabilità e di chiaroveggenza dello stimare le conseguenze della propria apparente disobbedienza: se si può e si deve educare sé stessi e i dipendenti al sentimento dell'obbedienza, non si può certo fare un codice della disobbedienza. Basta ricordare che ci può capitare di dover anche disobbedire, ma mai senza avere la coscienza di rendere un servigio al proprio Paese" .

L'Ammiraglio sapeva bene quel che diceva. Nell'estate 1943, egli era al comando di una Divisione di incrociatori, con il compito di raggiungere la rada di Palermo, occupata dalle forze anglo-americane, e bombardare le navi all'ancora. Saputo che un ricognitore avversario lo aveva localizzato, decise d'iniziativa di interrompere l'incursione e rientrare in porto. Naturalmente, fu rimosso dal comando, ma evitò – come si seppe dopo – di dover

fronteggiare le forze decisamente superiori che gli Alleati avevano inviato per intercettarlo.

Più in generale, l'applicazione del modello è possibile soprattutto quando il leader non abbia ricevuto ordini, bensì delle direttive per la missione che deve compiere, ed ha quindi una certa libertà di azione.

Conclusioni

Da quanto detto finora appare chiaro che ogni leader si trova in una situazione di debolezza nei confronti di chi è il suo superiore, che sia un militare, un funzionario o un politico, dato che rischia, in ogni momento, di essere rimosso dall'incarico. Egli, però, ha il dovere di svolgere una missione, anche al rischio che il superiore lo destituisca, come è avvenuto nei casi dell'Ammiraglio americano Anderson e del suo omologo Fioravanzo.

Per il leader, comunque, il conseguimento della missione, o il suo annullamento quando questa è impossibile, va ben al di sopra di ogni altra considerazione. Certo, l'adozione di uno o dell'altro modello comportamentale dipende, oltre che dalle circostanze, dal carattere e dalla personalità del leader. Egli potrà, quindi, decidere se seguire il proprio superiore nella possibile rovina del Paese (o dell'Azienda), se ingaggiare con lui un dialogo serrato, ma produttivo, oppure se agire di testa propria, quando gli ordini ricevuti si rivelassero profondamente errati.

Nell'ultimo caso, che richiede un notevole coraggio morale, quasi pari a quello necessario per affrontare un nemico, sarà l'esito dell'azione a decidere il fato del leader, come avvenne a Nelson: il successo non viene mai criticato dai superiori, che – al massimo – tendono ad appropriarsi del merito, come se fossero stati loro a dare l'ordine risolutivo. In ogni caso, va detto che il leader deve essere animato dal sentimento di lealtà verso i propri capi, lealtà che arriva fino al punto di disobbedire loro pur di proteggerli da un rischio di fallimento generale.

Ecco, il conseguimento della missione e la lealtà verso i propri capi sono i due cardini sui quali deve ruotare il comportamento del leader nei suoi rapporti verso l'alto. In tal modo, egli avrà, comunque vadano le cose, la consolazione del dover compiuto fino in fondo.

CONFERENCE REPORT

SIMONE PASQUAZZI

Dottore di Ricerca in Scienza Politica.
Professore a contratto in Security Policies presso la LUISS "Guido Carli".
Magg. (Ris. Sel.) EI - attualmente in servizio presso l'Istituto Ricerche e Analisi della Difesa

PANEL CASD SUL CONFLITTO RUSSO-UCRAINO

Lunedì 10 marzo 2025 si è tenuto, presso la sede del Centro Alti Studi Difesa in Palazzo Salviati, un interessante panel in lingua inglese sulla guerra russo-ucraina. All'incontro hanno partecipato, in qualità di uditori, molti frequentatori civili e militari del CASD, italiani e internazionali, nonché selezionati ospiti provenienti da vari ambiti della società civile.

Il panel, moderato dal Consigliere d'Ambasciata Emanuele Farruggia, ha visto intervenire, nell'ordine, il diplomatico e politico italiano Giulio Terzi di Stantagata, già Ministro degli Esteri ed attualmente Senatore della Repubblica; l'Ambasciatore svedese in Italia Jan Björklund, già Vice Primo Ministro, Ministro dell'Istruzione e Parlamentare della Svezia; il diplomatico italiano di lungo corso Pier Francesco Zazo, Ambasciatore d'Italia in Ucraina fra il 2021 e il 2024 e precedentemente in servizio, fra le altre sedi diplomatiche, presso l'ambasciata italiana a Mosca.

