CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Wanda Nocerino

"Il sostegno delle idee innovative: Proposte volte a favorire la contaminazione del mainstream di pensiero militare attraverso contributi di esperti e cultori di settori complementari o anche apparentemente distanti dalla difesa al fine di sintetizzare la più pregnante e pervasiva essenza delle nuove tecnologie mentre ne è in corso la maturazione e si approssima il momento di trarne il massimo vantaggio competitivo"

(AS-SMA-07)

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e *cyber security*; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore della Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

Wanda Nocerino

"Il sostegno delle idee innovative: Proposte volte a favorire la contaminazione del mainstream di pensiero militare attraverso contributi di esperti e cultori di settori complementari o anche apparentemente distanti dalla difesa al fine di sintetizzare la più pregnante e pervasiva essenza delle nuove tecnologie mentre ne è in corso la maturazione e si approssima il momento di trarne il massimo vantaggio competitivo"

(AS-SMA-07)

"Il sostegno delle idee innovative: Proposte volte a favorire la contaminazione del mainstream di pensiero militare attraverso contributi di esperti e cultori di settori complementari o anche apparentemente distanti dalla difesa al fine di sintetizzare la più pregnante e pervasiva essenza delle nuove tecnologie mentre ne è in corso la maturazione e si approssima il momento di trarne il massimo vantaggio competitivo"

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.
Questo volume è stato curato dall'Ufficio Studi, Analisi e Innovazione dell'IRAD**.**

Direttore
Col. c. (li) s. SM Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Revisione e coordinamento
C.V. Massimo GARDINI – S.Ten. Elena PICCHI – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra

Autrice
Wanda Nocerino

Stampato dalla Tipografia del Centro Alti Studi per la Difesa

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a dicembre 2023

ISBN 979-12-5515-060-2

INDICE

SOMMARIO

Riuscire a prevedere gli scenari futuri per stare al passo con la rapida evoluzione morfologica delle minacce alla sicurezza e all'integrità della Repubblica a ogni suo livello (sociale, economico, politico, militare, informativo, informatico, ecc.) e in ogni sua dimensione (fisica, virtuale, cognitiva), impone di pensare al futuro in maniera ultronea agli schemi "tradizionali" che – seppur validi per affrontare le sempre attuali minacce convenzionali – vanno integrati e contaminati, scrutinando le idee innovative di campi estranei al contesto militare, con lo scopo di cogliere le potenzialità inespresse o "limitate" dal fine civile che talvolta le animano.

In questo contesto, la presente ricerca si propone l'obiettivo 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[1] – con un approccio "sistemico" e integrato.

Conviene immediatamente precisare che il tema della capacità informativa, intesa come la «capacità di acquisire, proteggere e processare la mole di informazioni necessarie per il conseguimento di una più approfondita conoscenza e un maggiore apprezzamento delle situazioni» (*Documento programmatico pluriennale della Difesa per il triennio 2022-2024,* Ed. 2022, 40), sembra tangere il sistema Difesa senza incidervi in maniera significativa in considerazione della sua intrinseca "staticità".

Nella stessa misura, le criticità e i dubbi che investono il tema sembrano interessare il mondo giuridico solo "indirettamente", in quanto l'attività informativa è tradizionalmente posta in una "zona" collocata al margine del procedimento atto a rispondere e reprimere l'offesa.

Ebbene, in un contesto "sistemico" nel quale sono oggi chiamati a far parte le componenti dei diversi settori della società (civile e militare), questa prospettiva appare "miope" perché non vede come la neutralizzazione della minaccia – che passa inevitabilmente attraverso la raccolta di informazioni utili al fine di disporre di una completa *Situational Awareness* su ciò che accade nelle aree di interesse – rappresenti un momento

[1] 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.

indispensabile per il raggiungimento degli obiettivi propri della Difesa (cfr. *Strategia di Sicurezza e Difesa per il Mediterraneo – Ed. 2022*).

Precisamente, allo stato dell'arte, a fronte di una minaccia c.d. "liquida"[2] e della sfumata distinzione tra esigenze di difesa e sicurezza, «occorre ripensare il modo di affrontare il confronto nella dimensione militare» (*Documento programmatico pluriennale della Difesa per il triennio 2022-2024,* 36), sviluppando nuove capacità e metodologie per rispondere alle sfide dell'era digitale.

In quest'ottica, al fine di adeguare il tradizionale impiego delle Forze armate alle nuove minacce, emerge la necessità che la Difesa debba rispondere sfruttando la capacità di acquisire e processare le informazioni per garantire una maggiore consapevolezza di ciò che accade nelle aree di interesse, in modo da ottimizzare le risorse disponibili ed efficientare il sistema attraverso un intervento "mirato" (c.d. efficienza sistemica)[3].

Sicuramente, l'utilizzo delle nuove tecnologie risulta un fattore dirimente per ottenere un vantaggio nell'acquisizione e nell'integrazione dei dati e delle informazioni provenienti dai vari domini operativi (terrestre, marittimo, aereo, spaziale e cibernetico), con lo scopo di gestire al meglio – sotto il profilo della tempestività e dell'accuratezza delle decisioni strategiche – i nuovi scenari di sempre più crescente complessità.

Il riferimento è ai nuovi strumenti di indagine capaci di offrire rilevanza operativa, il cui impiego è neutralizzato e/o circoscritto in nome della tutela degli interessi civili e privati, estranei alle finalità militari appannaggio della Difesa. Si pensi all'attività di captazione e manipolazione da remoto non solo di documenti o *files*, ma addirittura di interi sistemi operativi e/o di gestione di *hardware* collegati al dispositivo oggetto di controllo.

Più in particolare, i non infrequenti attacchi malevoli allo spazio cibernetico che colpiscono procedimenti 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 di diritto internazionale del "*ius in bello*" che vengono in buona sostanza aggirate e la cui assenza determina una disparità di condizioni che per il

---

2 Sul concetto *de quo,* cfr. *Considerazioni preliminari.*

3 Nel documento diffuso dallo Stato Maggiore dell'Esercito, III Reparto Pianificazione Generale, *Il Concetto operativo dell'esercito italiano 2020-2023,* in *www.centrostudiesercito.it,* 2020, 1, si legge: «[...] la sfida che si pone di fronte all'Esercito [è quella di] individuare [...] soluzioni efficaci, sul piano organizzativo e capacitivo, per anticipare e rispondere con successo alle sfide dell'ambiente operativo futuro [...]». Inoltre, nel medesimo documento si legge che nel quadro del paradigma operativo emergente l'Esercito dovrà «[...] sfruttare le opportunità del dominio spaziale [nonchè] incidere nella dimensione cibernetica e informativa]».

sistema Difesa si traduce in un *vulnus* giuridico, fonte di mortificazione del grado di operatività e di efficienza dello Strumento militare.

Può, dunque, sostenersi che il quadro giuridico di riferimento non sembra consentire alla Difesa (soprattutto allorquando si è al di sotto della "soglia di conflitto")[4] di sviluppare adeguatamente le proprie capacità militari per condurre operazioni nel dominio *cyber* attraverso una raccolta di dati e informazioni utili a "mappare" i sistemi potenzialmente oggetto di futuro attacco e ad intercettare gli indicatori della minaccia alla sicurezza nazionale.

Detto in altre parole, alla necessità di assicurare il più elevato livello di *cyber-defence* agli assetti critici nazionali non sembra corrispondere un apparato normativo e regolamentare del tutto adeguato.

Occorre, quindi, interrogarsi sulla 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 certo meno dannosi di quelli esperiti sul campo di battaglia, proprio perché sviluppati in maniera silente e capaci di influenzare le masse fino a consentire la superiorità strategica dell'avversario.

Il presente elaborato si sofferma sugli aspetti or ora delineati, con lo scopo di valorizzare la transizione digitale in chiave efficientista per il sistema Difesa: in questo senso, si ritiene indispensabile garantire un approccio olistico basato sulla contaminazione del *mainstream* militare che può essere avvantaggiato dallo sfruttamento delle potenzialità degli strumenti tecnologici, ancora oggi "represse" e condizionate dai limiti giuridici tipici dell'impiego civile.

Dal punto di vista strutturale, partendo dall'analisi della rinnovata funzione d'*intelligence* militare[5], la ricerca si concentra sui principali attori istituzionali che giocano un ruolo dirimente nel settore "sicurezza", con lo scopo di individuare meccanismi di collaborazione efficienti tra le Forze statuali fondati su un coinvolgimento diretto e immediato del comparto militare, al fine di ottimizzare le procedure di accesso alle informazioni e adeguarsi alle minacce poste in essere da avversari tecnologicamente avanzati (c.d. approccio integrato e multidominio).

---

[4] A tal proposito non può sfuggire come in un modello di rapporto tra Stati che propone una neonata condizione di "*continuum of competition*" – da affrontare, dunque, attraverso l'indispensabile, situazionale ricorso e pieno coinvolgimento di ciascuno dei fattori di potenza statuali (Diplomatico, Militare, Economico, Informativo) ed in necessaria coerenza con il concetto di *multi-domain operation* – la stessa notazione di "sotto-soglia" non appaia più in alcun modo armonica con lo scenario di riferimento.

[5] Come meglio si dirà nel prosieguo (cfr. Cap. I, § *a*), *l'intelligence* militare – lungi dal figurare come un'attività di appannaggio esclusivo dei Servizi di informazione e sicurezza – va intesa come attività di raccolta e gestione delle informazioni utili ad anticipare le minacce all'integrità dello Stato.

Si procede, poi, ad analizzare lo scenario giuridico di riferimento che, come è noto, tende a limitare e comprimere la Difesa (in condizioni "ordinarie") nello sviluppo delle capacità militari: in questo senso, al fine di rendere effettiva la superiorità informativa e cognitiva delle Forze armate, la ricerca si sofferma sulla possibilità di impiegare – a livello militare – i principali e più sofisticati strumenti offerti dalla tecnologia per intercettare gli indicatori delle minacce alla sicurezza nazionale e permetterne un'immediata neutralizzazione.

Una volta affrontato il quadro normativo "interno" e le prospettive futuribili di supporto innovativo, lo studio prosegue soffermandosi sulle forme di condivisione "informativa" esistenti: prendendo atto di un quadro cooperativo non certo all'avanguardia, la ricerca si concentra sulla necessità di migliorare l'assetto vigente alla luce delle nuove e sofisticate tecnologie emergenti con lo scopo di superare le distonie legislative dei singoli Stati coinvolti.

