CENTRO ALTI STUDI

PER LA DIFESA

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

Istituto Superiore di Stato Maggiore Interforze

25° Corso – 2ª Sezione – 6° Gruppo di Lavoro

"La Law Enforcement Intelligence (LEINT) nel Cyber Domain quale strumento di contrasto avanzato alla minaccia ibrida "

(AS- CC-02)

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 dalla 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.

CENTRO ALTI STUDI

PER LA DIFESA

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

Istituto Superiore di Stato Maggiore Interforze

25° Corso – 2ª Sezione – 6° Gruppo di Lavoro

"La Law Enforcement Intelligence (LEINT) nel Cyber Domain quale strumento di contrasto avanzato alla minaccia ibrida "

(AS-CC-02)

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

Autore
ISSMI – 25º Corso 2ª Sezione 6º Gruppo di Lavoro

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 luglio 2023

ISBN 979-12-5515-045-9

CENTRO ALTI STUDI PER LA DIFESA

ISTITUTO SUPERIORE DI STATO MAGGIORE INTERFORZE

25° CORSO SUPERIORE DI STATO MAGGIORE INTERFORZE

2ª Sezione – 6° GdL

La *Law Enforcement Intelligence* (*LEINT*) nel *Cyber Domain* quale strumento di contrasto avanzato alla minaccia ibrida

Anno Accademico 2022-2023

COMPOSIZIONE DEL GRUPPO DI LAVORO

C.C. (MM)	RIZZO	Pierpaolo	*Presidente*
Magg. (AM)	GIALLAMINE	Giovanni	*Segretario*
Magg. (AM)	BENEDETTI	Gabriele	
Ten. Col. (AM)	DI TRANI	Massimiliano	
Ten. Col. (CC)	CARPINO	Vincenzo	
Ten. Col. (SRB)	GAVRILOVIC	Lazar	
Ten. Col. (MAR)	ELKHADIR	Si Mohamed	
Magg. (EI)	MANCARELLA	Adelaide	
Magg. (EI)	MALVEZZI	Daniele	
Magg. (EI)	NIGRO	Michele	
Magg. (EI)	ROCCHETTI	Denis	
C.C. (MM)	MIZZI	Francesco	
Dott.	PANERO	Emmanuele	

INDICE

ELENCO DEGLI ALLEGATI:

ABSTRACT

Il sistema sicurezza affronta un mondo sempre più complesso, interconnesso ed imprevedibile, attraversato da crescenti instabilità e contraddistinto dal sorgere di nuove minacce trasversali. Un ambiente caratterizzato da elevata volatilità, incertezza, complessità, ambiguità e repentinità dei cambiamenti (V.I.C.A.R.[1]) che lo rendono estremamente indeterminato, privo di riferimenti e quindi di difficile interpretazione. In questo scenario, nuovi strumenti divengono necessari per anticipare, prevenire e contrastare proattivamente lo spettro delle condotte malevole, integrandosi sinergicamente con quelli preesistenti. Proprio in quest'ottica, la combinazione di capacità di *Law Enforcement Intelligence* (LEINT) e di risorse offerte dal dominio cibernetico possono fornire alle operazioni militari, ed in particolare nella condotta di attività di *Stability Policing* (SP) in aree di crisi, un vantaggio significativo nel contrasto avanzato alle minacce ibride. Se infatti la raccolta ed analisi informativa di polizia può contribuire ad ampliare, diversificare e rafforzare il quadro di intelligence, lo spazio virtuale consente di accedere agilmente a quantità rilevanti di informazioni, assicurando un presidio essenziale di un ambiente crescentemente contestato ed ostile.

Il presente studio, partendo dall'analisi del complesso scenario geopolitico contemporaneo e delle sfide poste dal dominio cibernetico, si pone l'obiettivo di inquadrare la LEINT come strumento militare, definendone limiti giuridici ed operativi, nonché valorizzando le opportunità di implementazione ed integrazione con le altre funzioni militari. Nello specifico, dopo aver delineato il quadro operativo di riferimento, esso analizza i principali strumenti di risposta alle minacce di natura ibrida, con preciso riferimento alle attività di *Stability Policing* ed al passaggio dal concetto di *Cyber Defence* a quello di *Cyber Operations*. Alla luce di questi elementi, la ricerca approfondisce il beneficio apportato da attività di LEINT nel dominio cibernetico, dedicandosi poi successivamente a dettagliare tecnicamente e con riferimento a precisi casi studio le specifiche componenti di *Social Media Intelligence* e *Web Intelligence*, per concludere con un riferimento alle prospettive offerte dal fenomeno dei *Big Data* e dalle applicazioni dell'Intelligenza Artificiale. Infine, il lavoro presenta una proposta concreta di implementazione delle attività di intelligence di polizia nel dominio cibernetico alle operazioni di *Stability Policing*, sviluppando il concetto di *SP LEINT Team* ed applicandolo ad un *case study*.

[1] V.I.C.A.R.: Volatili, Incerti, Complessi, Ambigui e Rapidamente mutanti (cfr. l'acronimo VUCA contenuto nella pubblicazione *Strategic Leadership Primer* del *Department of Command, Leadership and Management*, a cura dello *USA War College*).

INTRODUZIONE

La complessità è la misura essenziale dell'epoca contemporanea, segnata dall'intrecciarsi tumultuoso di competizioni geopolitiche, volatilità economiche e sfide sistemiche. Dalle pandemie ai cambiamenti climatici, dai fenomeni migratori alle crisi energetiche, i fattori di disarticolazione della sicurezza internazionale possono determinare effetti a cascata su realtà statuali fragili, favorendo conflitti interni segnati da fratture e frammentazioni etniche, religiose e sociali, sfruttate non di rado da attori esterni. La conseguente instabilità ed insicurezza di Paesi segnati da Istituzioni friabili, isolamento politico e contestato controllo del territorio, è frequentemente il sedime su cui sorgono *hub* criminali e terroristici, fonte prolifica di minacce trasversali agli interessi collettivi.

Il rischio generato da queste attività postula la necessità di iniziative internazionali unitarie e sistemiche, capaci di integrare sinergicamente strumenti, capacità e competenze per generare effetti incisivi su avversari dai centri di gravità multipli e mobili. L'obiettivo della stabilizzazione non può infatti prescindere dal contributo decisivo ed abilitante di tutte le componenti dell'intero sistema sicurezza, al fine di arrestare il propagarsi transnazionale dei fenomeni di instabilità. Un contributo significativo in questa direzione, soprattutto all'interno di strutturati interventi di natura anche militare, è svolto dalle attività di *Stability Policing* (SP), le quali apportano nei teatri di operazione capacità militari di polizia altrimenti assenti.

L'evoluzione dello spettro delle minacce in particolare investe crescentemente i nuovi domini, incluso specificamente quello cibernetico, divenuto teatro, specchio e strumento per le condotte di attori malevoli. L'assenza di limiti fisici e la diversa dimensione umana che contraddistinguono il *cyber*, lo rendono infatti un dominio privilegiato per la condotta di azioni ibride. Questo nuovo fronte richiede di individuare soluzioni avanzate ed attagliate alle esigenze operative al fine di generare effetti incisivi sugli avversari. In questa direzione, l'impiego efficace della *Law Enforcement Intelligence* (LEINT), contestuale ed integrato al riorientamento da una postura reattiva di *Cyber Defence* ad una proattiva di *Cyber Operations* può completare efficacemente le capacità espresse dagli assetti tradizionali.