L'intervento del senatore Terzi ha ricostruito in modo preciso e puntuale le origini del conflitto, evidenziando la completa responsabilità dell'esecutivo russo rispetto all'inizio delle ostilità militari. L'esposizione ha inquadrato la non legittimità giuridica del comportamento di Mosca, sia sulla base di specifici riferimenti al diritto internazionale consuetudinario e pattizio, sia attraverso una serie di parallelismi storici tratti da vicende degli ultimi due secoli. Specularmente, è stato ben evidenziato il diritto all'autodifesa da parte dell'Ucraina, *ergo* la necessità da parte della Comunità Internazionale di difendere, di riflesso, tanto il principio di "non aggressione" quanto quello di "legittima difesa", sostenendo economicamente, politicamente e con aiuti militari la parte attaccata. Pur non disconoscendo le evidenti difficoltà registrate dall'inizio della guerra rispetto ad una soluzione diplomatica della crisi, anche in sede ONU, il Senatore ha sostenuto come tale soluzione possa e debba ancora essere ricercata; tuttavia affermando, contestualmente, l'esigenza diproseguire a supportare l'Ucraina (onde non comprometterne, non più di tanto almeno, la forza negoziale rispetto alla Russia). In questo quadro, il supporto a Kiev dovrebbe assumere anche il significato di un sostegno ad un Paese il cui sistema istituzionale è impostato (pur se "in modo imperfetto") in base ai princìpi della *Rule of Law*, laddove il sistema russo sembra negare tali princìpi sia nella gestione dei suoi affari interni che nella conduzione della sua politica estera.

L'ambasciatore Björklund si è viceversa concentrato sugli effetti del conflitto, mettendone in evidenza alcuni dei principali impatti politici, economici e securitari di carattere globale ma soprattutto regionale, guardando specialmente al contesto europeo e, all'interno di questo, al suo Paese in particolare. L'intervento ha chiarito come sia cambiata la percezione della sicurezza europea da parte svedese a seguito dell'inizio delle ostilità militari fra Mosca e Kiev. L'Ambasciatore ha sottolineato come l'attacco russo all'Ucraina abbia contribuito in modo dirimente ad orientare l'opinione pubblica e la classe politica svedesi verso l'adesione alla NATO, ufficialmente sancita, dopo un processo durato quasi due anni e non privo di ostacoli e fasi di rallentamento, nel marzo 2024 - quando la Svezia è divenuta il 32° Stato membro dell'Alleanza (così seguendo l'adesione della Finlandia, avvenuta, per ragioni simili, l'anno precedente). Di fronte all'uso "non provocato" della forza da parte della Russia, ha sostenuto l'Ambasciatore, e alle tesi poco credibili veicolate da Mosca (anche tramite una sistematica attività di disinformazione) sulle origini e la natura del conflitto, la neutralità politico-militare svedese, risalente al XIX secolo, è stata abbandonata. Ciò al fine di

proteggere più efficacemente la Svezia, ma anche di contribuire fattivamente, tramite programmi di cooperazione mirata nel settore militare, alla difesa degli Stati europei. L'Ambasciatore ha infine posto l'accento sull'esigenza di arrivare, prima che ad una pace "potenzialmente prematura", che rischi di essere poco equa, ad un accordo per "il cessate il fuoco", propedeutico all'avvio di negoziati fra i contendenti e a testare l'effettiva volontà di Mosca di addivenire ad un accordo di pace stabile e duraturo.

D'altra parte, come sottolineato dall'ambasciatore Zazo, proprio la volontà e le intenzioni di Mosca hanno rappresentato, sin dall'inizio della guerra, uno dei fattori più complessi da comprendere rispetto all'intero quadro del conflitto e ai suoi possibili sviluppi. Tutto questo anche in considerazione dell'opacità che ancora caratterizza il sistema russo, inclusa la cerchia di figure più vicine a Vladimir Putin. Secondo Zazo, la rigidità diplomatica mostrata nel corso della crisi dalla Federazione Russa sarebbe dipesa in larga parte dal suo Presidente, che riterrebbe il territorio ucraino, in virtù della sua storia e della sua rilevanza economica e strategica, una pedina irrinunciabile dell'attuale prospettiva geopolitica russa, incline a tendenze espansionistiche in grado di rievocare, pur con le dovute differenze, la politica estera di Mosca in alcune fasi dei due secoli precedenti. Per questo, secondo l'ambasciatore, prima di arrivare a un processo di pace è indispensabile che la leadership russa mostri segnali concreti e inequivocabili di volontà negoziale. Almeno fino ad allora, il sostegno europeo a Kiev non dovrà essere messo in discussione.

Pur incentrando i loro interventi su aspetti differenti, i tre relatori hanno dunque tutti sostenuto, anche se con sfumature diverse, la necessità, da parte europea, di mantenersi pronti a supportare Kiev con appoggi di natura politico-diplomatica e forniture economiche, umanitarie e militari, da modulare a seconda dell'andamento della crisi. Tutto questo, e veniamo al punto chiave del panel, anche alla luce della complessità politica ed economico-commerciale dell'attuale fase delle relazioni transatlantiche, con l'amministrazione Trump che ha mostrato da una parte di voler offrire ai contendenti una via d'uscita diplomatica dalla crisi, dall'altra segnali quanto meno ambivalenti rispetto alla sua volontà di continuare a sostenere convintamente Kiev, manifestando in ogni caso una certa tendenza prospettica a disimpegnarsi, almeno in parte, dalle vicende di sicurezza riguardanti l'Europa.