Pur nella consapevolezza di non potersi opporre alle "sfide della modernità" in ragione dei vantaggi offerti dal progresso in termini di risorse di tempo, di uomini, di mezzi e della migliore efficacia ed efficienza delle attività poste a presidio della sicurezza (inter)nazionale, non ci si deve illudere che l'innovazione sia "a costo zero". I rischi che in essa si annidano, infatti, sono molteplici, alcuni peraltro silenti, capaci di minare i valori fondanti il sistema democratico.

Di qui, l'analisi non può che spostarsi sul versante dogmatico, sui principi che regolano l'assetto costituito, individuando gli argini e i confini costituzionali e convenzionali oltre i quali non è possibile (al di fuori dello stato di emergenza) spingersi, arrivando a superare l'idea dell'esistenza di una contrapposizione netta tra "libertà" e "sicurezza", da considerare oramai due facce della stessa medaglia, parimenti meritevoli di tutela per l'ordinamento (Minniti, 2018).

Al termine della ricerca – lo si anticipa – si propende per una ridefinizione del quadro giuridico di riferimento che, in condizioni ordinarie, continua a limitare la Difesa nello sviluppo delle sue capacità militari, e, di conseguenza, per una rivalutazione organizzativa del sistema in chiave interforze e multidominio[6], postulando un approccio sistemico che coinvolga tutte gli altri Strumenti del *national power* (c.d. DIME - Diplomatico, Informativo,

[6] In linea con quanto espresso nel *Documento programmatico pluriennale della Difesa per il triennio 2022-2024,* Ed. 2022, 36. Conviene precisare che «il termine *Multi-Domain* (MD) si è fortemente diffuso negli ultimi anni per lo sforzo profuso da parte di alcuni Paesi, principalmente occidentali, che hanno cercato di codificare il loro approccio alle operazioni militari oltre i domini tradizionali di terra, mare e cielo, al fine di integrare i nuovi domini *Cyber* e Spazio, con conseguente estensione del campo di battaglia, e di fronteggiare le possibili strategie dei potenziali *peer-competitor* che, attraverso l'impiego coordinato di tutti gli strumenti del potere nell'ambito del *continuum of competition*, mirano a negare la possibilità di risposta della controparte e a perseguire incontrastati i propri interessi strategici». Cfr. *Approccio della Difesa alle Operazioni Multidominio*, Ed. 2022, 7.

Militare ed Economico) e promuovendo una sinergia tra settore pubblico e privato, nell'ottica di una risposta più immediata, efficace ed efficiente alle minacce in grado di attentare all'integrità dello Stato.

ABSTRACT

This research aims to identify innovative solutions to support a digital transition for Defense in "efficiency" terms, focusing on the information capacity of military apparatuses to respond to cyber threats.

Precisely, faced with a "liquid threat", the need arises for the Defense to respond by exploiting the ability to acquire and process information to ensure greater awareness of what is happening in the areas of interest, in order to optimize the available resources and make the system through a "targeted" intervention (so-called systemic efficiency).

Certainly, the use of new technologies is a decisive factor in obtaining an advantage in the acquisition and integration of data and information from the various operational domains (land, sea, air, space and cybernetics), with the aim of managing best – in terms of timeliness and accuracy of strategic decisions – the new scenarios of increasing complexity.

However, it should be noted that at the state of the art, the legal framework of reference does not allow the Defense (especially when it is below the conflict threshold) to develop its military capabilities to conduct operations in the cyber domain through a collection of data and information useful for "mapping" the systems potentially subject to future attacks and for intercepting indicators of the threat to national security.

At the end of the research - it is anticipated - the interpreter leans towards a redefinition of the legal framework of reference - which, in the state of the art, limits and compresses the Defense in the development of military capabilities - and, consequently, for an organizational reassessment of the system in a joint key, postulating a systemic approach that involves all the institutions involved and promoting a synergy between the public and private sectors, with a view to a more immediate, effective and efficient response to threats capable of undermining the integrity of the State.

CONSIDERAZIONI PRELIMINARI

La necessaria contaminazione del *mainstream* militare in risposte alle nuove minacce alla sicurezza nazionale

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 inerente al peculiare momento storico-politico e all'attuale evoluzione geo-economica che coinvolge l'assetto planetario in cui la Repubblica italiana riveste un ruolo di primo ordine, in ragione della sua collocazione strategico-territoriale rispetto a uno dei punti geografici più sensibili agli "smottamenti" geo-politici.

Come è dato leggere nella *Strategia di Sicurezza e Difesa per il Mediterraneo* (Ed. 2022, 9), il «pre-requisito per creare un vantaggio decisionale» è rappresentato dalla c.d. "superiorità informativa" che, al pari di quella cognitiva[7], è un *asset* immateriale imprescindibile dell'arsenale della Difesa, in grado di determinare il controllo degli equilibri strategici.

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 attentati alla stabilità della Repubblica che, in molte circostanze, si concretizzano in pericoli in cui vi è un totale appiattimento tra prevenzione e repressione (Cinelli, 2020a, 13).

Si tratta, in buona sostanza, di una "minaccia liquida" (Di Liddo, 2018), 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.

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.

[7] Quella cognitiva rappresenta 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 effetti, il dominio cibernetico – quello che viene definito il «sesto continente» (Caligiuri, 2016, 3) – determina il proliferarsi di minacce alle infrastrutture strategiche del Paese che, seppur immateriali, sono in grado di produrre ricadute assai violente nella realtà fisica, attentando così la sicurezza nazionale[8]. In altre parole, nel rinnovato contesto bellico non sono sempre ravvisabili formazioni militari paragonabili a brigate, divisioni e corpi armati, così come non sono sempre presenti le armi convenzionali quali unici strumenti di lotta all'integrità dello Stato.

Come già sostenuto da Pisano nel 2008, «[l]l tipico campo di battaglia [...] non è più, o lo è solo raramente, quello classico in cui si contrastano le Forze armate di Paesi sovrani avvalendosi della potenza di fuoco e della capacità di manovra nel generale, ancorché non universale, rispetto delle norme del diritto internazionale di guerra»[9].

Sotto altro profilo, nel rinnovato contesto non va sottaciuta la presenza di nuove forze ostili non più identificabili in Stati sovrani ma riconducibili ad "agglomerati di potere", le cui finalità offensive esulano da ragioni ideologico-politiche ma sono legate alla necessità di espandere e rafforzare la propria sfera di influenza. Si tratta di entità non governative capaci di ricoprire un ruolo dirimente negli equilibri delle controversie nazionali, influenzando opinioni, masse e interessi economici, alle volte in maniera ancora più pervasiva dei Governi stessi. Dunque, i moderni attacchi all'integrità del Paese possono essere perpetrati sfruttando una varietà indefinita di assetti e di attori (anche non statali o militari), rendendo particolarmente complessa l'attività di riconoscimento immediato delle minacce, così da esporre la Difesa al rischio di una risposta poco tempestiva e addirittura inefficace. Di conseguenza, il *mainstream* militare è chiamato a mettere in cantiere operazioni caratterizzate da schemi "atipici", strumenti tecnologici che richiedono un elevato grado di competenza tecnica e contraddistinti dall'incalcolabilità di rischi ed effetti collaterali.

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.

---

8 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 uno 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*).

9 Come si legge nel *Dossier* della Camera dei Deputati sulla *Sicurezza e Difesa nello spazio cibernetico,* del 21 dicembre 2017, 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. Le 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».

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 a differenza di quest'ultimo "imponderabili" 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 che non garantisce 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 necessaria 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, la capacità di gestione e analisi delle informazioni si fonda, *in primis,* sulla disponibilità di avvalersi di dati aggiornati, completi e corretti. In tale ottica, appare evidente l'utilità e la potenzialità intrinseca degli strumenti tecnologici d'indagine che, sposati alla causa militare, possono senz'altro essere in grado di coniugare l'attitudine cognitivo-informativa alla funzionalità difensiva di cui sono capaci, anche se *de facto* giuridicamente "sterilizzati". Pertanto un *virus* informatico, "spogliato" della sua "funzione civile" e delle restrizioni giuridiche che inevitabilmente comprimono le sue potenzialità, è sicuramente in grado di assicurare al comparto militare un efficiente sistema di difesa proattivo o di attacco repressivo.

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» (Corte cost., 23 febbraio 2012, n. 40), abbia inglobato nel suo paradigma la tutela della sicurezza 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 ad 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 tutte le sue plurime, 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 rappresenta l'unica metodologia in grado garantire un intervento efficace e tempestivo di contrasto e neutralizzazione delle minacce alla sicurezza nazionale[10]. 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): servono regole di ingaggio per il suo utilizzo e cornici normative per stabilire chi, quando e come può decidere di impiegarla» (*Dossier* della Camera dei Deputati sulla *Sicurezza e Difesa nello spazio cibernetico,* 2017).

Come è stato precisato dalla Ministra Elisabetta Trenta (2018), «[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».

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.

[10] 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 «[l] 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».

CAPITOLO I
LA CENTRALITÀ DELLA CAPACITÀ INFORMATIVA "STRATEGICA" DELLA DIFESA: ASPETTI TECNICO-ORGANIZZATIVI

a. La capacità informativa e le funzioni di *intelligence:* alcuni chiarimenti terminologici

Nell'immaginario collettivo, l'*intelligence"* è considerata feudo esclusivo dei c.d. "Servizi segreti", indissolubilmente legata a specifici organi istituzionali che svolgono la propria attività per salvaguardare la Repubblica da ogni pericolo e minaccia proveniente sia dall'interno sia dall'esterno del Paese[11].

Pur non negando che essa rappresenti un'attività propria dei Servizi di informazione per la sicurezza, l'*intelligence* non può e non deve essere identificata con un "organo" statuale, costituendo tutt'al più un'attività (*rectius:* funzione) che, in via trasversale, accomuna gli apparati istituzionali posti a protezione dello Stato, i quali, nell'adempimento delle proprie funzioni, espletano un autonomo potere di acquisizione e gestione di elementi informativi necessari a prendere le opportune decisioni.

Di qui, al fine di superare le disarmonie linguistiche che possono trarre in inganno gli "addetti ai lavori" – inducendoli a non cogliere appieno le riflessioni che saranno svolte nel prosieguo della ricerca –, occorre preliminarmente analizzare la nozione di *intelligence*, allo scopo di mettere in evidenza l'importanza della c.d. capacità informativa, intesa come la «capacità di acquisire, proteggere e processare la mole di informazioni necessarie per il conseguimento di una più approfondita conoscenza e un maggiore apprezzamento delle situazioni» (*Documento programmatico pluriennale della Difesa per il triennio 2022-2024,* Ed. 2022, 40) che, nell'economia del presente elaborato, rappresenta un elemento "ancillare" per la pianificazione dello Strumento militare e per la condotta delle operazioni e delle missioni della Difesa.