L'inclusione della componente LEINT nel dominio cibernetico alle attività di *Stability Policing*, alla luce del mutevole quadro operativo di riferimento, è l'oggetto centrale del presente studio. Partendo infatti da una minuziosa attività di ricerca, analisi e comparazione delle scarse risorse sviluppate sul tema in ambito NATO e di singole Nazioni, nonché con il contributo decisivo del NATO SP *Centre of Excellence* di Vicenza, promotore attivo della questione negli ultimi anni, esso mira a inquadrare la LEINT come strumento militare. Nello specifico, il lavoro, partendo dall'analisi del complesso scenario internazionale e del nuovo

dominio di riferimento, intende definirne limiti giuridici ed operativi, valorizzandone le opportunità di implementazione ed integrazione con le altre funzioni militari, sia quale strumento di prevenzione e contrasto alle minacce ibride, sia in chiave repressiva quale contributore effettivo alle attività di intelligence nel loro complesso. A questo fine, sono approfondite, con puntuale riferimento a casi studio di attività condotte nell'ambito del contrasto a terrorismo e criminalità organizzata transnazionale, soprattutto le caratteristiche degli aspetti di *Social Media Intelligence* e *Web Intelligence*, nonché, in prospettiva, le possibilità derivanti dallo sfruttamento dei *Big Data* e dalle applicazioni dell'Intelligenza Artificiale allo specifico settore.

In conclusione, supportati dalle risultanze analitiche, la ricerca intende non solo contribuire all'evoluzione dell'approccio alla raccolta informativa in scenari di instabilità, ma si propone di fornire un concreto contributo all'inclusione di capacità LEINT nelle attività di *Stability Policing*. In questa prospettiva, essa fornisce dunque un pragmatico esempio di un possibile assetto dispiegabile, delineandone le caratteristiche in termini di personale, risorse e competenze necessarie, nonché di compiti e funzioni assegnabili.

Capitolo I: UNO SCENARIO COMPLESSO

1. La Crescente Instabilità del Contesto Internazionale

Fragilità regionali e locali sono alla base della crescente instabilità del contesto internazionale. Tra il 2012 e il 2019, infatti, si è assistito ad un ricorrente riorientamento delle priorità di difesa e sicurezza dell'area Euro-Atlantica. L'invasione della Crimea ha messo in luce il fallimento definitivo della politica dell'*engagement* con la Russia portata avanti da varie amministrazioni americane. In seguito alle primavere arabe l'instabilità si è estesa lungo tutto l'arco dell'area *Middle East and North Africa* (MENA) contestualmente al sorgere e radicarsi di cellule terroristiche di matrice islamista ed in particolare di ISIS. Nell'ultimo ventennio si è, inoltre, verificato gradualmente uno spostamento dell'orientamento strategico statunitense verso l'Indo-pacifico con politiche nazionali e accordi multilaterali lasciando la responsabilità della difesa del vecchio continente agli alleati europei che hanno dimostrato un impegno crescente nell'adempimento dei propri obblighi in ambito NATO con uno sforzo teso al conseguimento della soglia del 2% del PIL destinato alla Difesa. Nonostante questo riorientamento mirato al rafforzamento del fianco est il cui massivo trasferimento di armi a favore del governo ucraino ne è la prova tangibile, in seno l'alleanza restano irrisolte alcune croniche criticità: le difficoltà nella gestione del *burden sharing,* già rappresentate dalle Amministrazioni Obama e Trump, l'arretratezza dei sistemi d'arma[2] di molti Paesi europei, rispetto agli standard concordati in sede NATO, e la frammentazione di posizioni tra i suoi stessi membri, eterogenei percettori della minaccia ovvero di una difforme esigenza di sicurezza, in merito alle prioritarie finalità dello strumento atlantico. Se per la NATO, del Vertice di Londra 2019, la Cina poteva rappresentare ancora una opportunità per l'Alleanza, nel 2022 il nuovo Concetto Strategico dichiara apertamente la pericolosità delle operazioni ibride e informatiche della Repubblica Popolare Cinese che con la sua retorica conflittuale e la disinformazione mina gli alleati a danno della loro sicurezza[3].

L'invasione dell'Ucraina da parte della Fed. Russa ha ampliato la divaricazione degli interessi tra Stati Uniti e Paesi europei, con i primi sempre più orientati globalmente al contenimento della potenza competitrice cinese in netta ascesa ed i secondi alle prese con una crisi d'identità aggravata dal conflitto alle porte.

La guerra attualmente in corso in Ucraina sembra assumere le sembianze di un conflitto classico, convenzionale, simmetrico, ad alta intensità e su vasta scala tra eserciti

---

2 https://www.esercito.difesa.it/comunicazione/Le-5-Sfide/Pagine/pagina-capacita-e-sistemi.aspx

3 NATO *Strategic Concept 2022* - 13. «*The People's Republic of China's (PRC) stated ambitions and coercive policies challenge our interests, security and value[...]. The PRC's malicious hybrid and cyber operations and its confrontational rhetoric and disinformation target [...]*».

regolari (sia pure affiancati da gruppi militari privati) che cercano di conquistare territori e posizioni di vantaggio facendo largo uso di mezzi corazzati e artiglieria pesante: insomma, un conflitto che ha inopinatamente riportato nel cuore dell'Europa la guerra tradizionale, in una forma che sotto molti aspetti ricorda i due conflitti mondiali[4].

D'altro canto, il conflitto russo-ucraino è contraddistinto da aspetti tipici delle cosiddette "nuove guerre" – spesso definite con l'espressione diffusa di "guerre ibride" – caratterizzate dalla contemporanea azione di forze regolari e di attori privati e semi-privati (come i *foreign fighters*, i mercenari del Gruppo *Wagner* e i *kadyrovcy* ceceni). Questo allargamento del conflitto si riflette anche nella scelta delle strategie di attacco con il ricorso a un'ampia varietà di strumenti non convenzionali quale la tattica dell'*energy weaponization* con l'uso strumentale del gasdotto *Nord Stream 2*[5] quale arma di pressione, l'impiego massiccio di droni e di altri sistemi d'arma *hi-tech*. Il conflitto russo-ucraino nella sua declinazione ibrida – interpretata a pieno ed a tratti eccessivamente enfatizzata dalla *leadership* di Volodymyr Zelenskyy – sta dimostrando anche ai più scettici l'importanza strategica della condotta delle operazioni nel dominio cibernetico (*hackering*) e in quello cognitivo (*psyops*), proiettando l'arte della guerra in una dimensione virtuale dove si combatte per influenzare i "cuori e le menti" con le lame affilate degli strumenti *Social* e delle *Info Ops,* capaci di amplificare la portata di eventi bellici circoscritti a fenomeni di risonanza globale.