Sullo sfondo di questa immagine, durante il panel sono emerse alcune significative incognite. Tali interrogativi hanno preso forma soprattutto dal *question time* finale, che ha visto molteplici domande e interventi da parte di ufficiali superiori provenienti non solo da Paesi europei, ma anche da Stati non appartenenti all'Europa, il cui punto di vista è stato, trattandosi peraltro di personale in linea generale emotivamente meno coinvolto dalle vicende legate al conflitto, particolarmente utile ed arricchente ai fini di un confronto fertile, obiettivo e plurale (…difficile però, per la platea come per i relatori, restare emotivamente indifferenti al momento di un intervento giunto da un ufficiale ucraino…).

Le incognite emerse hanno riguardato non solo e non tanto la volontà del Regno Unito e dei principali Stati membri dell'UE di continuare a sostenere Kiev (volontà ribadita di recente anche dal rifiuto di revocare le sanzioni economiche verso Mosca), ma anche e soprattutto le modalità tramite cui questo sostegno dovrà concretizzarsi, per giunta in una fase in cui le posizioni di Washington e quelle europee sui termini di una possibile pace potrebbero non coincidere. Laddove su questi termini potrebbe influire, almeno in parte o indirettamente, anche un appoggio cinese verso Mosca, e mentre discordanze potrebbero emergere in seno agli stessi Stati europei - come a es. accaduto di recente in merito al tipo di mandato e alla stessa opportunità di una ipotetica missione internazionale di sostegno (eventualmente sotto egida ONU) al processo di pace partecipata anche da forze militari europee (evenienza verso cui Mosca per parte sua ha mostrato, sinora, scarso gradimento). Assunto peraltro che il sostegno in questione implica tanto complessi aspetti operativi e di coordinamento, quanto, soprattutto, fondamentali decisioni di natura politico-strategica − riguardanti, già a breve termine e poi quando Mosca e Kiev dovessero effettivamente raggiungere un accordo di pace (non facile anche alla luce della tregua molto parziale faticosamente raggiunta lo scorso 25 marzo), anche quale attore, o quali attori, dovranno agevolarne e verificarne la stabilità in rapporto agli interessi europei (facendolo possibilmente secondo una voce direttrice sufficientemente unitaria). Tutto ciò peraltro mentre l'UE dovrà iniziare, in conformità al piano *Readiness 2030* e al Libro Bianco sulla Difesa europea, ingenti investimenti per il

riarmo dei singoli Paesi membri e per una maggiore integrazione ed autonomia nell'industria militare, e più in generale ripensare, alla luce dell'assertività russa e della maggiore competizione politico-militare che si sta profilando nel sistema internazionale, la sua intera politica di difesa. Il che richiederà di trovare convergenze sufficienti, sia fra i principali Stati membri che al loro interno, circa quale modello potrà risultare in tal senso coerente ed effettivamente percorribile ‑ le ipotesi in campo spaziano da meccanismi di cooperazione rafforzata che consentano di procedere, sul piano delle missioni operative come su quello dell'integrazione dei sistemi d'arma e delle forze, anche soltanto con quei Paesi che vogliano farlo (pur coordinati in entrambi i casi da un livello sovraordinato a quelli nazionali), all'istituzione di una vera e propria forza di difesa comune permanente, del tutto distinta e autonoma dai livelli nazionali (difficile però da immaginare senza una revisione dei Trattati vigenti, ovvero almeno a breve e medio termine).

Evidente in ogni caso come tutto ciò possa rappresentare un *puzzle* di non facile soluzione, in grado di porre sfide quasi esistenziali rispetto all'identità e al ruolo dell'Unione Europea e della NATO, così come in merito ai loro rapporti e a quelli fra l'UE e il Regno Unito e, più in generale, alle stesse relazioni fra le due sponde dell'Atlantico. L'auspicio è in ogni caso che il panel, anche lasciando emergere questi interrogativi, abbia sollevato spunti di riflessione utili al dibattito su una crisi in corso ormai da oltre tre anni; la cui fine, per quanto ancora incerta, e pur nella chiara consapevolezza di chi sia stato ad iniziarla, dovrà prima o poi essere raggiunta.

FEDERICO GIROTTI

Dottore in Economia e Laureando Magistrale in Scienze della Pace e della Cooperazione Internazionale presso Università Pontificia Lateranense

WARGAME "MEDITERRANEO" AL CASD

Negli ultimi anni, il CASD è diventato il principale hub italiano per il wargaming della Difesa, con l'obiettivo di rafforzare la formazione del capitale umano, strategic foresight e capacità di gestione delle crisi.

Il fenomeno di valorizzazione accademica del wargaming non è recente; il contributo scientifico al serious gaming risale almeno agli anni '50, con professionisti accademici impegnati nello studio dei processi decisionali. Ad esempio, la Carnegie Mellon University è stata una delle prime istituzioni universitarie a sviluppare Business Strategy Games, ispirandosi ai wargame del U.S. Naval War College. Successivamente, il Center for International Studies del MIT contribuì a ulteriori innovazioni, in particolare con l'applicazione delle variabili sociali come quella politica, psicologica ed economica. In un approccio sperimentale al wargaming, vennero successivamente eliminati vincoli prestabiliti di gioco per rendere l'esperienza più realistica e privilegiare la decisione collettiva. Nel tempo, la strutturazione dei wargame è diventata sempre più articolata e applicabile in molteplici contesti con fini ludici quanto didattici. A livello nazionale, dal 2023 il Centro Alti Studi per la Difesa ha iniziato a promuovere l'adozione del wargame all'interno del proprio programma accademico, valorizzandolo come strumento interdisciplinare di ricerca e formazione.