Il termine "*intelligence*" deriva dalla parola latina "*intelligentia*" che, a sua volta, trae origine dal verbo "*intelligere*", che letteralmente vuol dire "intendere, capire, trascegliere"; in quest'ottica, *intelligence* significa conoscenza e cognizione. Più concretamente, può dirsi che l'*intelligence* consista in un procedimento di raccolta ed elaborazione di elementi conoscitivi da parte di organizzazioni complesse (Dell'Anno, 2020, 208), grazie al quale queste ultime sono messe nelle condizioni – su un piano "predittivo" – di formulare previsioni

[11] Ci si riferisce, ad esempio, al Dipartimento delle informazioni per la sicurezza (DIS); all'Agenzia Informazioni e Sicurezza Esterna (AISE), ovvero all'Agenzia Informazioni e Sicurezza Interna (AISI).

in ordine al verificarsi di potenziali future situazioni critiche e – su un piano "preventivo" – di individuare la miglior soluzione possibile a prevenirle o neutralizzarle (Di Bitonto, 2005).

Così ragionando, l'*intelligence* rappresenta uno strumento operativo e analitico di indubbia centralità tanto per la complessa attività di tutela della sicurezza nazionale e delle alleanze internazionali, quanto per il "consapevole" espletamento della politica estera[12].

a.1 L'*intelligence* militare

In base alla ricostruzione offerta, può dirsi che l'obiettivo fisiologico dell'attività *d'intelligence* sia quello di garantire la sicurezza (inter)nazionale attraverso la c.d. superiorità informativa e cognitiva: lo sviluppo e la protezione di una nazione, infatti, dipendono sempre più dalla fruibilità di accesso alle informazioni strategiche e dall'elevato grado di capacità di analizzarle. Tuttavia, se è vero che il concetto di "sicurezza" ha subìto una rapida evoluzione in ragione del mutato contesto geo-politico che l'ordine mondiale si è trovato ad affrontare[13], è altrettanto vero che lo scopo dell'*intelligence* è anche quello di supportare la capacità di difesa militare dello Stato, la sua indipendenza rispetto ad altri soggetti internazionali e la salvaguardia delle istituzioni poste a fondamento della Repubblica.

Come si legge nel documento intitolato "*Approccio della Difesa alle Operazioni Multidominio*", Ed. 2022, 10, «[L]a capacità di gestione della grande mole di dati sarà uno dei parametri fondamentali per determinare il peso di ciascun attore in ambito economico e politico, tanto che si parla di sovranità digitale ovvero della possibilità che soggetti, anche privati, siano in grado di intercettarli e renderli fruibili, riscrivendo gli equilibri geostrategici ed imponendo nuove regole ad una realtà *internet-based*».

La c.d. *military intelligence* ha come oggetto di ricerca e di analisi «ogni fatto o atto estero di rilevanza o attinenza militare, la cui conoscenza è necessaria o utile ai fini di predisporre ed effettuare la difesa nazionale e di pianificare e compiere azioni o interventi militari – inclusa la guerra – a livello tattico, operativo e strategico» (Gelao, 2023, 1; Pioppi, 2018; Pisano, 2008, 88).

In questo senso, utilizzando approcci di raccolta e analisi delle informazioni per fornire guida e direzione nell'assunzione di decisioni rapide e mirate, l'*intelligence* militare diventa un'area multidisciplinare che combina linguaggio, teoria, politica, economia, sociologia e

[12] In base alla tipologia della fonte informativa, si possono distinguere differenti attività: OSINT (*Open Source intelligence*), ossia la raccolta delle informazioni mediante l'analisi di fonti aperte; IMINT (*Imagery intelligence*), ossia raccolta delle informazioni mediante l'analisi di fotografie aeree o satellitari; HUMINT (*Human intelligence*), ossia raccolta delle informazioni mediante contatti interpersonali; SIGINT (*Signal intelligence),* ossia raccolta delle informazioni mediante l'intercettazione e analisi di segnali, sia tra persone sia tra macchine; TECHINT (*Technical intelligence*), riguardante armi ed equipaggiamenti militari; MASINT (*Measurement and Signature intelligence*), ossia raccolta delle informazioni non classificabili nelle precedenti categorie.

[13] Sul punto, si rinvia a *Considerazioni preliminari*.

psicologia e include informazioni su forze, piani e operazioni militari di altre nazioni che vengono raccolte attraverso una varietà di mezzi.

In altre parole, l'*intelligence* militare è l'arte di «*know your enemies*» (Sadiku e Musa, 2021), ponendosi l'obiettivo di fornire un supporto informativo tempestivo, pertinente e accurato alle esigenze tattiche, operative e strategiche della Difesa.

Si articola in tre aree di intervento:

- *Tactical intelligence*, che si concentra sulle potenzialità del nemico per analizzare le tecniche e le procedure dei reparti e dei raggruppamenti militari*;*
- *Operational intelligence,* che riguarda la raccolta di informazioni per svolgere campagne e operazioni militari su territorio estero;
- *Strategic intelligence,* che si sofferma sugli obiettivi del nemico e le sue possibili intenzioni. In questo settore, sono particolarmente rilevanti gli elementi che costituiscono l'ordine di battaglia (*order-of-battle intelligence*), ossia la composizione, la disposizione e la forza numerica delle truppe impiegate in un'area specifica, i loro principi tattici ed operativi, l'addestramento ricevuto, il sistema logistico organico, l'efficacia operativa, i dati tecnici di varia natura e gli aspetti biografici (inclusi lineamenti caratteriali o psicologici) di determinati gradi gerarchici.

Da tale ricostruzione emerge un dato difficilmente confutabile: pur riconoscendo che la prima missione assegnata alla Difesa è quella di proteggere lo Stato contro ogni possibile aggressione per salvaguardare l'integrità della Repubblica[14], non può sottacersi come il comparto militare sia chiamato a svolgere attività di dissuasione e deterrenza alle minacce portate agli interessi nazionali attraverso una capillare opera di neutralizzazione dell'offesa che passa anche attraverso la raccolta e la gestione dei dati. In questo senso, la capacità di analisi delle informazioni – che rappresenta una inevitabile premessa di ogni processo decisionale – si poggia, *in primis*, sulla disponibilità e sull'accesso ad informazioni aggiornate, complete e corrette.

Conviene anticipare sin d'ora che la capacità informativa rappresenta di per sé un bene giuridico da proteggere; pertanto – come meglio si dirà nel prosieguo[15] – tanto più è estesa la mole di informazioni sensibili elaborate e processate, tanto più elevata sarà l'esposizione al pericolo per la Difesa nel caso in cui non sia assicurato il più alto grado di sicurezza alla protezione dei dati.

[14] Cfr. artt. 89 e 92, d.lgs. 15 marzo 2010, n. 66 (c.d. Codice dell'Ordinamento Militare).
[15] Cfr. Cap. IV.

b. L’importanza delle informazioni nel modello DIME e nelle operazioni multidominio

Una volta chiarito in cosa si sostanzi la funzione informativa e, nello specifico, quella applicata al campo militare, occorre soffermarsi sulla centralità dell’attività di raccolta e gestione dei dati per la neutralizzazione delle minacce alla sicurezza dello Stato quale prodromo ineludibile di ogni processo decisionale e, di conseguenza, analizzare le strategie da mettere in campo per garantire la c.d. superiorità informativa.

Come è noto, le minacce all’integrità della Repubblica che la Difesa ha il compito di neutralizzare tendono a manifestarsi sul piano oggettivo e soggettivo in forme “non convenzionali” in ragione dell’esigenza dell’aggressore di aggirare la prevedibilità ed innalzare il livello di offensività dell’attacco.

I tratti caratteristici di una minaccia non sono, quindi, più riconducibili in modo esclusivo ai convenzionali parametri bellici “geografici” o “fisici”: il potenziale offensivo degli Stati sovrani e degli enti ostili è ormai “ibrido”, in quanto alla capacità di impiegare metodi tradizionali per attentare i “confini” nazionali si affiancano strumenti bellici “liquidi”, privi non solo di riferimenti oggettivi ma in alcune circostanze sprovvisti di tratti utili ad individuarne la “paternità”. Più precisamente, lo spazio *cyber* permette di preservare l’anonimato degli attori a causa della difficoltà oggettiva di tracciare la fonte degli attacchi: grazie alla possibilità di operare attraverso falsi IP e *server* stranieri, chi attacca gode di una relativa impunità (*non attribution*). Si pensi ad esempio all’attività di hackeraggio che ha interessato alcuni *hotspot* della Repubblica francese, impedendo l’erogazione di servizi essenziali ai cittadini (strutture ospedaliere) ed ha creato “crepe” nel colosso aereospaziale *Thales*, la cui responsabilità non è stata accertata in modo definitivo[16].

Dunque, l’analisi degli eventi che caratterizzano l’attuale scenario internazionale disvela un quadro globale completamente trasformato, permeato da una diffusa instabilità e da un elevato grado di imprevedibilità delle minacce che – di riflesso all’evoluzione tecnologica dell’ultimo tempo – diventano multiple, multidimensionali e anche poco riconoscibili. In questo contesto, la Difesa è chiamata ad assumere il controllo del dominio cibernetico, qui da intendere sia come ambiente “autonomo” sia come spazio funzionale a garantire la piena capacità operativa ai domini più tradizionali, sul presupposto per cui le azioni condotte a livello *cyber,* pur sviluppandosi in una dimensione immateriale, producono effetti concreti nel mondo reale.

[16] https://www.cybersecitalia.it/lockbit-contro-la-francia-nuovo-attacco-informatico-al-gigante-aeropaziale-thales/21714/.

Perché ciò accada, è indispensabile garantire al comparto militare la superiorità informativa, funzionale a preservare la superiorità decisionale nella gestione degli attacchi all'integrità della Repubblica attraverso 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[17].

Dunque, per poter decifrare e comprendere le minacce circostanti, gestendone al contempo risposte efficaci, tempestive e capaci di generare effetti duraturi nel tempo 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'ineludibile necessità di disporre di reali capacità multidominio in grado di assicurare la sincronizzazione delle azioni e degli effetti.

In tale contesto, lo Strumento militare deve contribuire efficacemente a garantire la difesa del Paese e degli interessi nazionali solo 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.