2. NATO *Strategic Concept* 2022 e Concetto del Capo di Stato Maggiore della Difesa

In armonia con gli indirizzi forniti dal Concetto Strategico NATO 2022, dal Concetto strategico del CaSMD 2022 e nelle più recenti Linee Programmatiche del Ministro della Difesa 2022, entro il 2026, la Difesa dovrà consolidare le sue capacità di condurre operazioni interforze con la costituzione di una Forza di intervento in grado di operare in tutti i domini, *cyber* e spazio inclusi, autonomamente o integrata in dispositivi multinazionali, su scala regionale. Al fine di garantire la massima efficacia e interoperabilità nell'ambito delle Organizzazioni Internazionali di riferimento, lo strumento militare deve perfezionare la propria visione strategica e la propria *policy* in riferimento alle nuove dimensioni del confronto strategico, anche prevedendo aliquote di forze dedicate, generate da ciascuna Forza Armata e collocate sotto Comando interforze. Se, fino a qualche anno fa, l'ambiente *cyber* era considerato un abilitante dei domini classici, grazie alla presenza di sistemi in grado di fornire servizi vitali a supporto delle operazioni militari, oggi è divenuto un dominio

[4] Alessandro Colombo, Paolo Magri e Giampiero Massolo, *Ritorno al Futuro*, Rapporto ISPI 2023.
[5] Anders Åslund, *Europe can win Putin's gas war but must learn Nord Stream lessons*, Atlantic Council, 6 Settembre 2022.

operativo a tutti gli effetti. Ciò impone di dotarsi di un nuovo *mindset*, che trascende la sola dimensione tecnologica apportata dal nuovo dominio, ma che investe tridimensionalmente l'aspetto umano dello stesso, implicando lo sviluppo di capacità e competenze, anche di Comando, tese ad uno "scetticismo attivo" integrante la dimensione cognitiva e STRATCOM[6]. Parallelamente è necessario assicurare, con visione unitaria, la protezione dei sistemi satellitari militari nazionali e di quelli civili in ambito Europeo e NATO. È quindi necessario perseguire l'obiettivo di consolidare e incrementare le capacità militari già esistenti (SATCOM, OT e PNT)[7], sviluppare sensori e capacità di osservazione e analisi necessarie per comprendere ciò che avviene nel dominio spaziale. In tale ottica ed in una prospettiva futura a più ampio respiro, è opportuno dunque investire e valutare la possibilità di dotarsi di una capacità autonoma di accesso allo spazio, anche in virtù della "spinta miniaturizzazione" di talune tipologie di satelliti. Nell'ambito di un'azione coordinata con tali Enti, sarà importante acquisire la capacità di condurre l'intera gamma delle operazioni *cyber*, anche attraverso il coinvolgimento del mondo accademico e del comparto industriale nazionale. Tra le capacità più richieste, quelle computazionali e di memorizzazione centralizzate che assicurino la piena interoperabilità tra i sistemi in uso per l'analisi e la valorizzazione dei dati in un unico ambiente. Tuttavia, non è possibile generare una concreta capacità multi dominio[8] della Difesa prescindendo da una decisa e coordinata accelerazione del già avviato processo di integrazione interforze, destinato, giocoforza, ad essere superato e compreso nello stesso concetto di *Multi-Domain Operations*[9]. Dette potenzialità troveranno la loro massima espressione se abbinate a una capacità di comprendere con largo anticipo gli obiettivi e le azioni complessive dei potenziali avversari. I mutamenti nell'ordine internazionale, quali il ritorno della competizione tra le grandi potenze, l'emergere di potenze revisioniste e una globalizzazione sempre più fragile, ulteriormente accentuati dall'aggressione russa all'Ucraina, in corso dal 24 Febbraio 2022, richiedono una strategia integrata comune.

L'attuale conflitto, così come la periodica necessità di riadattarsi al contesto internazionale, hanno portato la NATO a delineare l'ambiente strategico (*Strategic environment)* in cui l'Alleanza si trova ad operare, individuando le sfide e le minacce alla sicurezza nei tre campi di azione principali dell'Alleanza:

- difesa e sicurezza collettiva;

---

6 STRATCOM (*Strategic Communication*) integrazione delle capacità comunicative e informative con altre attività militari tese a comprendere e modellare l'ambiente informativo a supporto dello scopo e degli obiettivi della NATO.

7 SATCOM indica l'insieme dei satelliti e delle apparecchiature di bordo su navi, aerei e stazioni terrestri, inserite a sua volta nella rete di telecomunicazioni mondiale.

8 Rfr. Approccio della Difesa alle Operazioni Multidominio ed.2022 pag. 1.

9 Ibidem

- prevenzione e gestione delle crisi;
- sicurezza cooperativa.

Per quanto attiene il primo campo d'azione, si evidenzia il richiamo dell'art.5 del Patto Atlantico, che prevede la solidarietà tra membri in caso di aggressione. Tuttavia, se precedentemente era possibile invocare il menzionato articolo solo in un contesto di aggressione armata e scenari che avevano al centro *la hard security*[10], il suo campo è stato esteso a terrorismo e minacce asimmetriche[11]. Il nuovo Concetto formalizza la possibilità di invocare l'art. 5 anche in caso di cyberattacchi che possano produrre gli stessi effetti di un attacco convenzionale. Sarà importante seguire gli sviluppi in questo campo, dal momento che il Concetto incarica gli strateghi di elaborare una dottrina sul *cyberwarfare*[12]*.* L'Alleanza aveva iniziato a muoversi in questa direzione, con il programma DIANA (*Defence Innovation Accelerator for the North Atlantic*), per affinare le tecnologie militari dell'Alleanza. Il progetto intende affiancare alle figure tradizionali del mondo della difesa i professionisti delle *start-up*, ricercatori e società private. Il programma sarà avviato dal 2023.

3. Minacce Nuove, Ibride e Trasversali

Negli ultimi anni la situazione delle minacce è cambiata notevolmente. Questo traspare, in particolare, per il deterioramento duraturo delle relazioni tra Occidente e Russia sulla scia della crisi ucraina, per l'intensificarsi della minaccia del terrorismo jihadista e per la portata delle attività illegali e dell'uso improprio nel *cyber*-spazio. Le minacce e i pericoli nel loro complesso sono diventati ancora più complessi, interconnessi e indefiniti.

Una sfida peculiare per la sicurezza è rappresentata dalla combinazione o dalla concatenazione delle varie minacce, cosa che conferisce ad esse il carattere trasversale ovvero la capacità di rivolgersi ad ognuna delle cinque dimensioni (riconosciute attualmente dalla dottrina NATO e USA) impiegando strumenti diplomatici, informativi, militari ed economici (DIME) per conseguire gli obiettivi designati, contestualmente incidendo diffusamente negli ambiti politico, militare, economico, sociale, infrastrutturale ed informativo (PMESII).

---

[10] Rfr. In https://www.agid.gov.it/ L'insieme delle tecnologie e dei processi utilizzati per garantire la protezione di reti, sistemi operativi, programmi e dati da attacchi, danni o accessi non autorizzati (ultimo accesso il 18/02/23).

[11] Conflitto ad armi impari, non dichiarato, nel quale una delle parti è costretta a difendersi da un nemico non identificabile, trovandosi in situazione di palese svantaggio.

[12] Rfr. Cyber War. "La guerra prossima ventura" di Alessandro Curioni e Aldo Giannulli, ed.2019 p.10-11 «Per comprendere la natura della cyber war dobbiamo concentrarci sul termine cyber. L'etimologia rivela che si riferisce alla costruzione di macchine in grado di riprodurre le funzioni del cervello umano e più in generale a sistemi capaci di autoregolarsi attraverso input e output di comando e di controllo idonei a sviluppare alti livelli di automazione di attività complesse».