Wargame "Mediterraneo"

Nella prima settimana di dicembre 2024, il CASD ha organizzato un'importante applicazione pratica del wargame, attraverso l'evento 'Mediterraneo: Science & Defence Industry'. Questa occasione ha rappresentato un momento di confronto nell'ambito della strategia e della sicurezza internazionale, rivolto ai frequentatori della 76ª sessione di studio dell'Istituto Alti Studi Difesa (IASD). Tra i partecipanti figuravano Ufficiali Generali e Superiori di tutte le Forze Armate, dirigenti e funzionari di Corpi Armati dello Stato, rappresentanti di vari ministeri, industrie e organizzazioni nel settore della difesa.

Questo primo wargame condotto dallo IASD assieme alla Direzione Alta Formazione e Ricerca (DIAFR) e sviluppato dal Prof. Andrea Bernardi, è stato appositamente progettato con il contributo di esperti per permettere una combinazione efficace tra esperienza ludica e meccaniche realistiche relative ai processi industriali e di difesa nell'area designata del Mediterraneo. Il wargame, preceduto da seminari accademici, è iniziato il 3 dicembre impiegando tre giorni per arrivare alla sua conclusione. È stato supportato da un team di esperti e facilitatori, svolgendosi in uno scenario geopolitico realistico che ha incluso eventi come la crisi del regime siriano, le politiche estere statunitensi e i progetti industriali comuni europei. La simulazione si è focalizzata sull'area del "Mediterraneo allargato" ed è stata concepita con l'obiettivo di approfondire tematiche chiave quali la sicurezza internazionale e lo sviluppo industriale della difesa europea. Non meno importante, l'esercizio pratico ha permesso lo sviluppo di quelle soft skills fondamentali come il decision making in condizioni di ambiguità e stress, la negoziazione in situazioni di crisi e la comunicazione strategica.

Funzionamento di Mediterraneo

Il Wargame Mediterraneo si è concentrato sulle dinamiche industriali e strategiche all'interno di un orizzonte temporale simulato in dieci–vent'anni, strutturato in sei turni. I settanta partecipanti, suddivisi in più squadre nazionali, rappresentavano i principali paesi europei, insieme agli stati nordafricani, alla Turchia, alla Russia e alla Cina. Le squadre erano

organizzate in due blocchi: quello blu, comprendente le nazioni europee, e quello rosso, rappresentato da Russia e Cina, più gli altri paesi all'interno di un'area grigia. I giocatori, con interessi divergenti, dovevano bilanciare competizione e cooperazione per raggiungere obiettivi nazionali in ambito scientifico, tecnologico ed economico.

Il gioco prevedeva l'uso di risorse finanziarie e scientifiche per condurre azioni diplomatiche, economiche, legali, militari e industriali. Le nazioni europee investivano risorse nello sviluppo dell'industria della difesa comune, cercando di conciliare interessi nazionali e obiettivi collettivi. Dal lato opposto, Russia e Cina perseguivano strategie spesso in contrasto con quelle dei paesi blu. Gli stati mediterranei grigi, invece, dovevano conseguire i rispettivi obiettivi negoziando con gli attori rossi, blu e gli altri attori grigi.

L'intera simulazione ha avuto come riferimento visivo una mappa del Mediterraneo Allargato creata appositamente, affiancata da una plancia per monitorare l'integrazione industriale europea e da un influence track. Quest'ultimo era necessario per misurare l'equilibrio di soft power tra i blocchi blu e rosso e si modificava in base alle azioni degli stati, rappresentando la loro influenza. La vittoria, infatti, dipendeva dall'avvio di progetti comuni di difesa e dal raggiungimento degli obiettivi nazionali, determinando il successo strategico complessivo.

Considerazioni finali

L'osservazione dei risultati, insieme al feedback dei giocatori, ha evidenziato come il Laboratorio Wargaming della Difesa abbia generato un impatto significativo su tre livelli principali. Ha contribuito alla diffusione della cultura del wargaming tra i partecipanti e le istituzioni coinvolte, stimolando il pensiero critico e l'approccio interdisciplinare. Ha permesso di riflettere sulle dinamiche di ottimizzazione delle risorse e pianificazione strategica in settori industriali. Mentre a livello sociale e interpersonale, ha stimolato quelle competenze trasversali utili nelle dinamiche di gruppo, come il problem solving, il decision making, l'analisi strategica e le capacità negoziali. I partecipanti hanno riconosciuto il wargame come un mezzo efficace e coinvolgente per affrontare tematiche complesse, come il ruolo strategico del Mediterraneo e l'integrazione della difesa europea, evidenziando un legame diretto tra l'esperienza ludica e l'apprendimento formativo. Inoltre, i fattori di cooperazione e di comunicazione efficace tra i gruppi sono stati indispensabili per il successo finale. Questi hanno facilitato il coordinamento e la negoziazione tra i giocatori, soprattutto all'interno di un lasso di tempo limitato che rappresentava una parte della sfida per i partecipanti.