Di qui, si richiede una sinergia ad assetto variabile tra i suddetti Strumenti, in uno sforzo condiviso e bilanciato per ridurre il rischio di uno scontro di tipo cinetico che deve essere inteso come *extrema ratio*.

c. Il ruolo degli attori statuali per l'accesso alle informazioni strategiche: prospettive di collaborazione

Una volta compresa l'importanza della superiorità informativa per la protezione degli interessi vitali dello Stato, occorre interrogarsi sullo stato dell'arte, ossia sul se e in che misura il sistema Difesa sia parte integrante del meccanismo poc'anzi richiamato, rilevando – in prospettiva *de jure condendo* – la necessità di prevedere nuove forme di collaborazione tra le forze dello Stato per ampliare l'accesso alle informazioni per "competere" con l'avversario tecnologicamente avanzato e di semplificare le procedure che richiedono l'espressione di consensi e/o pareri autorizzativi vincolanti, spesso da autorità esterne al "circuito" militare.

Per poter illustrare le prospettive di miglioramento futuribili, occorre partire dallo stato dell'arte e individuare le criticità che – sul piano sistemico – pregiudicano il pieno livello di efficienza dell'attività operativa.

---

[17] Per tali considerazioni, si rinvia a Cap. I, § *c* e alle *Considerazioni conclusive*.

Come è noto, l'attuale assetto ordinamentale viene disegnato dalla legge 3 agosto 2007, n. 124[18], la quale istituisce il Sistema di Informazioni per la Sicurezza della Repubblica (SISR) che consiste nell'insieme degli organi e delle autorità deputate ad assicurare le "attività informative" allo scopo di salvaguardare lo Stato dalle minacce provenienti sia dall'interno che dall'esterno[19].

Prima facie, si potrebbe arrivare a sostenere che l'attività di raccolta e gestione delle informazioni per la protezione degli interessi militari del territorio dello Stato sia di appannaggio esclusivo dei Servizi di *intelligence* e, dunque, di competenza degli organi che dipendono dal Ministero dell'Interno. Un simile approdo, tuttavia, rischia di mostrarsi "miope" perché non considera il ruolo svolto anche da altri organi che, per converso, dipendono dal Ministero della Difesa.

Precisamente, il II Reparto Informazioni e Sicurezza (RIS) – non integrato nel Sistema di informazione per la Sicurezza della Repubblica ma in stretto contatto con l'AISE – per espressa previsione normativa «svolge [...] compiti di carattere tecnico militare e di polizia militare, e in particolare ogni attività informativa utile al fine della tutela dei presidi e delle attività delle Forze armate all'estero [...]» (art. 8, comma 2, l. 124/2007)[20].

Il RIS è caratterizzato da un sistema organizzativo particolarmente articolato, il cui perno è rappresentato dal Centro *Intelligence* Interforze, deputato a svolgere compiti di carattere tecnico-militare e, in particolare, di raccolta ed elaborazione di dati strategici per la Difesa (c.d. *intelligence* militare).

Così ricostruito – seppur in termini sommari – l'organigramma del comparto Difesa, deve ammettersi che la funzione informativa per l'assolvimento di compiti militari non è del tutto estranea alle Forze armate.

---

[18] In passato, la legge 24 ottobre 1977, n. 801 istituì il Servizio per le informazioni e la sicurezza militare (SISMI) e il Servizio per le informazioni e la sicurezza democratica (SISDE). Le due strutture erano poste, rispettivamente, alle dipendenze del Ministro della Difesa e del Ministro dell'Interno. Il SISMI era prevalentemente deputato a difendere la sicurezza nazionale da qualsiasi minaccia in Italia e all'Estero; si trattava, dunque, di un organo chiamato a svolgere attività di *intelligence* militare con il compito di difendere l'integrità nazionale da qualsiasi minaccia in Italia e all'Estero anche con azioni di controspionaggio dirette a tale scopo. Accanto al SISMI, ogni Forza Armata disponeva di proprie strutture di vertice (Servizio Informazioni Operativo Sicurezza - SIOS); reparti, questi, in seno ai tre Stati Maggiori di Forza Armata, con il compito di tenere aggiornata la situazione dei fattori costituenti il potenziale militare dei Paesi possibili avversari, forniti dall'organo informativo superiore (SISMI) o direttamente raccolti dagli addetti militari, navali e aeronautici presso le ambasciate e dagli organi informativi periferici. Poi un cambio di rotta: con la legge 18 febbraio 1997, n. 25 (detta anche Riforma dei vertici militari) vennero sciolti i SIOS di Forza Armata e la componente "Informazioni" venne concentrata in un unico reparto dello Stato Maggiore della Difesa (il II Reparto Informazioni e Sicurezza – RIS) con, alle proprie dipendenze, il "braccio operativo" costituito dal Centro *Intelligence* Interforze (CII).

[19] In particolare, all'AISI (Agenzia di Informazioni Sicurezza Interna) e all'AISE (Agenzia di Informazioni Sicurezza Esterna) viene attribuito il compito di svolgere attività di informazione, anche mediante assetti di ricerca elettronica, esclusivamente verso l'estero, a protezione degli interessi politici, militari, economici, scientifici e industriali della Repubblica (artt. 6 e 7, l. 124/2007), prescrivendo peraltro che «[L]e funzioni attribuite dalla presente legge al DIS, all'AISE e all'AISI non possono essere svolte da nessun altro ente, organismo o ufficio» (art. 8, comma 1, l. 124/2007).

[20] Cfr. pure l'art. 30, d.lgs. 15 marzo 2010, n. 66 (Codice dell'Ordinamento Militare), per cui il «Reparto informazioni e sicurezza dello Stato maggiore della difesa Il Reparto informazioni e sicurezza dello Stato maggiore della difesa svolge i compiti previsti dall' articolo 8 della legge 3 agosto 2007, n. 124».

Allo scopo, l'attuale impianto normativo e regolamentare predispone dei meccanismi di collaborazione interistituzionale tra le Forza Armate, organi statuali e gli organismi di *intelligence* da attuarsi mediante uno scambio informativo e una cooperazione anche di tipo tecnico-operativo. Appare evidente, tuttavia, come nel predetto impianto il ruolo della Difesa nell'accesso, nell'elaborazione e nella diffusione delle informazioni sia "marginale" rispetto a quello degli organi di *intelligence*[21]*.*

Tale squilibrio, che pur è giustificato dal riparto di attribuzioni caratteristico delle diverse funzioni svolte dai due comparti, tende a generare un *bias* di efficienza nel sistema Difesa che, a differenza degli omologhi *competitors,* non è nelle condizioni di avere una capacità informativa "diretta" e "completa" relativamente a settori di interesse apparentemente estranei alla Difesa.

Più concretamente, l'accesso alle informazioni di non diretta pertinenza del Dicastero è "filtrato" dall'intermediazione del DIS, al quale il sistema vigente attribuisce una posizione di monopolio gestionale, rappresentando l'unico referente cui tutte le istituzioni (le Forze armate e di polizia, le amministrazioni dello Stato e gli enti di ricerca anche privati) sono tenute a fornire informazioni.

Ciò determina un'attività di intermediazione che, sul piano sostanziale, oltre a operare una classificazione dei dati secondo un approccio estraneo al *mainstream* militare[22], provoca sia un ritardo nell'accesso a informazioni sensibili, sia un filtro selettivo a monte che potrebbe mal conciliarsi con le esigenze di tempestività della reazione e/o con l'opportunità di conoscenza di elementi la cui rilevanza possa essere oggetto di non coincidente valutazione tra i due versanti. Non va, infatti, sottaciuto che la complessità e la volatilità della minaccia richiede un'inevitabile e significativa compressione dei tempi decisionali di azione, esigendo di disporre di strumenti e procedure che garantiscano, a tutti i livelli, un'agilità decisionale che, nell'ambito di una strategia complessiva, permetta l'assunzione di decisioni rapide e attagliate alla continua evoluzione della situazione.

Di qui, l'esigenza di rivedere i meccanismi di cooperazione descritti nell'ottica di un riequilibrio della posizione della Difesa nell'accesso alle informazioni.

In virtù delle sfide che si profilano nello scenario internazionale, si ritiene tanto auspicabile quanto doveroso procedere ad un adeguamento dell'architettura istituzionale in materia di Difesa e Sicurezza e ad uno snellimento delle procedure allo scopo di assicurare coerenza, efficienza e agilità all'azione governativa.

---

[21] Si veda, sul punto, l'art. 12, l. 3 agosto 2007, n. 124, per cui «[…] le Forze Armate […] forniscono ogni possibile cooperazione […] al personale addetto ai Servizi di informazione per la sicurezza».

[22] Individuare primariamente minacce di tipo "strategico", ad esempio, rischia di non tenere in adeguato conto altre minacce indirette o ibride, oltre che di non programmare la tempestiva reazione ad una sorpresa.

Al di là dell'esigenza di prevedere – in chiave sistematico-organizzativa – uno Strumento militare interforze resiliente e tecnologicamente avanzato[23], si intravedono prospettive di miglioramento anche con specifico riferimento all'efficientamento della capacità informativa (quale premessa della superiorità cognitiva e decisionale) in considerazione del ruolo centrale delle informazioni nel modello DIME e nelle operazioni multidominio.

Precisamente, si potrebbe pensare di affidare alle riunioni periodiche (quelle che, ad oggi, regolano i meccanismi di scambio informativo tra il DIS e le istituzioni statuali) una funzione "sussidiaria", prevedendo in prim'ordine l'istituzione di un Organo permanente di coordinamento in cui sia assicurata la diretta presenza della Difesa in seno al comparto deputato al recepimento delle informazioni.

Tale organo interforze, congegnato in termini paritetici tra i suoi componenti, potrebbe essere in grado di assicurare la contaminazione reciproca tra il *mainstream* militare e il *modus operandi* degli altri attori statuali, garantendo la completa integrazione e interoperabilità tra i comparti coinvolti nel campo della capacità informativa.

Nella piena consapevolezza di non poter più contare su un sistema caratterizzato da una rigida separazione delle competenze tra i vari dicasteri, l'obiettivo è quello di garantire un più efficace meccanismo di difesa e sicurezza attraverso un impegno olistico e un approccio sinergico delle compagini istituzionali per trarre il massimo vantaggio competitivo in termini di efficienza e tempestività. In questo modo, la capacità di sintesi strategica, le priorità stesse e gli interventi troverebbero – per strutturata definizione – valutazione diretta, ispirata ad una visione integrata, riducendosi il rischio concreto di aprire spazi di vulnerabilità per le organizzazioni statuali democratiche.