Il carattere primario di queste minacce si concreta nella natura ibrida che le contraddistingue come evidenziato dalla definizione fornita dallo *European Parliament Research Service* (EPRS) che afferma che «una minaccia ibrida è un fenomeno derivante dalla convergenza e dall'interconnessione di elementi diversi che concorrono a formare un pericolo imminente complesso e multidimensionale». La loro trasversalità rispetto ai domini operativi ed il ricorso a strategie "escalatorie" e "deescalatorie", rende il *cyber*spazio particolarmente impiegabile per le sue caratteristiche intrinseche. Dati i diversi livelli di intensità e di intenzionalità che compongono la minaccia, l'EPRS distingue tra la definizione di conflitto e guerra ibrida, per cui la prima individua una situazione in cui le parti astenendosi dall'uso delle Forze armate fanno affidamento sull' intimidazione militare (pur non al livello di un attacco convenzionale), sfruttamento delle vulnerabilità economiche, politiche e tecnologiche, rimanendo al di sotto della soglia della guerra dichiarata formalmente; nella seconda accezione un paese ricorre all'uso delle Forze armate contro un soggetto politico statuale o meno, oltre che all'attivazione di altri mezzi (economici, politici, diplomatici, tecnologici).

La definizione di «minacce ibride» rimane dunque flessibile anche nella sua dimensione giuridica, assecondandone la natura multiforme ed in continua evoluzione. Il concetto generale mira dunque a delineare l'insieme di attività coercitive e sovversive, metodi convenzionali e non posti in essere da attori statuali o meno per destabilizzare un avversario, sebbene non dichiarato formalmente come tale. La «minaccia ibrida» è dunque identificata da nozioni più ampie che designano il verificarsi di minacce simultanee alla sicurezza. Secondo l'EPRS, tale concetto può spiegare situazioni diversificate, inclusi atti terroristici e di gruppi criminali armati, azioni contro la sicurezza informatica, controversie marittime, limitazioni all'uso dello spazio orbitale, atti economici ostili, operazioni militari coperte. Per questo motivo l'Unione Europea ha spesso focalizzato l'attenzione sul concetto di minaccia, non necessariamente sovrapponibile a quello di guerra ibrida, al fine di prevenire gli attacchi alla sicurezza dello spazio comune, senza trascurare al contempo il concetto di guerra ibrida, che si fonda su attività eterogenee, violente e non, non trascurando peraltro i paradigmi individuati dalla NATO.

Sebbene non esista una definizione univoca di minaccia ibrida, la NATO ricorre a questo termine per descrivere avversari capaci di impiegare contemporaneamente mezzi convenzionali e non-convenzionali adattandoli alle caratteristiche dei propri obiettivi.

La nozione di minaccia ibrida è stata difatti molto controversa da quando è entrata a far parte del lessico della Difesa. Parte della dottrina la definisce, semplicisticamente, come l'ultimo termine utilizzato per identificare i metodi irregolari o asimmetrici per combattere

contro una forza convenzionale superiore. Invero, nel corso degli anni, sia *insurgents* che Stati-Nazione hanno impiegato combinazioni molto creative di capacità convenzionali e non per raggiungere i propri obiettivi. I critici restano, però, dell'idea che la locuzione minaccia ibrida sia troppo astratta, correndo il rischio di utilizzarla come termine generale per descrivere tutte le minacce non lineari e convenzionali. Tuttavia il termine ibrido è stato utilizzato per descrivere formazioni amiche, come per esempio ha fatto il Comando delle *Special Forces* USA, per descrivere strutture e organizzazioni che mettono a sistema l'impiego delle forze speciali con le forze convenzionali.

I sostenitori del concetto di minaccia ibrida affermano che gli attori che utilizzano questo tipo di minaccia stiano creando un differente modo di fare la guerra utilizzando il nuovo campo di battaglia del XXI secolo, i *social network*, che sono impiegati secondo metodologie che non ricalcano quelle convenzionali comunemente utilizzate in guerra. Frank G. Hoffman, uno dei teorici più attivi nello sviluppo di nuovi concetti strategici capaci di contrastare la minaccia ibrida, è stato il primo a proporre un elenco di quelle che possono essere definite le caratteristiche proprie di questo tipo di minaccia:

a. insieme di tattiche di combattimento – la minaccia ibrida usa un insieme di tattiche convenzionali e non convenzionali unite con attività criminali e terroristiche;
b. simultaneità – avversari ibridi che utilizzano metodologie differenti di conflitto simultaneamente ed in maniera coerente e coordinata;
c. fusione – la minaccia ibrida vede l'impiego contemporaneo di militari professionisti, terroristi, guerriglieri, e organizzazioni criminali;
d. criminalità – la minaccia ibrida usa attività criminali per sostenere le proprie operazioni e, talvolta, le utilizza palesemente come metodo di conflitto.

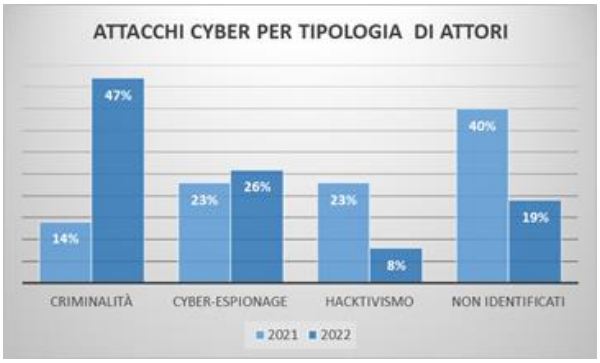
4. Le Sfide del Dominio Cibernetico

Tra l'ampio spettro di minacce presenti nello scenario contemporaneo, quelle che si riversano nel dominio cibernetico mostrano aspetti complessi e al contempo sfidanti per il comparto *Intelligence*, non solo per la loro pervasività, ma anche in merito all'attribuibilità. La minaccia perpetrata nel cyberspazio presenta infatti sfide peculiari attinenti anche la sua dimensione giuridico-dottrinale (*lawfare*), comportando proprio per tale ragione il suo ricorrente impiego da parte di attori come la Federazione Russa, al fine di permanere, nel caso di specie, al di sotto della soglia dell'art. 5 del Trattato dell'Atlantico del Nord (NATO). Ciò connota una trasversalità delle finalità degli attacchi che possono coinvolgere il Sistema Paese, quali le relazioni geopolitiche, il terrorismo internazionale, l'immigrazione irregolare, l'eversione, gli estremismi e la criminalità organizzata, cui si aggiunge anche la sfida

ambientale. Divengono quindi sostanziali le operazioni di *cyber-intelligence*, finalizzate tramite una sistematica azione di monitoraggio, alla tempestiva rilevazione, alla prevenzione e al contrasto, che in Italia sono attività precipue degli Organismi del Sistema di Informazione per la Sicurezza della Repubblica (SISR).