Infine, l'evento ha confermato il valore formativo e analitico del wargaming, potenziando la cooperazione istituzionale e delineando nuove prospettive per il CASD come hub di riferimento nello studio e nella diffusione del wargame nella Difesa.

La conferenza si è conclusa con una riflessione sul futuro della democrazia americana e sulle sue implicazioni globali. Giannetti ha posto così una domanda provocatoria riguardo a quale sarà il futuro dell'Unione Europea in relazione agli shock esterni che potrebbero derivare dalla politica estera di Trump, suggerendo che la risposta dell'UE potrebbe richiedere un ripensamento delle proprie politiche di difesa e cooperazione internazionale.

RECENSIONI

MICHELE VELLANO, ALBERTO MIGLIO (a cura di)

SICUREZZA E DIFESA COMUNE DELL'UNIONE EUROPEA

Ed. Wolters Kluwer, Milano 2023, pp. 432
con Prefazione del GEN. C.A. Francesco Paolo Figliuolo
ISBN 978 8813379834

Il volume *Sicurezza e difesa comune dell'Unione europea* affronta in modo organico il tema della Politica di Sicurezza e Difesa Comune (PSDC), parte della Politica Estera e di Sicurezza Comune (PESC). Questa politica, tra le più strategiche dell'azione esterna dell'Unione europea (UE), mira a promuovere la pace, garantire la sicurezza internazionale e rafforzare la cooperazione tra gli Stati membri.

La pubblicazione arriva in un momento cruciale, segnato dall'invasione russa dell'Ucraina che ha riportato la guerra in Europa, spingendo l'UE a intraprendere azioni senza precedenti, come il finanziamento della fornitura di armamenti a uno Stato terzo. Il volume risponde così alla crescente attenzione accademica verso la PSDC, colmando una lacuna nella letteratura esistente. Il libro fornisce infatti una visione integrata e aggiornata della PSDC, trattando aspetti istituzionali giuridici, operativi e strategici. La capacità di collegare il dibattito accademico alle sfide geopolitiche attuali è uno dei punti di forza del volume, che offre chiavi di lettura utili per comprendere il ruolo dell'UE nel panorama internazionale.

Il volume si articola in tre parti, che guidano il lettore dai fondamenti istituzionali fino agli sviluppi operativi e tecnico-strategici.

La prima parte del volume esplora i profili istituzionali della PSDC, analizzando l'evoluzione normativa, il ruolo delle istituzioni dell'UE e le dinamiche di *governance* multilivello. Il capitolo iniziale, curato del Prof. Greppi, introduce il quadro storico e giuridico della PESC e della PSDC, evidenziando il ruolo delle istituzioni europee e degli Stati membri. Il Prof. Vellano, nel capitolo secondo, approfondisce gli aspetti istituzionali della PSDC, con particolare attenzione al Servizio Europeo per l'Azione Esterna e all'Agenzia Europea per la Difesa, sottolineandone il contributo operativo. Il lavoro del Prof. Miglio esamina poi il meccanismo della PESCO, evidenziandone il ruolo nell'integrazione differenziata degli Stati membri. Segue un capitolo dedicato al mercato unico della difesa, a cura del Prof. Calzolari. La parte si conclude con il contributo del Prof. Saluzzo, che esplora i rapporti della PSDC con le altre politiche esterne dell'UE.

La parte seconda è dedicata alla componente operativa della PSDC. Il Dott. Grossio distingue fra missioni civili, missioni militari e operazioni militari, analizzandone le basi giuridiche, la pianificazione strategica e la condotta. La collaborazione tra UE con ONU e NATO viene trattata dalla Prof.ssa Poli e dal Dott. Minervini, evidenziandone le criticità operative. La Prof.ssa Pineschi approfondisce il diritto internazionale applicabile alle operazioni militari dell'UE, specificatamente su diritti umani e diritto umanitario. Infine, il contributo del Prof.

Spagnolo esamina le responsabilità internazionali nelle operazioni UE, con un focus sugli *Status of Forces Agreements* (SOFA) e sul caso studio dell'operazione ATALANTA.

La terza parte affronta temi emergenti selezionati. La Dott.ssa Perotto analizza la cooperazione tra gli Stati membri al di fuori del quadro formale della PSDC, come gli EU Battlegroups e l'Eurocorpo. La Dott.ssa Chiussi Curzi tratta le sfide normative e operative legate alla cybersicurezza, con un focus sulla lotta alla disinformazione e sul coordinamento tra le agenzie dell'Unione in materia e la NATO. Il lavoro del Dott. Mauri si sofferma invece sulle minacce spaziali, concentrandosi sulle armi anti-satellite. La Prof.ssa Cellerino esplora il regime per il controllo delle esportazioni di beni a duplice uso, bilanciando interessi di sicurezza e politica commerciale. Nel suo contributo poi, il Dott. Rosanò tratta la cooperazione post-Brexit tra UE e Regno Unito nel settore di sicurezza e difesa. La parte si conclude con due casi studio: il contributo del Prof. Spagnolo e del Contrammiraglio Turchetto circa l'operazione navale EUNAVFOR MED IRINI mette in luce il ruolo innovativo dell'UE come attore di sicurezza marittima *sui generis;* il Dott. Grossio e il Generale di Brigata De Sio trattano invece la missione di addestramento EUTM Somalia nel rafforzare le forze armate somale, con un'attenzione alla collaborazione sul campo con le istituzioni locali somale.