[23] Cfr. *Considerazioni conclusive*.

CAPITOLO II
PROPOSTE DI SVILUPPO DEL POTENZIALE MILITARE. UN NUOVO IMPIEGO DELLE TECNOLOGIE "INVESTIGATIVE" NEL RINNOVATO CONCETTO DI "CONFLITTO BELLICO"

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

Come si è avuto modo di anticipare[24], 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 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, ad 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" che si presenta inadatto a fronteggiare le moderne forme di minaccia perpetrate attraverso l'impiego di 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

[24] Cfr. *Considerazioni preliminari*.

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 dall'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 a celare traffici, attività illecite e l'identità di chi li perpetra, generando non poche difficoltà per gli inquirenti e gli investigatori nell'opera di ricostruzione dei fatti e di 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, necessitano sempre più spesso 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 difronte 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 all'impiego di 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 cybernetiche "franche" (c.d. *deepweb*) 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 l'impiego della tecnologia sia utilizzato 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 (Curtotti *et al*, 2023).

Ebbene, all'evoluzione delle forme di manifestazione del crimine corrisponde un cambiamento del modo di investigare, soggetto ad un ineluttabile processo di 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" estranee al *background* che caratterizza la formazione della "prassi operativa". Pertanto, le contrapposte esigenze – da un lato, garantire un'attività inquisitoria efficiente ed al passo con il darwinismo tecnologico-delinquenziale, dall'altro, dotare il comparto investigativo di un elevato grado di 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[25].

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» (Nocerino, 2021a, 2). 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.

[25] 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: difronte 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.

Ebbene, i tangibili riscontri positivi derivanti dal processo di 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 Giustizia e Difesa, pongono la presente ricerca a prospettare un approccio "mutualistico" dello 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 Armate possono trarre dalle capacità operative delle tecnologie investigative, il cui potenziale è compresso dal "*civil use*" 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 ed 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 di ogni individuo. Ebbene, le *skills* gestionali-operative di cui sono muniti tali strumenti paiono poter rappresentare un'utile soluzione per il comparto militare allorquando il campo di azione non presenta i tratti tipici del conflitto bellico, essendo l'attività di Difesa condotta 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 (allorquando 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.

Si vuole fare nello specifico 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 dicastero, innalzando il livello di reattività e l'efficienza della neutralizzazione della minaccia, nell'ottica di un sistema difensivo multidominio integrato.

b. 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.

Tuttavia, prima di soffermarci più nel dettaglio sulla proposta *de qua*, appare 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 lavoro delle procure di contrasto alla criminalità 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)[26], nonché tecnologie strumentali al miglioramento della loro applicazione, tra i quali di notevole interesse è l'IMSI *Catcher*[27] (Nocerino, 2021a; Nocerino, 2021b).

---

[26] Il captatore informatico rientra nella *species* della sorveglianza elettronica (*Working Group on International Cooperation, International cooperation involving special investigative techniques*, Vienna, July 2020) che permette di controllare a distanza i dispositivi "attenzionati", assumendone il pieno controllo e, di conseguenza, di acquisire una mole in(de)finita di dati e di informazioni che difficilmente potrebbero essere conosciuti (e conoscibili) ricorrendo alle tecniche di indagine tradizionali, sfruttando la portabilità e l'imperscrutabilità dello strumento.

[27] L'IMSI *Catcher* in grado di monitorare tutti i dispositivi elettronici presenti in un certo raggio di azione, identificare i titolari delle utenze individuate e procedere alla captazione di comunicazioni e al tracciamento dei dati che transitano sulla "macchina-bersaglio".
Si tratta, più precisamente, di un falso ripetitore che si interpone tra il telefono "bersaglio" e le torri delle compagnie telefoniche, sfruttando la tecnica "man in the middle", così da agganciare tutti i dispositivi elettronici chiamanti presenti in un certo raggio di azione. In questo modo, riesce a monitorare tutte le utenze ivi localizzate e, attraverso l'estrapolazione dell'IMSI (*International Mobile Subscriber identity Mo*dule), è in grado di individuare il soggetto fisico cui la SIM risulta intestata.
Soprattutto, tramite l'impiego di speciali *software* che implementano le potenzialità del *Catcher* (c.d. *Decifer*), gli investigatori possono svolgere sul dispositivo individuato ed identificato attività di intercettazione e controllo da remoto attraverso l'inoculazione di un captatore informatico, finendo così per "gestire" il complesso di sistemi che si trovano nello spazio oggetto di interesse investigativo.

Ebbene, nel bel mezzo del loro impiego, è balzato agli occhi degli operatori del settore l'enorme potenziale insito in dette strumentazioni, la cui multifunzionalità si scontra con l'unico binario sul quale il sistema giudiziario è incardinato, 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 nella 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 invece 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) al fine di acquisire elementi utili alle indagini e/o a prevenire fatti di particolare allarme sociale, nel campo militare potrebbero consentire il pieno controllo dei 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[28].

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 attraverso una rivisitazione dell'architettura normativa che

[28] Su queste riflessioni, si rinvia a Cap. II, § *d.*

attualmente imbriglia la piena esplicazione dello Strumento militare in un contesto estraneo alla dimensione conflittuale.

b.1 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 dei 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[29]. In altri termini, i principi costituzionali e convenzionali rappresentano il principale argine dell'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[30] e, a seguito di una più recente impostazione giurisprudenziale, alle intercettazioni telematiche (Cass., Sez. V, 30 maggio 2017, n. 48370, in *C.E.D. Cass.,* n. 271412).

Di conseguenza, il *virus* informatico può essere usato solo nei confronti di soggetti identificati[31], allorquando emergono "gravi" o "sufficienti" indizi di reato[32] ovvero "specifici elementi che giustificano l'attività di prevenzione"[33], per un tempo limitato[34], solo su autorizzazione dell'autorità giudiziaria[35], con il precipuo intento di evitare che il sistema si

---

29 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.

30 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*.

31 Cfr. art. 267, comma 1, c.p.p.

32 Nel caso di intercettazioni "processuali" (ossia quelle esperiti nel corso di un procedimento penale già avviato), affinchè 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.

33 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 (Nocerino, 2018, 254).

34 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.

35 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).*

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 (Nocerino, 2021a, 147; Orlandi, 2018, 540; Signorato, 2019, 301); dunque, nell'ordinamento nazionale il "controllo" di qualsivoglia sistema "infetto" non può, allo stato dell'arte, essere ammesso in condizioni ordinarie.

c. 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 essere chiari, in campo "militare" è da considerarsi "ingiusta" ogni intrusione nella dimensione privata fuori dalle condizioni di straordinarietà che si palesano in ipotesi di conflitto bellico.

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, palesarsi un "conflitto armato" in grado di consentire un abbassamento delle garanzie individuali in nome delle esigenze di sicurezza collettiva.

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[36]: 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 sulla 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[37].

---

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

[37] 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.

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 ad 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[38] 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 gius-politico 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, rappresenta il principale limite all'uso militare della tecnologia in contesti di (apparente) non ostilità (fisica). 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

[38] 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.

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[39].

d. 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 ricorrere all'uso di strumenti tecnici in grado di porre tempestivo rimedio alla situazione di pericolo attraverso l'esercizio delle 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

[39] Cfr. *Considerazioni conclusive.*

e protocolli operativi che ne indirizzino l'impiego. 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[40] – 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*[41].

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.

[40] 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. Cfr. *Approccio della Difesa alle Operazioni Multidominio*, cit., 22.

[41] Sulla proposta *de qua,* cfr. *Considerazioni conclusive.*

CAPITOLO III
Il RUOLO DELLA COOPERAZIONE PER LA SICUREZZA INTERNAZIONALE

a. Le nuove esigenze di sicurezza cooperativa

Il processo di globalizzazione – inteso come riconoscimento in via universale di interessi collettivi umanitari – ha visto un'accelerazione a seguito del crescente sviluppo tecnologico.

Parallelamente, la crescente influenza della dimensione *Cyber* ha determinato la nascita di uno spazio globale privo di riferimenti geografici, la cui influenza impone un ripensamento del ruolo della cooperazione per la sicurezza internazionale tra gli Stati sovrani territoriali, chiamati a creare un sistema aggregato e multilivello che superi e ridimensioni la concezione statica dei confini nazionali, i quali evidentemente non sono più capaci di contenere e delimitare il perimetro delle minacce.

Inoltre, aspetto caratterizzante la nuova descritta dimensione è la reciproca influenza delle variabili che lo compongono che, nella maggior parte dei casi, è causa di "effetti sorpresa" dovuti alla mancanza di una condivisione informativa. In buona sostanza, in uno scenario in cui le singole variabili non sono indipendenti ma si combinano e si influenzano reciprocamente, è dovere dei singoli attori, mossi da intenti comuni, operare una gestione condivisa e istantanea delle rispettive fonti informative.

Su un piano più concreto, l'esigenza di coordinamento cui si discorre deve tenere conto del grado di affidabilità dei *partners* chiamati a prendere parte alla rete di cooperazione, posto che l'efficienza della condivisione informativa è direttamente proporzionale alla comunanza di intenti dei partecipanti; pertanto è necessario in primo luogo verificare la sussistenza, in capo ai soggetti coinvolti, di elementi sufficienti a garantire una solida "*affectio societatis*"[42]*.* In altri termini, senza una comunanza "politico-strategica" la cooperazione non può che ritenersi un sogno chimerico.

Invero, sul versante politico internazionale, già a partire dalla primavera del 2014 – che, a causa di un mutato orientamento strategico globale della Federazione Russa, può esser considerato l'anno mille della cooperazione internazionale – sta maturando tra le Forze poste a difesa della stabilità liberaldemocratica occidentale un approccio globale e interconnesso che tiene in debito conto la necessaria compattezza degli Stati Sovrani nella

[42] Considerato il carattere ibrido e transnazionale delle minacce, è necessario sviluppare partenariati reciprocamente vantaggiosi con Paesi che condividono i medesimi valori.

lotta comune alle sfide del futuro in un mondo in cui, al pericolo delle ambizioni politiche delle autocrazie, va aggiunta la minaccia di "oligopolismi" dai tratti soggettivi "meta-nazionali" dotati di pari potenzialità destabilizzanti. Ebbene, se il nobile scopo di edificare un sistema reticolare multilivello rappresenta un'esigenza non più procrastinabile[43], deve tuttavia ammettersi che, sul piano fattuale, l'obiettivo non è di semplice realizzazione.