Nella relazione annuale sulla politica dell'informazione per la sicurezza del 2022, l'attività info-operativa condotta dall'intelligence ha rilevato un sensibile incremento di atti illeciti di natura *cyber* per fini criminali (attestatisi al 47% del totale degli attacchi) su filiere energetiche, dei trasporti e dei servizi governativi, soprattutto connessi al conflitto russo-ucraino, volti a discreditarne la reputazione internazionale. Tra questi, il prototipo di attacco preminente ma anche remunerativo, è quello *ransomware*[13] (28% del totale di *malware* utilizzati) non finalizzato unicamente all'indisponibilità del dato tramite crittografia ma alla divulgazione dello stesso nel *Deep*[14] *Web* e *Dark Web*[15].

Le significative campagne *ransomware*, condotte da gruppi criminali e da attori strutturati sponsorizzati, in taluni casi, da entità statuali, hanno distolto *in primis* l'attenzione di organi statuali e privati deputati alla *cybersecurity* sulle attività di spionaggio cibernetico e dall'altro, il massiccio traffico generato in rete ha permesso l'occultamento delle operazioni di raccolta informativa o di *exploitation* delle vulnerabilità.



Non mancano tuttavia impieghi di tale tipologia di armi direttamente da entità statuali (pari al 26% del totale) con lo scopo di interrompere attività produttive piuttosto che occultare tracce di attività informativa o indiretta (*state-sponsored*) facendo ricorso a gruppi cyber-criminali a cui era delegata l'esecuzione dell'operazione di spionaggio ovvero lo sviluppo del *software* malevolo, affinché sia ulteriormente incrementato il grado di anonimizzazione così da rendere più complessa l'attribuzione. Da ciò emerge la complessità del processo di attribuzione di una operazione *cyber* (pari al 40% del totale nel 2021 e in tendenza decrescente nel 2022, ascrivibile alle accresciute capacità di rilevamento sviluppate da AISE e AISI), ovvero una sfida per chi è

[13] Def. tratta da "Glossario Intelligence" di maggio 2019: Malware che cifra i file presenti sul dispositivo della vittima, richiedendo il pagamento di un riscatto per la relativa decodifica. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti che paiono legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

[14] Il *Deep Web* (o Web Sommerso) è l'insieme delle risorse informative del *World Wide Web* non indicizzate dai normali motori di ricerca.

[15] Il *Dark Web* è una piccola parte del Deep Web costituito da *Darknet* includenti piccole reti, *friend to friend peer-to-peer*, nonché reti grandi come Tor, Freenet, e I2P, in cui operano organizzazioni pubbliche e singoli individui.

deputato all'analisi, riconducibile alla natura intrinseca del dominio, de-territorializzato, transnazionale, mutevole, fluido e sul quale influisce fortemente lo sviluppo tecnologico degli attori.

La peculiarità del *cyberspace* è essenzialmente dovuta al fatto che tale dominio non è un *global common* puramente naturale come gli altri, ma una realtà ibrida. Ne consegue che alla sua formazione concorrono sia elementi naturali che virtuali. Un modo utile per comprendere la sua natura ibrida – secondo Martin C. Libicki – è rappresentarla su tre livelli. Il livello fisico è costituito dagli elementi materiali, i cavi a fibra ottica, i satelliti, i router, le antenne, ecc. Tale livello può essere interrotto o rimosso attraverso classiche operazioni cinetiche. Il livello sintattico: in posizione superiore rispetto a quello fisico, è costituito dalle informazioni e dalle istruzioni che i progettisti e gli utenti danno allo strumento informatico; si tratta in particolare, dei protocolli operativi per mezzo dei quali i computer o le macchine interagiscono con le infrastrutture di riferimento e con altri dispositivi. In questo strato del *cyberspace* si possono verificare azioni c.d. *hacking* ovvero, individui *outsider* che possono introdursi nel sistema per affermare la propria autorità ai danni di progettisti e di utenti. Il livello semantico: rielabora i dati contenuti nelle macchine. Libicki raffigura il *cyberspace* attraverso una triplice stratificazione: fisica, logica e sociale così come riportato nella Figura 1.

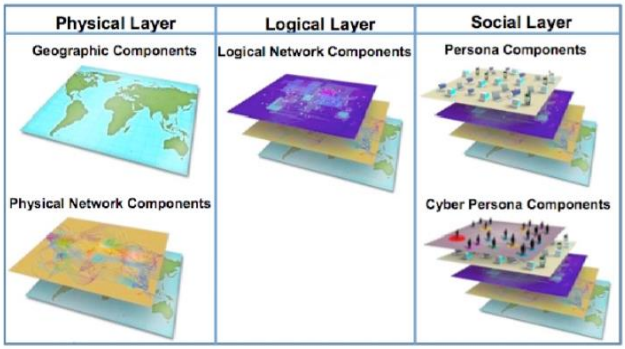


Figura 1: Triplice stratificazione dello spazio cibernetico secondo Libicki.
Fonte: *Department of the Army Headquarters, United States Army*.

Un ulteriore fattore di complessità è dato dalla crescente registrazione di azioni prodromiche a potenziali successivi attacchi a cui non è possibile attribuire una chiara finalità, ma che denotano una strutturata pianificazione. Le *Advanced Persistent Threat* (APT) sono un esempio di questa tipologia di minaccia, con finalità di *cyber espionage,* che nella maggior parte dei casi è condotta contro le cosiddette infrastrutture critiche, strategiche per le Nazioni, che interessano settori dalle telecomunicazioni all'industria della Difesa. Difatti, da quanto emerge dal resoconto 2022 della Polizia postale e delle comunicazioni e

dei Centri operativi sicurezza cibernetica, gli attacchi rivolti alle infrastrutture critiche informatizzate dell'Italia sono aumentati del 138% nel corso del 2022 rispetto all'anno precedente (12.947 contro 5.434).

Se intrinsecamente l'azione illecita esercitata da/attraverso/verso il *cyber* spazio rappresenti un certo grado di complessità, l'eterogeneità degli attori in grado di esercitare un atto ostile cibernetico nei confronti di una entità statuale rende emblematica la difficoltà dell'analisi *ex post*. La minaccia *cyber,* in altri termini, è il metodo paradigmatico del conflitto asimmetrico, considerando che possa esser attuata da cyber-terroristi, cyber-attivisti, cyber-criminali, mercenari, gruppi armati organizzati, fino agli *Script Kiddy,* giovani che mettono alla prova le proprie capacità svolgendo azioni poco dannose ma di grande impatto mediatico. Si evidenzia, inoltre, come sia in corso un progressivo spostamento dottrinale dal concetto di attribuibilità a quello di associazione, afferente all'aderenza del modello di attacco condotto con una determinata fonte, piuttosto che all'attribuzione della sua concreta pianificazione ed esecuzione ad un preciso soggetto.

Oltre alla problematica dell'attribuzione, dovuta anche all'*entry cost* di accesso allo strumento cibernetico relativamente basso e alle diversificate possibilità di agire segretamente o addirittura delocalizzarsi in posti diversi, l'attacco può portare con sé interrogativi relativi all'immediatezza e nello specifico al nesso di causalità tra azione condotta ed effetti manifestati, rendendo difficile procedere alla quantificazione immediata del danno. A differenza di un attacco convenzionale, che richiede un tempo di organizzazione e di esecuzione che ipoteticamente, potrebbe essere intercettato nella sua imminenza, l'attacco *cyber,* per sua natura, viene individuato, a volte, al momento della produzione degli effetti, talora anche irreversibili.