Di rilievo per la collocazione del volume è certamente l'integrazione di prospettive accademiche e militari, che arricchiscono significativamente il dibattito sulla PSDC. La sinergia fra ufficiali delle Forze Armate italiane e studiosi di diritto internazionale e dell'UE consente di collegare gli sviluppi istituzionali e normativi della PSDC alle sfide emergenti dai contesti operativi, fornendo un quadro utile tanto agli studiosi quanto ai decisori politici e agli operatori del settore. In questo senso, va altresì ricordata la collaborazione tra l'Università degli Studi di Torino e il Centro Alti Studi per la Difesa (CASD), all'origine dell'opera. Questo impegno congiunto non solo amplia l'orizzonte delle analisi condotte, ma contribuisce a rafforzare il legame tra accademia e pratica operativa. L'approccio olistico del presente volume, inoltre, offre una chiave di lettura integrata che risulta particolarmente utile nell'attuale panorama geopolitico.

Un ulteriore elemento di forza è la tempestività del volume rispetto agli sviluppi geopolitici più recenti, come la guerra in Ucraina e l'attuazione della Bussola Strategica dell'UE. L'analisi è arricchita dall'inclusione di temi solitamente trascurati dalla letteratura, come le implicazioni operative. Inoltre, la capacità di collegare in modo coerente i profili di diritto dell'UE e di diritto internazionale amplia ulteriormente il raggio d'azione del volume.

Dunque, il presente testo costituisce certamente un'opera di riferimento per diversi ambiti professionali e accademici. La sua capacità di combinare rigore accademico, prospettive operative e attenzione alle sfide geopolitiche lo rende, *inter alia*, rilevante come strumento didattico nell'ambito di master *post-lauream*, quali il Master in Studi Internazionali Strategico-Militari (ISSMI) e il Master in Diritto Internazionale Umanitario e dei Conflitti Armati (DIUCA).

Fornendo un'analisi integrata e sistematica della PSDC, il volume offre chiavi di lettura necessarie per interpretare i cambiamenti in corso nel panorama internazionale. La continua evoluzione di alcuni ambiti trattati, come la cybersicurezza, suggeriscono che molte questioni resteranno centrali nei futuri dibattiti accademici e politici. Questo carattere dinamico conferma che tale opera non solo fotografa lo stato attuale della PSDC, ma getta anche le basi per ulteriori lavori di ricerca su questioni fondamentali per il futuro dell'Unione. Inoltre, la qualità complessiva e il suo contributo al dibattito sulla sicurezza e difesa dell'UE lo rendono un riferimento indispensabile, in grado di stimolare ulteriori riflessioni e ricerche in un campo sempre più cruciale per il futuro dell'Unione Europea.

Cecilia Nota

Margherita Penna

STRATEGIC LEADERSHIP JOURNAL
Challenges for Geopolitics and Organizational Development

CODICE ETICO

"STRATEGIC LEADERSHIP JOURNAL. Challenges for Geopolitics and Organizational Development" (di seguito SLJ) è una rivista peer-reviewed che si ispira al codice etico delle pubblicazioni elaborato dal COPE (Commitee on Publication Ethics). Pertanto assume tutte le decisioni necessarie contro eventuali frodi che si possano verificare nel corso della pub- blicazione di un lavoro sulla rivista stessa. Le parti coinvolte - Organi istituzionali, Referee e Autori - devono conoscere e condividere i seguenti requisiti etici.

DOVERI DEGLI ORGANI ISTITUZIONALI DI SLJ

1. Compete alla Direzione, con il supporto del Comitato Scientifico e del Comitato Editoriale, la scelta finale degli articoli che saranno pubblicati in SLJ, effettuata tra i contributi pervenuti in Redazione, sulla base delle risultanze della peer-review.
2. La scelta viene effettuata esclusivamente sulla base del contenuto scientifico e intellettuale e senza discriminazioni di razza, genere, orientamento sessuale, religione, origine etnica, cittadinanza, orientamento politico degli autori.
3. Gli articoli scelti verranno sottoposti alla valutazione di Revisori e la loro accettazione è subordinata all'esecuzione di eventuali modifiche richieste e al parere conclusivo della Direzione.
4. Il Direttore Scientifico e i componenti del Comitato Scientifico e del Comitato Editoriale si impegnano a non rivelare informazioni sugli articoli proposti dagli autori e pervenuti in Redazione, nonché sugli esiti dei referaggi, verso terzi estranei alla composizione degli organi di SLJ.
5. Le comunicazioni concernenti il contributo elaborato possono intercorrere con l'autore o con i valutatori ai soli fini del referaggio.
6. Il Direttore Scientifico, i componenti del Comitato Scientifico, del Comitato Editoriale e i valutatori si impegnano a non usare in ricerche proprie, senza esplicito consenso dell'autore, i contenuti di un articolo proposto per la pubblicazione/ revisione.
7. Se alcuno degli organi di SLJ rileva o riceve segnalazioni in merito a eventuali conflitti di interessi o plagio in un articolo pubblicato ne darà tempestiva comunicazione alla Direzione.
8. SLJ rende noto nel proprio colophon i nomi del Direttore Responsabile e dei componenti del Comitato Scientifico, del Comitato Editoriale e della Redazione.