Sul versante giuridico, la sopravvivenza del sistema deve, infatti, fare i conti con le disarmonie legislative, normative e ordinamentali proprie dei singoli Stati Nazionali[44] che – inevitabilmente – ostacolano la libera e indiscriminata circolazione di informazioni (*anche se* o, a seconda dei casi, *specie se*) strategiche.

Sul versante diplomatico, invece, vanno evidenziate le possibili asimmetrie caratterizzanti le relazioni reciproche tra gli interlocutori coinvolti a diversi livelli.

Con riferimento a tale ultimo aspetto, è emblematica l'attuale postura strategica della Repubblica Italiana nel panorama globale che impone l'adozione di una politica di cooperazione internazionale indirizzata nel solco di tre direttrici strategiche: il contesto NATO, la politica di Difesa Comunitaria e – sul piano nazionale – la cooperazione plurilaterale con le diverse anime politico-culturali presenti nel Mediterraneo allargato.

Appare evidente che l'eterogeneità degli interlocutori appena menzionati e il complesso bilanciamento dei rapporti bilaterali di cui la diplomazia deve tener conto, impone cautela nella prospettazione di un sistema di difesa comune fondato sullo scambio informativo privo di filtri.

Ed altrettanto palese appare l'importanza del ruolo della Difesa italiana che, in ragione del posizionamento geografico in un crocevia politico-culturale di indubbio equilibrio strategico, è destinata a ricoprire un ruolo di elevata responsabilità nella difesa della stabilità internazionale.

In questo contesto, diventa imprescindibile costruire una prospettiva globale comune che favorisca la raccolta e la circolazione delle informazioni – anche in Paesi diversi da quelli in cui è emersa l'esigenza di sicurezza e difesa – filtrata sulla base di parametri che tengano conto della natura degli interlocutori e degli obiettivi propri degli Accordi di

---

[43] Come anche rileva l'Unione Europea nell'ambito della *Commons Security and Defence Policy* (CSDP), il primo passo per contrastare le minacce ibride consiste nell'identificazione della minaccia per poi decidere la linea di azione più idonea da intraprendere, nella consapevolezza che il livello di ambizione non potrà essere lo stesso per tutti gli attori. In un contesto come quello descritto, il modello proposto dall'UE si basa sulla definizione degli obiettivi strategici e soglie di risposta comuni.

[44] Si faccia l'esempio della differente gestione delle *Multi-Domain Operations* (MDO): se il modello "esercito-centrico" statunitense prevede l'inquadramento della MDO nella sola risposta militare per penetrare eventuali strategie *Anti Access-Area Denial* avversarie, il modello inglese, con la propria *Joint Concept "Multi-Domain Integration",* propende per un'integrazione già a livello governativo e nell'ambito dell'intero spettro della competizione a tutti i livelli delle operazioni militari. Il modello prescelto dall'Alleanza Atlantica, invece, è volto a combinare le azioni in tutti e cinque i domini delle operazioni, ampliando le capacità disponibili per sfruttare la sorpresa, la convergenza e il successo delle operazioni.

cooperazione, così da evitare una perniciosa condivisione indiscriminata di dati strategici. Dunque, in una visione integrata, sistemica e multidominio, il tema della sicurezza cooperativa diventa di centrale importanza per garantire una stabilità duratura delle Nazioni.

Di qui, l'obiettivo è quello di prevedere e rafforzare l'interoperabilità tra i sistemi, soprattutto a livello internazionale e sovranazionale, per favorire un processo di armonizzazione attraverso l'implementazione di strumenti di consultazione collettiva in chiave Strategica e di Difesa.

b. Gli sviluppi a livello NATO, Unione Europea e nuove Strategie di Sicurezza e Difesa per il Mediterraneo

A livello internazionale, la NATO rappresenta la più potente forma di cooperazione per proteggere e difendere la sicurezza delle Nazioni Alleate.

In particolare, la NATO è impegnata nello sviluppo di un approccio condiviso e sinergico tra i suoi Membri, mirato – tra l'altro – a un progressivo miglioramento delle capacità di sicurezza cooperativa: non a caso, infatti, nell'Agenda 2030 (pubblicata a giugno 2020), la NATO chiarisce che le linee direttrici lungo le quali si svilupperà il futuro dell'Alleanza si fondano proprio sul rafforzamento delle relazioni tra gli Stati, sulla valorizzazione degli strumenti di consultazione collettiva, nonché sull'implementazione delle infrastrutture civili a fini di Difesa e Deterrenza (Marrone *et al*, 2021).

D'altro canto, l'invasione dell'Ucraina da parte della Russia e la crescente assertività della Cina, nonostante abbiano determinato l'effetto di cementare la coesione della NATO e di elevare il ruolo dell'Unione Europea ad organizzazione con valenza geopolitica, con la contestuale decisione di rinforzare anche la dimensione militare, hanno inoltre imposto una "rivisitazione" dello *Strategic Concept*.

Precisamente, la NATO e l'Unione Europea – di concerto con gli Stati membri dell'UE e con gli Alleati NATO – hanno intensificato l'attività di cooperazione attraverso la sottoscrizione di una nuova Dichiarazione (del 10 gennaio 2023) a Bruxelles, fondata proprio sulla necessità di implementare gli strumenti cooperativi nell'ottica di garantire la sicurezza internazionale.

Di qui, sulla scia delle precedenti Dichiarazioni del 2016 e del 2018, la terza Dichiarazione individua ulteriori aree in cui le Organizzazione intendono rafforzare la cooperazione internazionale nell'ottica di un "*Comprehensive approach*", ossia un approccio globale internazionale per gestire le crisi derivanti dalle più evolute forme di attacco alla sicurezza degli Stati.

Si tenga ben presente che, tra le nuove aree di intervento, la terza Dichiarazione punta sulla necessità di prevenire e combattere le minacce ibride e cibernetiche per rafforzare la competizione geo-strategica e la resilienza proprio attraverso la costruzione di sistemi che garantiscano una più sinergica cooperazione informativa.

Parallelamente, considerata l'importanza riconosciuta dalla NATO al "Fianco-Sud", la Strategia di Sicurezza e Difesa per il Mediterraneo (ed. 2022) si pone come obiettivo primario la necessità di incrementare la capacità di raccolta informativa al fine di poter garantire la sicurezza cooperativa per disporre di una più completa *Situational Awareness* su ciò che accade nell'area del Mediterraneo.

Alla luce di tali premesse, appare inevitabile concentrarsi sull'importanza della cooperazione a fini di sicurezza e, di conseguenza, sull'implementazione delle infrastrutture esistenti e sulla costruzione di nuovi strumenti di consultazione collettiva per garantire una più idonea capacità informativa e decisionale, senza tuttavia trascurare le esigenze di sicurezza (*rectius:* riservatezza) delle informazioni per evitare di perdere superiorità cognitiva conquistata.

L'obiettivo prefissato può essere centrato dotando lo Strumento militare di sistemi interconnessi che, mediante lo sfruttamento della capacità olistica della dimensione digitale, siano idonei a coprire in modo trasversale tutti e cinque i domini, senza con ciò implicare un eccessivo dispiego di energie operative.

Appare chiaro che, a fronte del vantaggio in termini di efficienza della dimensione digitale, nella costruzione di un sistema di cooperazione informativa l'impiego del dominio *cyber* è altrettanto idoneo ad innalzare il livello di vulnerabilità del sistema che s'intende strutturare; pertanto, l'agibilità del *framework* auspicato non può che passare dalla precauzionale installazione di uno strumento di comunicazione protettivo del flusso di informazioni scambiate.

In buona sostanza, in considerazione della qualità delle informazioni oggetto di scambio, la cooperazione può essere efficacemente garantita mediante l'impiego di mezzi di comunicazione impenetrabili, alla luce dell'imprescindibile priorità della riservatezza informativa, la cui assenza può trasformarsi in un pericolo direttamente proporzionale all'importanza delle informazioni scambiate.

Come meglio si dirà nel prosieguo[45], occorre focalizzare l'attenzione sul concetto di "*secure-by-design*" nella progettazione dei nuovi sistemi comunicativo/informativi, la cui

[45] Cfr. Cap. III, § *d.*

concretizzazione è garanzia di piena interoperabilità a livello interforze, NATO/UE e di coalizione, nonché con Dicasteri, Autorità, Agenzie ed Enti del Settore Pubblico e Privato.

c. Le disarmonie legislative nello scambio informativo transnazionale

Come noto, il rapporto di diretta proporzionalità tra capacità cognitiva e quantità di informazioni da elaborare postula la continua implementazione di quella che è comunemente definita attività di *surveillance.* Attività, questa, che inevitabilmente si scontra con la tutela del diritto alla riservatezza, la cui "intensità" rappresenta, nei singoli contesti politici, la principale "variabile" che ostacola una piena armonizzazione del sistema di cooperazione in materia di circolazione dei dati.

In altri termini, l'esigenza di favorire la semplificazione delle procedure di acquisizione e scambio transfrontaliero di informazioni al fine di garantire la sicurezza cooperativa stride, in maniera sempre più incisiva, con il sostrato socio-culturale della tradizione occidentale improntato alla tutela della *privacy*. Ebbene, pare doveroso evidenziare il diverso approccio al tema che pone USA e UE – i principali pilastri dell'Alleanza Atlantica – su piani regolamentari "disallineati" (Resta, 2015, 23).

Senza scendere nel dettaglio normativo, è sufficiente constatare che – come è dato evincere dalla recente storiografia (ci si riferisce, in particolare, alla dichiarata invalidità del piano c.d. *Safe Harbour* prima, e del *Privacy Shield* dopo, alla luce dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati nel maggio 2018)[46] – l'UE affronta la *quaestio* relativa alla raccolta dei dati attraverso attività di sorveglianza con un atteggiamento tendenzialmente "garantista" che, in nome della primazia del diritto alla riservatezza rispetto all'esigenza di approvvigionamento di dati liberamente forniti per scopi ben specifici, ha caratterizzato il bilanciamento tra *privacy* e sicurezza operato dalle istituzioni Europee.

Di contrario avviso è, invece, l'impostazione degli Alleati d'oltreoceano che, sul piano normativo, – a partire dall'11 settembre 2001, a seguito di un'interpretazione estensiva della c.d. "dottrina Bush" – hanno relegato la tutela alla riservatezza in una posizione deteriore, subordinando il rispetto della *privacy* alla tutela della sicurezza Nazionale (Bradley, 2002, 465; Cole e Dempsey, 2012, 194).