Appare quindi evidente come l'attività di monitoraggio preventivo, sia da società di sicurezza nazionali sia da articolazioni tecniche estere e privatistiche, sia fondamentale non solo in termini di contrasto agli attacchi informatici, ma anche di controllo delle attività di propaganda terroristica e finanziamenti illeciti, nonché verso le principali direttrici dei flussi migratori e alle aree regionali di instabilità. Benché la cooperazione internazionale in questo settore sia a volte critica a causa dei diversi ordinamenti interni, del disomogeneo livello tecnologico e dalla volontà preservatrice di una sovranità informativa in seno agli Stati, sembrerebbe che i tempi siano maturi per creare un unico ambiente internazionale sicuro, almeno tra i Paesi *like-minded,* superando la Convenzione sulla criminalità informatica di Budapest del 2001 che rappresenta una guida all'elaborazione di una legislazione completa per combattere la criminalità informatica, nonché un quadro per la cooperazione tra i gli Stati

partecipanti anche attraverso programmi di creazione di competenze come il progetto GLACY (*Global Action on Cybercrime*).

A supporto della linea collaborativa vi è, inoltre, la portata globale della minaccia che nel *dark web* e con le innovazioni nei servizi finanziari, reperisce nuovi metodi di finanziamento quali il *crowdfunding,* le *crypto*-valute, il *new digital payment* e l'*Informal Value Transfer Systems*, in una commistione di circuiti economici legali e gruppi organizzati criminali e terroristici.

Prevenire ciò, oggi significa necessariamente analizzare grandi agglomerati di informazioni detti *Big Data* la cui interpretazione necessita della primigenia forma di intelligence: quella umana. Il ruolo dell'analista di intelligence permane infatti centrale, per i necessari requisiti di competenza multisettoriale ed esperienza professionale, necessari alla corretta interpretazione delle informazioni, anche qualitativamente e quantitativamente elaborate dal ricorso a tecnologie avanzate. D'altra parte, si valuta che negli anni aumenterà sempre di più il divario tra le identità virtuali e quelle fisiche, mentre i dispositivi connessi ad internet (c.d. *Internet of Things*) già nel 2022 circa 17 miliardi, poco più di due dispositivi per ciascun abitante del pianeta, nel 2025 arriveranno a 22 miliardi. Ogni attività svolta nel cyberspazio diviene forma e sostanza nei *Big Data*, assumendo la forma intangibile di un potente e selettivo microscopio sociale del comportamento umano, sia individuale che collettivo. Attraverso l'analisi dei *Big Data*, l'osservazione delle relazioni instaurate sui *social network* o durante la telefonia mobile consente la precisa ricostruzione della rete delle relazioni personali e l'intensità dei rapporti. Da qui, l'utilizzo di tecniche proprie della *Network Science*[16]. Per sfruttare le potenzialità informative dei *Big Data* è fondamentale che l'intelligence, affiancando in ausilio sistemi di Intelligenza Artificiale, istituisca e formi dei *data scientist*, operatori con una elevata capacità di gestione, acquisizione, organizzazione e contestualizzazione delle informazioni, ma anche in grado di sapere quali e come estrarre i dati dai diversi dispositivi ed infine come renderli intellegibili ad uso del comparto. Una figura professionale multidisciplinare, in grado di individuare e valorizzare le informazioni preziose nascoste nei *Big Data*, con l'ausilio di algoritmi ed analisi statistiche avanzate fornite dall'Intelligenza Artificiale.

5. Dalla Cyber Defence alle Cyber Operations

La c.d. guerra cibernetica rappresenta la più grave forma di attacco informatico perpetrato da uno Stato nei confronti di un altro Stato per uno qualsiasi degli scopi

[16] La network science (scienza delle reti) è una disciplina che si occupa dello studio delle reti complesse come le reti di telecomunicazioni, le reti biologiche, Internet, e le reti sociali.

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*), intesa come l'insieme della dottrina, dell'organizzazione e delle attività atte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti tramite lo spazio cibernetico.

La letteratura scientifica che si occupa di questo argomento è solita far risalire all'attacco all'Estonia del 2007 il primo caso di *cyber war*. Per alcuni giorni i siti istituzionali e di comunicazione dell'Estonia, uno dei paesi al mondo maggiormente informatizzato, sono stati messi fuori uso a seguito di alcuni attacchi cibernetici. Questo il primo caso in cui uno Stato membro della NATO ha richiesto l'applicabilità dell'art. 5 del Trattato istitutivo dell'Alleanza Atlantica, a seguito di un attacco di natura telematica alle proprie strutture digitali.

La guerra e la difesa cibernetica tra Stati sono, ad oggi, eccetto alcune avvisaglie, uno scenario soltanto possibile, pur tuttavia un numero crescente di analisi strategiche individua nello spazio cibernetico un nuovo fondamentale campo di battaglia e di competizione geopolitica dell'umanità[17]. In tali analisi è infatti ricorrente l'affermazione secondo la quale «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»[18].

Gli attacchi cibernetici più sofisticati non solo sono potenzialmente in grado di danneggiare o paralizzare il funzionamento di gangli vitali dell'apparato statale e la fornitura di servizi essenziali ai cittadini, ma possono avere anche effetti potenzialmente distruttivi (soprattutto in prospettiva) se impiegati per indurre il malfunzionamento delle infrastrutture critiche (ad esempio centrali elettriche, nucleari, dighe, torri di controllo aeroportuali, sistemi di navigazione aerea e di trasporto civile, sistemi di comando e controllo militari, nonché fabbriche altamente automatizzate, che impieghino robot interconnessi) generando danni materiali ingenti e la potenziale perdita di vite umane.

In un contesto di *cyber war* la minaccia cibernetica può dunque manifestarsi sotto diverse forme. In alcuni casi potrebbe, ad esempio determinare un'errata percezione da parte dei Comandanti della situazione operativa tale da influire in maniera viziata le scelte di comando e controllo dei propri assetti; in altri, la minaccia cibernetica potrebbe consistere in un'intrusione nei sistemi di comando e controllo finalizzata non solo allo spionaggio, ma

[17] Cfr. Programma dell'indagine conoscitiva sulla difesa e sicurezza dello spazio cibernetico.
[18] Cfr. Libro bianco per la difesa e la sicurezza internazionale 2015.

anche al sabotaggio e al malfunzionamento degli stessi con effetti distruttivi analoghi a quelli condotti con armi convenzionali.

L'estensione dei domini d'azione a quello cibernetico e dello spazio comporta infatti che a tali ambiti siano dedicate specifiche capacità operative difensive, al fine di preservare la sicurezza del Sistema Paese e di rafforzare la tenuta delle strutture politiche, economiche e sociali. La Difesa italiana, al pari dei principali Paesi della comunità internazionale, sta da tempo rafforzando le proprie capacità militari nel dominio cibernetico attraverso apposite strutture di comando e controllo per lo svolgimento di operazioni nel *cyber space*, dotandosi di specifici strateghi per valutazioni militari nello specifico settore e di un quadro normativo che, di fatto, recependo direttive comunitarie, ha creato una cornice di sicurezza cibernetica (composta da Uffici strategici e norme dedicate alla specifica materia) idonea a fronteggiare le sfide di questo nuovo dominio.