REFEREE

1. Gli articoli pubblicati sono soggetti alla valutazione dei referee secondo il sistema di peer-review c.d. "double-blind" (I revisori non conoscono gli autori e gli autori non sanno chi sono i revisori).
2. Attraverso la procedura di peer-review (double blind) i referee assistono gli Organi di SLJ nell'assumere decisioni sugli articoli proposti ed inoltre possono suggerire all'autore emendamenti tesi a migliorare il proprio contributo.
3. Qualora i referee non si sentano adeguati al compito proposto o sappiano di non poter procedere alla lettura dei lavori nei tempi richiesti sono tenuti a comunicarlo tempestivamente alla Redazione.
4. Ciascun contributo pubblicato in SLJ è sottoposto al giudizio di referee.
5. I referee sono selezionati dalla Direzione o dal Comitato Scientifico o dal Comitato Editoriale - in considerazione del settore scientifico-disciplinare cui risulta riferibile il saggio da valutare - tra professori, ricercatori e studiosi, in ruolo o in quiescenza, ovvero esperti particolarmente qualificati nelle singole materie o discipline.
6. Il giudizio del referee viene comunicato all'autore in forma anonima.
7. Il contenuto dei referaggi è riservato, fatto salvo per le informazioni e comunicazioni eventualmente richieste dai competenti organi di valutazione del sistema universitario nazionale.

8. Il referaggio deve avere ad oggetto il contenuto dell'articolo, i risultati raggiunti, il metodo seguito, la chiarezza dell'esposizione.
9. I referee segnalano alla Redazione eventuali sostanziali somiglianze o sovrapposizioni del testo ricevuto con altre opere a loro note.
10. I referee si impegnano a considerare riservate tutte le informazioni o indicazioni ottenute durante il processo di peer-review e a non discutere i testi con altre persone senza esplicita autorizzazione della Direzione.
11. Le revisioni dei referee devono essere ispirate da criteri di oggettività e imparzialità, in un'ottica di critica costruttiva. Il feedback che forniscono deve essere d'aiuto agli autori per migliorare la qualità del manoscritto, fatta salva la possibilità di giudicare non pubblicabile l'articolo stesso.
12. In considerazione del particolare prestigio o rilevanza di taluni autori, il Direttore Responsabile e il Direttore Scientifico possono, dopo essersi consultati, decidere di pubblicare un articolo senza che questo sia stato sottoposto a referaggio. In tal caso, l'articolo sarà edito con la dicitura "su invito della Direzione".

AUTORI

1. Gli articoli devono essere frutto di ricerche originali degli autori. Dagli articoli deve potersi ricavare il metodo seguito e i risultati raggiunti.
2. Se l'articolo è il frutto del contributo di più autori, essi vanno tutti riconosciuti quali coautori e l'articolo, qualora pubblicato, recherà tutti i nominativi dei singoli autori.
3. Gli autori non devono inviare a SLJ articoli nella sostanza uguali ad altri già pubblicati da loro stessi o da altri.
4. Gli autori, nell'inviare i loro contributi per la pubblicazione in SLJ, si impegnano a non sottoporre gli stessi ad altre riviste ai fini di pubblicazione in Italia e all'estero.
5. Gli autori devono citare ogni fonte, propria o altrui, che sia automaticamente rilevante rispetto al lavoro. Ogni genere di dato, formulazione, figura o idea presa da altri deve essere appropriatamente citata e non può mai essere spacciata come propria.
6. Nel caso in cui gli autori riscontrino un errore all'interno di un manoscritto inviato in valutazione, devono immediatamente informare la Redazione e richiedere eventuali correzioni o la ritrattazione di precedenti affermazioni.
7. Nella redazione degli articoli da proporre per la pubblicazione, gli autori devono attenersi a quanto previsto nelle Norme redazionali consultabili al seguente link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