[46] Cfr. le sentenze della Corte di Giustizia dell'Unione Europea del 6 ottobre 2015, C-362/14 (c.d. sentenza *Shrems*) e del 16 luglio 2020, C-311/18 (c.d. *Shrems* II), con cui i giudici del Lussemburgo dichiarano l'invalidità dei sistemi che informavano la trasmissione dei dati dall'Europa a Paesi terzi.

Nonostante i recenti sforzi profusi a livello internazionale per tentare di adeguare la normativa USA/UE nella gestione e nello scambio dei dati[47], il divario continua a sembrare insormontabile. Il quadro, già assai critico, si complica se consideriamo le differenti impostazioni prescelte dai singoli Stati Membri dell'Unione Europea.

In breve, può dirsi che in Europa si registra in materia una disarmonia legislativa brutalmente contraria a quel processo di armonizzazione auspicato dalla Comunità sin dalle sue origini, peraltro favorita dai più recenti orientamenti della Corte Europea dei Diritti dell'Uomo[48]: infatti, se in alcuni ordinamenti (principalmente Francia, e più di recente Polonia e Bulgaria) viene adottata una normazione che consente l'esperimento di attività di sorveglianza, in altri, apparentemente più garantisti (come l'Italia e la Germania), non sono ammesse tecniche di acquisizione di informazioni su larga scala (Nino, 2016, 756).

Le disarmonie legislative or ora richiamate impediscono, di fatto, una circolazione delle informazioni che coinvolga in modo diretto Enti privati e Stati terzi, proprio a causa dei limiti interni e sovranazionali[49] che regolano la cessione dei dati tra cittadino privato e cessionario. Pertanto, al fine di superare l'ostacolo in questione, è auspicabile che ogni singolo Stato attribuisca al comparto Difesa una specifica funzione di "intermediazione teleologica" nella circolazione delle informazioni.

Più nel dettaglio, appare necessario erigere in seno allo Strumento militare un "sistema filtro" che sia investito del compito di acquisire su base nazionale – nel rispetto dei limiti interni e unionali – ogni dato informativo che presenti profili di rilevanza sul piano della sicurezza su scala interna e internazionale, anche tenendo conto delle informazioni già in possesso della Difesa.

L'adozione di un simile modello da parte dei partecipanti al sistema di cooperazione internazionale – accompagnato da un dovere di condivisione dei dati informativi soggettivamente determinato – ha il pregio di superare gli ostacoli giuridici anzi descritti e, al contempo, garantire l'integrità della competenza territoriale dei singoli Dipartimenti della Difesa di ogni Stato sovrano nell'attività di acquisizione dei dati.

---

47 Ci si riferisce, in particolare, al recentissimo "EU-US *Data Privacy Framework",* adottato dalla Commissione europea il 10 luglio 2023 con lo scopo – tra l'altro – di limitare l'accesso governativo statunitense ai dati trasferiti dall'UE.

48 Come ha messo in luce la dottrina (Nino, 2022, 106), se, in passato, la Corte EDU censurava le attività di sorveglianza di massa, in quanto lesiva del diritto alla riservatezza e della libertà di espressione (Corte EDU, 13 settembre 2018, *Big Brother e altri c. Regno Unito, applications* n. 58170/13, 62322/14 *and* 24960/15), più di recente, la Corte ammette tecniche di *surveillance* per l'acquisizione dei dati personali (CEDU, 11 gennaio 2022, *Ekimdzhiev c. Bulgaria*, *applications* n. 70078/12).

49 Cfr., per tutti, art. 45 GDPR, che legittima il trasferimento dei dati personali verso un Paese terzo (cioè fuori dallo Spazio Economico Europeo) solo se la Commissione europea verifica che il Paese in questione garantisce un livello di protezione adeguato.

d. La necessità di sistemi integrati e tecnologie di ultima generazione per garantire la sicurezza della circolazione delle informazioni strategiche

Il quadro finora ricostruito ci restituisce un panorama internazionale in cui – a dispetto degli ambiziosi obiettivi programmatici – i profili critici (in particolare quelli di ordine giuridico legati alla tutela della privatezza e della riservatezza) sembrano porre degli ostacoli difficilmente superabili dai comparti chiamati alla c.d. "operativizzazione".

Ebbene, prima di avanzare proposte istituzionali – che, a causa del necessario *placet* di burocrati e governanti rischierebbero, nelle lunghe pieghe degli *itinera* procedimentali, di perdere vigore e attualità –, appare futuribile "lavorare" su quanto già in possesso del comparto Difesa con un approccio migliorativo consistente nella diversa applicazione dello strumento tecnologico. Ciò in una duplice prospettiva: da una parte, prevedere la costituzione di nuovi e più evoluti strumenti di consultazione collettiva per facilitare la cooperazione e lo scambio informativo; dall'altra, adottare sistemi caratterizzati da importanti gradi di cifratura, così da ridimensionare il principale rischio cui è esposta la circolazione informativa, ossia la violazione della riservatezza delle comunicazioni che, per la natura delle informazioni detenute da chi ha il compito di difendere l'Ordine Nazionale da attacchi convenzionali e non, potrebbe tradursi in vulnerabilità strategica.

Come evidenziato[50], nel moderno concetto di difesa, tra gli obiettivi oggetto di protezione va ricompresa la stessa capacità informativa, il cui valore strategico è tanto più elevato ed efficace quanto maggiore è la segretezza della stessa. Appare, quindi, evidente che quando la Difesa – in ragione dei sopradescritti doveri di cooperazione sovranazionale – è chiamata alla condivisione di informazioni strategicamente sensibili che sono sussumibili nel serbatoio della propria capacità informativa, si espone ad una situazione di maggior pericolo rispetto all'ordinaria attività di elaborazione "interna" dei dati in questione. Ciò significa che il momento della trasmissione delle informazioni tra gli attori della cooperazione rappresenta il punto nevralgico della sicurezza strategica.

Al fine di evitare che tale segmento procedurale si trasformi in un'occasione di "opportunità strategica" per i potenziali avversari, è di fondamentale importanza soffermare l'attenzione sugli strumenti e sulle procedure che possono essere adottate per condividere e comunicare in ambito internazionale. A tale proposito, come si è già avuto modo di constatare in riferimento all'uso militare di *tools* investigativi[51], anche in tale contesto una proposta innovativa è suggerita dalla dimensione tecnologica che in tempi recenti ha assistito alla nascita e all'impiego di raffinate forme di cifratura delle comunicazioni

[50] Cfr. Cap. I, § *a.*
[51] Cfr. Cap. II.

trasmesse sfruttando la Rete. Si tratta delle c.d. "*encrypted platforms*" (piattaforme criptate), molto spesso impiegate dalle organizzazioni criminali per condurre e pianificare le proprie attività, avvantaggiandosi dell'impenetrabilità delle comunicazioni condotte mediante i criptofonini.

Alla luce degli indiscutibili vantaggi offerti dall'uso dei sistemi criptati – in termini di segretezza delle comunicazioni e invulnerabilità delle informazioni[52] – si propone l'impiego di tali sistemi anche nell'ambito del comparto Difesa così da favorire la previsione di strumenti di consultazione collettiva e, al contempo, garantire una più sicura circolazione delle informazioni.

Più precisamente, sul piano strutturale, tali sistemi fungono da veri e propri spazi assimilabili a consessi privi di riferimenti fisici: essi, quindi, a differenza di altri strumenti di comunicazione, sono potenzialmente in grado di riprodurre le fasi procedimentali di un'assemblea senza richiedere l'incontro fisico dei partecipanti, in modo tale da assicurare una vera e propria attività di consultazione collettiva.

Sul piano funzionale, le piattaforme in parola – attraverso le articolate chiavi di cifratura che ne caratterizzano l'operatività – sono in grado di elevare il grado di protezione del contenuto oggetto di interscambio assicurando, nel caso in cui siano trasmessi dati sensibili, il rispetto degli *standard* di riservatezza insiti nel concetto di *privacy*[53]*.*

[52] Queste piattaforme non devono essere confuse con le più note applicazioni di messaggistica sicure, ovvero applicazioni di *chat* private che utilizzano algoritmi di cifratura (*end-to-end*) per proteggere i dati durante tutto il tragitto dal mittente al destinatario (quali, ad esempio, *Signal, Telegram, WhatsApp*). In questi casi, i dati vengono criptati al momento dell'invio e quindi decriptati una volta a destinazione. La differenza fondamentale delle applicazioni di messaggistica sicura con i criptofonini sta nel fatto che, in quest'ultimi, le comunicazioni in entrata e in uscita sono sempre crittografate *end-to-end* e vengono trasmesse su un canale crittografato per proteggere ulteriormente le informazioni. La configurazione di quest'ultimo *tunnel* avviene tramite una VPN (*Virtual Private Network*) dinamica e può essere modificata da remoto dagli amministratori.

[53] Su cui v. *amplius,* Cap. IV, § *b*.

CAPITOLO IV
RISCHI E CRITICITA'

a. Le nuove attività operative della Difesa alla prova dello Stato di diritto

Giunti a questo punto della ricerca, occorre interrogarsi sulla fattibilità a livello pratico ed 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[54] 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[55] – anche l'invasione sostanziale della sfera privata (Cinelli, 2020b, 590).

A ben guardare, l'uso operativo delle tecnologie di indagine per finalità strategiche – secondo quanto proposto dal presente lavoro – se, da un lato, ha il merito di rappresentare un valido ed 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 dalla presenza di una previsione legislativa *ad hoc* – siano in concreto autorizzate, solitamente in via preventiva, dalla sussistenza di un provvedimento giurisdizionale che

[54] 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.).
[55] Cfr. Cap. II, § *d.*

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.).

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[56] 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 di *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

[56] 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 targetizzata" 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».

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 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.

b. 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 allorquando 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» (Auletta, 1978; Rescigno, 1993, 119), ossia «all’inaccessibilità della sfera intima dell’individuo comprensiva delle sue proiezioni spaziali e comunicative» (Caprioli, 2000,18) (c.d. riservatezza in senso stretto), sia quale «potere di controllare e gestire ogni informazione personale» (Rodotà, 1974, 551) (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* (Rodotà, 2014, 44).

Pur se legate da un rapporto di genere a spese, può dirsi che tanto la riservatezza quanto le *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[57] che, viceversa, trova esplicito riconoscimento nel diritto sovranazionale pattizio nell'art. 8 CEDU e nell'art. 16, paragrafo 1, TFUE[58]: 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, ad un'eccessiva cristallizzazione dei valori tutelati e, dall'altro, ad una ricostruzione riduttiva del concetto di riservatezza» (Marinelli, 2007, 84).