Nel quadro strategico nazionale per la sicurezza dello spazio cibernetico è stato previsto che spettasse al Ministero della Difesa definire e coordinare la politica militare, la *Governance* e le capacità militari nell'ambiente cibernetico, pianificare, condurre e sostenere operazioni (*Computer Network Operations* – CNO) nello spazio cibernetico atte a prevenire, localizzare, difendere (attivamente e in profondità), contrastare e neutralizzare ogni possibile minaccia e/o azione avversaria cibernetica, portata alle reti, ai sistemi ed ai servizi della Difesa sul territorio nazionale o nei teatri operativi fuori dai confini nazionali, nel quadro della propria missione istituzionale. In base al Piano nazionale per la protezione cibernetica, nel 2017 è stato costituito il Comando Interforze per le Operazioni Cibernetiche (CIOC) per adempiere alle citate funzioni di protezione delle reti strategiche e tattiche della Difesa dalle quali dipende l'esercizio della capacità di comando e controllo. Da collegare all'istituzione del CIOC la definizione di un apposito protocollo d'intesa attraverso il quale il Comparto intelligence e lo Stato Maggiore della Difesa hanno elaborato un quadro strategico e tattico tale da permettere il miglior posizionamento del costituendo CIOC con riguardo all'operatività nel dominio digitale, anche alla luce dell'esperienze in corso di sedimentazione nell'Alleanza Atlantica.

Per quanto concerne la protezione delle reti, la Difesa si avvale di due tipi di dominio di rete: l'uno chiuso, per le informazioni classificate; e l'altro aperto, cioè in collegamento con la rete di pubblico accesso e con internet, per le informazioni non classificate. Le diverse Forze armate condividono la componente materiale dell'infrastruttura di rete (il *layer* fisico, ossia il supporto trasmissivo, la rete fisica).

Ogni Forza Armata è poi organizzata col proprio dominio e ha la sua rete intranet, federata con le altre e con quella dell'area di Vertice interforze in una relazione di *trust*

reciproca rendendo così i servizi interoperabili come se si trattasse di un'unica rete. Inoltre ogni Forza Armata ha costituito un proprio CERT per la tutela dei rispettivi sistemi informatici, mentre la difesa nel suo insieme ha costituito un CERT Difesa, che ha il compito di prevenire la minaccia cibernetica, rilevare le attività di natura malevola e reagire contro gli incidenti informatici che interessano il sistema della Difesa nel suo insieme.

Su queste strutture la Difesa ha edificato la capacità di svolgere le *Computer Network Operations* oltre alla predisposizione di poligoni virtuali per l'addestramento del personale, alcuni dei quali già operativi. Da un punto di vista teorico le *Computer Network Operations* si articolano in operazioni di difesa attiva (*Computer Network Defence*), di raccolta informativa (*Computer Network Exploitation*) e di attacco (*Computer Network Attack*).

Nello specifico le *Computer Network Defence* (CND), consistono in azioni tese a proteggere le infrastrutture e gli assetti della Difesa da attività cibernetiche ostili. Questa attività si sostanzia nella difesa, analisi e sfruttamento dei dati. Le *Computer Network Exploitation* (CNE), sono azioni tese ad acquisire ed analizzare dati e informazioni contenute su computer e network d'interesse, al fine di ottenere un vantaggio. Le *Computer Network Attack* (CNA) sono azioni volte a rendere inaccessibili, degradare o distruggere informazioni contenute in un computer o in una rete, oppure la rete di computer stessa degli avversari. Questa capacità è stata implementata anche nei teatri operativi in cui sono impegnati i contingenti nazionali, nell'ambito dei Comandi militari delle forze proiettate, attraverso Cellule operative cibernetiche (Coc) che opererebbero anche in sistema con il CIOC in madrepatria, garantendo, da un lato, la protezione degli assetti militari, ormai sempre più digitalizzati e, dall'altro, la condotta delle possibili operazioni cibernetiche nell'area delle operazioni militari, secondo la missione istituzionale, le direttive operative e le regole d'ingaggio stabilite.

A compimento del processo di riorganizzazione e razionalizzazione del settore *cyber*, infine, lo Stato Maggiore della Difesa, per rendere più efficace ed efficiente il settore C4/ICT-*Cyber*, ha fondato nel 2020 il Comando per le Operazioni in Rete (COR), inserendolo alle dipendenze del Comando Operativo di Vertice Interforze (COVI) dal 2021. Questo rappresenta un'evoluzione estremamente significativa all'approccio della Difesa al cyberspazio, integrando sinergicamente sotto un unico Comando le competenze e capacità *cyber* di cui sono dotate le diverse Forze Armate. Il COR è infatti responsabile della condotta delle operazioni nel dominio cibernetico, nonché della gestione tecnico-operativa in sicurezza di tutti i Sistemi di *Information & Communications Tecnology*/C4 della Difesa, avendo l'obiettivo di armonizzare e distribuire tempestivamente le informazioni prodotte dai sistemi di comando e controllo, *computing*, *Intelligence Surveillance & Reconnaissance*.

Tale trasformazione si è concretizzata anche sul piano dottrinale attraverso il recepimento di quanto previsto in ambito NATO. Infatti, con l'AJP (*Allied Joint Pubblication*) 3.20 l'Alleanza evolve il precedente concetto di CND, CNA e CNE in quello *di Cyberspace Operations* (CO) che a sua volta è suddiviso in *Defensive Cyberspace Operations* (DCO) e *Offensive Cyberspace Operations* (OCO) in base agli effetti che il tipo di operazione consente di ottenere.

Per quanto riguarda, invece, la realizzazione di appositi ambienti virtuali finalizzati allo sviluppo di capacità *cyber* è in via di completamento, presso la scuola telecomunicazioni delle Forze Armate (STELTMIT) di Chiavari, il *Cyber Range* "UNAVOX", piattaforma di addestramento degli operatori cibernetici militari che potrebbe essere resa disponibile quale laboratorio tecnico anche alle Università di settore.

Le innovazioni organizzative della Difesa in ambito *cyber* sono state supportate da una cornice giuridica che stabilisse ruoli e competenze, ma anche limiti di impiego. A livello parlamentare è stata sempre ribadita la necessaria riconducibilità di queste operazioni nell'alveo di precise regole d'ingaggio che dovranno essere necessariamente definite in relazione allo sviluppo di questa nuova tipologia di operazioni militari, nel doveroso rispetto dell'ordinamento giuridico nazionale con particolare riferimento all'art. 11 della Costituzione in forza del quale il nostro Paese ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali.