ELENCO REFEREE

Dr. Antinori Arjie, Dr. Artoni Maurizio, Dr.ssa Astarita Claudia, Prof. Bagarani Massimo, Dr. Baggiani Gregorio, Dr. Baldelli Pietro, Dr. Balduccini Mauro, Dr. Batacchi Pietro, Dr. Beccaro Andrea, Prof. Bernardi Andrea, Prof. Battistelli Fabrizio, Dr.ssa Boldrini Chiara, Dr. Bongioanni Carlo, Dr.ssa Bonomo Silvia, Dott. Borsani Davide, Dr. Bressan Matteo, Dr. Bruschi Luigi, Dr. Elio Calcagno, Dr.ssa Carallo Gemma, Dr. Catalano Claudio, Dr.ssa Citossi Francesca, Dr.ssa Ciampi Annalisa, Dr. Cochi Marco, Dr.ssa Coco Antonella, Prof. Colacino Nicola, Dr. Colantonio Antonio, Dr. Coticchia Fabrizio, Dr.ssa Di Chio Raffaella, Dr. Di Leo Alessio, Dr. Di Liddo Marco, Dr. Dian Matteo, Dr. Donelli Federico, Prof.ssa Eboli Valeria, Dr. Fasola Nicolò, Dr. Felician Beccari Stefano, Dr.ssa Feola Annamaria, Dr. Fontana Simone, Prof. Foresti Gian Luca, Dr. Frappi Carlo, Prof. Gaspari Francesco, Prof. Gennaro Alessandro, Dr.ssa Gravina Rossana, Dr. Grazioso Andrea, Prof.ssa Icolari Maria Assunta, Dr. Indeo Fabio, Prof.ssa Irrera Daniela, Prof. La Bella Simone, Dr.ssa La Regina Veronica, Dr.ssa La Rosa Anna, Dr. Locatelli Andrea, Prof. Lombardi Marco, Dr. Macrì Paolo, Dr. Marcovina Marco, Dr. Marcuzzi Stefano, Dr. Marone, Francesco, Dr. Marrone Alessandro, Dr. Marsili Marco, Dr.ssa Martini Francesca, Prof. Martini Matteo, Dr. Mastrolia Nunziante, Dr.ssa Mauro Marlene, Prof.ssa Melcangi Alessia, Dr. Mele Stefano, Prof. Merlo Alessio, Dr. Napolitano Paolo, Dr. Negri Michele, Dr.ssa Nocerino Wanda, Dr.ssa Palloni Elena, Dr. Pasquazzi Simone, Dr. Pastori Gianluca, Dr. Pedde Nicola, Prof. Peluso Pasquale, Prof. Pezzimenti Rocco, Dr. Pezzoli Carlo, Dr. Pignatti Matteo, Dr.ssa Pistoia Emanuela, Dr. Pompei Alessandro, Dr. Rizzolo Ivan, Prof.ssa Rossi Marzia, Dr.ssa Rutigliano Stefania, Dr. Ruzza Stefano, Dr. Stilo Alessio, Dr. Striuli Lorenzo, Dr.ssa Trenta Elisabetta, Dr.ssa Triggiano Annalisa, Prof. Ugolini Francesco, Prof. Ursi Riccardo, Prof. Vagnini Alessandro, Prof. Valentini Tommaso, Dr. Vasaturo Giulio, Dr. Veca Mario, Dr. Vergura Silvano, Dr. Verzotto Davide, Dr. Viola Paolo, Dr. Zacchei Alessandro, Dr.ssa Zawadzka Sylwia.

ALCUNE INFORMAZIONI UTILI

Al fine di proporre un articolo per la pubblicazione in SLJ, è necessario:

- inviare il file (Word o Pages) del testo al seguente indirizzo di posta elettronica: redazione.slj@gmail.com;
- accludere, con file separato, un breve *abstract* del proprio curriculum (massimo 6 righe);
- accludere, con file separati, eventuali immagini, corredate da apposita didascalia.

Gli articoli sono soggetti a *Peer Review - Double Blind*.

Nel redigere l'articolo, gli Autori sono pregati di seguire le regole metodologico-redazionali (*desiderata*), consultabili al seguente link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

***

Coloro i quali desiderino ricevere SLJ in formato pdf al proprio indirizzo e-mail possono indicare il nominativo e l'indirizzo di posta elettronica alla presente casella, così da poter essere inseriti nella "mailing list": *redazione.slj@gmail.com*

***

In order to submit a paper for SLJ, it is necessary to:

- Send the Word or Pages file to the following email address: redazione.slj@gmail.com;
- Attach, as a separate file, a brief abstract of your curriculum (maximum 6 lines);
- Attach any images separately, accompanied by a suitable caption.

Authors submitting articles are hereby informed that their paper will undergo *Peer Review - Double Blind*.

Authors are kindly requested to adhere to the following methodological and editorial guidelines (desiderata), downloadable from the following link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

***

Readers who wish to receive a PDF of the SLJ at their own email address are kindly requested to subscribe to the following mailing list: *redazione.slj@gmail.com*

Stampato dalla Tipografia del
Centro Alti Studi Difesa

CENTRO ALTI STUDI DIFESA

SCUOLA SUPERIORE UNIVERSITARIA

LA NOSTRA MISSION
Sviluppare una leadership etica, equa e responsabile al servizio della comunità, nazionale e internazionale, attraverso una formazione d'eccellenza che potenzi talenti e competenze, valorizzi le differenze e costruisca nuova conoscenza mediante la ricerca e l'innovazione.

LA NOSTRA VISION
Costituire un punto di riferimento nel panorama nazionale e internazionale e divenire snodo vitale nella rete delle relazioni strategiche, per far fronte con successo al complesso scenario del mondo attuale.

STRATEGIC LEADERSHIP

JOURNAL