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 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

[57] All'assenza di qualsivoglia tutela costituzionale, la dottrina risponde attribuendogli una protezione "indiretta": a chi ritiene che il suo fondamento sia rappresentato dall'art. 2 Cost., in quanto norma "aperta" «in grado di esprimere la carica espansiva della carta fondamentale» (Baldassarre, 2000, 18; Cautadella, 1964, 2), si contrappone l'orientamento seguito da coloro che lo rintracciano nell'art. 3 Cost., facendo leva sui concetti di «dignità è pieno sviluppo della persona» (Auletta, 1978, 45; Busia, 2000, 123).

[58] 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.

attraverso la quale operare il continuo adeguamento delle garanzie giuridiche esigenze di tutela della persona» (Niger, 2006, 43).

Una volta riconosciuta la dignità costituzionale ai diritti in esame, occorre comprendere se e in che misura tali precetti possano subire una compressione da considerarsi 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, la prevenzione dei reati) o individuali (protezione di diritti libertà altrui)[59].

Segue il ragionamento: se l'ordinamento sovranazionale – e, di riflesso, quello interno, posta la clausola di "adattamento automatico" di cui all'art. 117 Cost. – 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 la 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.

c. 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 (Whitman, 2004).

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» (Cerrina Feroni e Morbidelli, 2018, 1).

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.

[59] 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.

In questo gioco di forze, c'è chi ritiene che l'esigenza di sicurezza che è alla base dell'attività 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» (Dershowitz, 2002, 33) e chi, per converso, ritiene imprescindibile considerare la sussistenza di un nucleo di diritti inviolabili che, indipendentemente dal contesto, non possono subire compressioni (Orlandi, 2016, 17).

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 (Minniti, 2018; Pace, 2014, 551).

Non parendo, 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[60], al fine di evitare l'«eccedenza dell'esigenza di giustizia rispetto alle possibilità di realizzazione umane» (Cartabia, 2018, 50).

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

[60] 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, 334 ss.

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 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 e limiti ordinamentali congegnati per il regolare esercizio delle funzioni statuali tra consociati e istituzioni possano tradursi in ostacoli all'autoconservazione della stabilità democratica affidata al Sistema 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.

CONSIDERAZIONI CONCLUSIVE

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

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 il contrapporsi di 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 ed 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 le fondamenta di 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 l'insieme di 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 ed il ripristino dell'ordinarietà. Ebbene, il compito della Difesa, come dimostrato dall'affidamento della gestione della crisi sanitaria al comparto militare (Gen.le Figliuolo) è proprio quello 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 ad 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 ed 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 interessante 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 ed 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 ed interdicasteriale (Ministero 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"[61] – 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.

Non si discorre di annullare le garanzie costituzionalmente e convenzionalmente poste a protezione dei diritti inviolabili ma di posticipare il sindacato giurisdizionale in una fase successiva qualora l'attività posta in essere sia qualificabile come militare secondo i criteri ermeneutici sopra menzionati.

Più concretamente, si tratta di abbandonare il concetto di "sotto-soglia" e 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 da tratti ontologici che si discostano dall'intervento militare convenzionale (e, dunque, il superamento della causa di giustificazione dello stato di necessità).

Si richiede, quindi, 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 successiva all'attività oggetto di controllo, al fine di 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

[61] Cfr. Cap. II, § ?.

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 ad avvalersi delle capacità multidirezionali (captativo-conservativa, gestionale e operativa)[62] 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 una fase iniziale di collaborazione interforze tra il comparto militare e altri corpi del Sistema Difesa 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.

[62] Cfr. Cap. II, § *b.*

BIBLIOGRAFIA

- Auletta T.A. (1978). *Riservatezza e tutela della personalità.* Milano: Giuffrè.
- Baldassarre A. (1989). Voce “Diritti inviolabili”. *Enciclopedia giuridica*. Roma: Treccani, XI: 10-21.
- Busia G. (2000). Voce “Diritto alla riservatezza”. *Digesto delle Discipline Pubblicistiche.* Torino: Utet, 476-510.
- Caligiuri M. (2016). *Cyber Intelligence: tra libertà e sicurezza*. Roma: Donzelli Editore.
- Caprioli F. (2000). *Colloqui riservati e prova penale*. Torino: Giappichelli.
- Cartabia M. (2018). *Edipo re*. In Cartabia M. e Violante L., a cura di, *Giustizia e mito*. Roma–Bari: Laterza.
- Cautadella A. (1965). Voce “Riservatezza”. *Enciclopedia Giuridica.* Roma: Treccani, XI: 1-12.
- Cerrina Feroni G. e Morbidelli G. (2018). La sicurezza. un valore superprimario*. Percorsi costituzionali,* 1: 10-26.
- Cinelli C. (2020a). *La disciplina degli spazi internazionali e le sfide poste dal progresso tecnico-scientifico*. Torino: Giappichelli.
- Cinelli C. (2020b). Sorveglianza digitale, sicurezza nazionale e tutela dei diritti umani. *Ordine internazionale e diritti umani,* 588-608*.*
- Curtotti D., Rizzi V., Russitto A., Giliberti G., Scarpa G. (2023). Piattaforme criptate e prova penale. *Sistema penale.*
- Dell’Anno P. (2020). Le attività d’intelligence. In: Scalfati A., a cura di, *Pre-investigazioni (Espedienti e mezzi).* Torino: Giappichelli.
- Di Bitonto M.L. (2005). Raccolta di informazioni e attività di intelligence. In: Kostoris R.E. e Orlandi R., a cura di, *Contrasto al terrorismo interno e internazionale*. Torino: Giappichelli.
- Di Liddo M. (2018). La minaccia liquida*. Insurance review.*
- Gelao N. (2023). Intelligence Militare. Testo disponibile al sito *www.ilnuovoterraglio.it.*
- Marrone A., Sabatino E. e Credi O., a cura di (2021). L’Italia e la difesa cibernetica*. Documenti IAI,* 12: 1-52.
- Minniti M. (2018). *Sicurezza è libertà*. Milano: Rizzoli.
- Niger S. (2006). *Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali.* Padova: Cedam.
- Nino M. (2022). La normalizzazione della sorveglianza di massa nella prassi giurisprudenziale delle Corti di Strasburgo e Lussemburgo: verso il cambio di paradigma del rapporto privacy v. security. *Freedom, Security, Justice. European Legal Studies,* 3: 105-133.

- Nino M. (2016). Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE. *Diritto dell'Unione Europea,* 4: 755-777.
- Nocerino W. (2018). *Le intercettazioni e i controlli preventivi sulle comunicazioni. Riflessi sul procedimento probatorio.* Padova: Cedam.
- Nocerino W. (2021a). *Il captatore informatico nelle indagini penali interne e transfrontaliere*. Padova: Cedam.
- Nocerino W. (2021b). Il tramonto dei mezzi di ricerca della prova nell'era 2.0. *Diritto penale e processo,* 8: 1017-1030.
- Orlandi R. (2018). Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma. *Rivista italiana di diritto e procedura penale,* 2: 538-547.
- Orlandi R. (2016). Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali. In: Associazione tra gli Studiosi del Processo Penale "G.D. Pisapia", a cura di, *La giustizia penale preventiva. Ricordando Giovanni Conso*. Milano: Giuffrè.
- Pace A. (2014). Libertà e sicurezza. Cinquant'anni dopo. In Torre A., a cura di, *Costituzione e sicurezza dello Stato.* Santarcangelo di Romagna: Maggioli.
- Pioppi S. (2018). A cosa serve l'intelligence militare? La risposta del ministro della Difesa. Testo disponibile al sito: *www.formiche.net.*
- Pisano V. (2008). L'intervento militare quale moltiplicatore del terrorismo globale? Apporto e limiti delle forze armate e dell'intelligence militare nella lotta contro il terrorismo. Testo disponibile al sito: *www.difesa.it.*
- Rescigno F. (1993). Il diritto all'intimità della vita privata. In: *Scritti in onore di F. Santoro Passarelli.* Napoli: Jovene.
- Resta G. (2015). La sorveglianza elettronica e di massa e il conflitto regolatorio USA/UE*. Diritto dell'informazione e dell'informatica,* 4–5: 23-48.
- Rodotà S. (2014). *Il mondo nella rete. Quali i diritti, quali i vincoli*. Roma–Bari: Laterza.
- Rodotà S. (1974). La privacy tra individuo e collettività. *Politica del diritto*, 545-551.
- Sadiku M.N.O. e Musa S.M. (2021). *Military Intelligence.* Berlino: Springer.
- Signorato S. (2018). *Le indagini digitali. Profili strutturali di una metamorfosi investigativa.* Torino: Giappichelli.
- Trenta E. (2019). Difesa e Sicurezza: prevenire il radicalismo per contrastare il terrorismo. Testo disponibile al sito: *www.difesa.it.*
- Whitman J.Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal,* 1151-1157.

Nota sull'IRAD e Nota sull'Autrice

IRAD[63]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.
Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.
Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Autrice

Wanda Nocerino è dottore di ricerca in Scienze Giuridiche presso l'Università degli Studi di Siena dal 16 dicembre 2020, con valutazione eccellente con lode. Il 25 maggio 2022, ha conseguito (con voto unanime della Commissione) l'abilitazione scientifica nazionale alla funzione di professore di II fascia, di cui all'art. 16 della l. 240/2010.
Attualmente è Ricercatore universitario a tempo determinato, ai sensi dell'art. 24, co. 3, lett. a), Legge 240/2010, con regime di impegno a tempo pieno, per il settore concorsuale 12/G2 "*Diritto processuale penale*" - settore scientifico-disciplinare IUS/16, presso il Dipartimento di Giurisprudenza dell'Università di Foggia.
È autrice di articoli, saggi, note a sentenza, commenti codicistici, aventi ad oggetto molteplici istituti di diritto processuale penale. Ha presentato *poster* in Convegni internazionali sulle scienze forensi. Nel 2018 ha pubblicato una monografia dal titolo "*Le intercettazioni e i controlli preventivi sulle comunicazioni. Riflessi sul procedimento probatorio*" e nel 2021, una seconda monografia dal titolo "*Il captatore informatico nelle investigazioni penali interne e transfrontaliere*", entrambe edite da Cedam, nella collana "*Problemi attuali della giustizia penale*".
È docente presso Scuole dottorali, nonché Corsi di formazione della Polizia di Stato e dell'Arma dei Carabinieri.

[63] http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx


9 791255 150602