Capitolo II: PRESIDIARE L'INSTABILITÀ

1. Il *Policing Gap* nei Teatri d'Operazione

Il concetto di *Stability Policing* (SP) include un ampio spettro di attività, collocate nel più grande alveo del concetto strategico di proiezione della stabilità[19]. Tale funzione trova riscontro nei più complessi teatri operativi, inquadrandosi all'interno del processo di stabilizzazione e ricostruzione, principalmente durante o dopo un conflitto, ma anche prima di esso, in chiave preventiva. Tali attività sono volte alla sostituzione temporanea delle forze di polizia locali (poiché non più esistenti o di efficienza fortemente ridotta) o al loro rinforzo o ricostruzione organizzativa e capacitiva, al fine di contribuire al ristabilimento del c.d. *Rule of Law*[20], all'interno di una cornice di sicurezza a tutela della popolazione civile, verso la quale la funzione è peculiarmente orientata. Nel 1997, nell'ambito della missione *Stabilization Force* (SFOR) in Bosnia-Herzegovina, l'Alleanza atlantica si è confrontata, per la prima volta, con l'esigenza di conformare la propria dottrina e le proprie capacità militari con le emergenti problematiche di ordine e sicurezza pubblica, difficilmente affrontabili attraverso gli strumenti ordinari. In tale scenario, il Comando *Supreme Headquarters Allied Powers Europe* (SHAPE) ha così evidenziato la presenza di una zona grigia denominata «*public security gap*»: se da un lato le forze dell'Alleanza e la *United Nations International Police Task Force* (UN IPTF) risultavano prive di mandato esecutivo, dall'altro le forze di polizia locali palesavano incapacità o scarsa volontà nel garantire il rispetto della legge. Tale divario è stato rilevato anche dalle Nazioni Unite nel 2000, le quali, nel sottolineare con il *Rapporto Brahimi*[21] la mancanza di capacità di polizia qualificate e prontamente dispiegabili, nonché l'esigenza di un cambio radicale di approccio al *crisis management*, hanno promosso la necessità di schierare rapidamente assetti con elevate capacità di polizia. Al contempo, il documento ha sottolineato l'opportunità di evolvere, da un ruolo di supervisione (*single police officer monitoring missions*), a un ruolo proattivo in riferimento alla riorganizzazione e all'addestramento delle forze di polizia locali. In estrema sintesi, appariva evidente, agli occhi degli osservatori internazionali, che il complesso scenario di una crisi, con il collasso delle istituzioni locali e gli evidenti, conseguenti effetti sulla popolazione civile, rendevano necessario affrontare, da un lato, il tema dell'adeguatezza

[19] MC 0655 Military Concept for Projecting Stability, 24 April 2018 § 16;

[20] AJP-3.22 *NATO Allied Joint Doctrine for Stability Policing*, para 0119, *The rule of law is based on three pillars (law enforcement, judicial, and correctional)*;

[21] Nel 1999 il Segretario Generale dell'ONU Kofi Annan istituì un *Panel* per approfondire i mandati ONU nelle operazioni di *peacekeeping* e *peacebuilding*, proponendo correttivi volti a impedire il ripetersi di quanto accaduto in Rwanda (1994) e a Srebrenica (1995) - *United Nations, Report of the Panel on United Nations Peace Operations, A/55/305 S/2000/809, Lakhdar Brahimi Chairman*;

degli strumenti a disposizione della compagine militare e, dall'altro, della stabilizzazione di lungo periodo dell'area di operazioni, per garantire, l'*end-state* desiderato, un ambiente sicuro quale pre-requisito per una rapida ed ordinata riassunzione delle responsabilità da parte della *Host Nation*. In ambito NATO, il *public security gap*, sotto il profilo specifico del *policing gap*, ha trovato una risposta operativa nel dispiegamento della *Multinational Specialized Unit* (MSU), composta da *Gendarmerie Type Forces* (GTF), integrate con forze di polizia e fanteria militari adeguatamente addestrate ed equipaggiate, a guida e *framework* dell'Arma dei Carabinieri, dotate di peculiari e specifiche capacità di polizia, impiegate con compiti di tutela dell'ordine e della sicurezza pubblica e controllo del territorio. Il modello MSU è stato successivamente replicato e integrato da forze specializzate dell'Alleanza[22], anche in Albania, Kosovo e Iraq, dimostrandosi un modello di riferimento per le attività di stabilizzazione in situazioni post-conflitto all'interno di Stati privi di un solido apparato di sicurezza pubblica. In ragione dell'efficacia di tale modello, i compiti delle MSU sono stati progressivamente ampliati, estendendosi all'addestramento delle forze di polizia locale e al supporto delle conseguenti attività di carattere anche operativo, espandendo la propria area di intervento anche a settori a elevata specializzazione, come le investigazioni scientifiche e la tutela del patrimonio culturale. Le esperienze maturate con le MSU hanno consentito di implementare, all'interno dell'Alleanza atlantica, la dimensione di polizia delle operazioni militari, conducendo all'odierno concetto di Polizia di Stabilità.

2. Lo Stability Policing (SP)

Nel Concetto Strategico della NATO[23] del 2010 compare un primo riferimento alla necessità per l'Alleanza di sviluppare capacità in materia di addestramento e sviluppo delle forze locali in aree di crisi (ivi comprese le forze di polizia), al fine di consentire alle autorità del luogo, il più velocemente possibile, di assicurare la sicurezza senza dover ricorrere all'assistenza internazionale[24]. Il documento, nel confermare l'impegno, per la NATO, a prevenire le crisi, gestire i conflitti e stabilizzare situazioni post-conflitto, individua, quali *core tasks* dell'Alleanza, funzionali alla sicurezza della popolazione e del territorio, la *collective defence*, il *crisis management* e la *cooperative security*. Con particolare riguardo al secondo *core task*, il *Concept* sancisce la necessità di un'appropriata combinazione di strumenti politici e militari atti a garantire la stabilizzazione e la ricostruzione, con il necessario

[22] Principalmente Polizia Militare e Forze Armate convenzionali.

[23] *Active Engagement, Modern Defence: Strategic concept for the defence and security of the members of the NATO, adopted by heads of state and government at the NATO summit in Lisbon, 19-20 Nov 2010;*

[24] «*…develop the capability to train and develop local forces in crisis zones, so that local authorities are able, as quickly as possible, to maintain security without international assistance*…»;

coinvolgimento di partner civili. Tale concetto viene ulteriormente rafforzato con la Dichiarazione del *Summit* di Lisbona del 2010, allorquando viene ribadito che l'Alleanza, al fine di garantire un *comprehensive approach*, deve essere in grado di pianificare, impiegare e coordinare capacità di *crisis management* di natura civile e militare messe a disposizione dalle nazioni nell'ambito delle missioni alleate. In tale quadro, la Dichiarazione del Vertice di Varsavia del 2016 costituisce una pietra miliare, affermando che la dimensione dello *Stability Policing*, menzionata per la prima volta, costituisce un elemento chiave per proteggere le popolazioni civili dagli effetti dei conflitti armati, secondo un approccio a 360° in cui l'Alleanza è proiettata all'esterno dei propri confini per assicurare stabilità e sicurezza[25]. A dispetto di tale importante statuizione a livello politico-strategico e nonostante nel 2016 abbia visto la luce la pubblicazione AJP-3.22 *Allied Joint Doctrine for Stability Policing*[26], negli anni successivi non si avverte una particolare attenzione della Comunità Internazionale verso la Polizia di Stabilità, che viene chiamata solo sporadicamente, se non del tutto tralasciata, verosimilmente nell'errato convincimento che lo strumento militare si debba focalizzare sull'obiettivo immediato (la sconfitta del nemico nell'area di operazioni), piuttosto che sull'obiettivo strategico (la stabilizzazione di lungo periodo di un quadrante).

La pubblicazione definisce lo SP come «l'insieme di attività connesse al settore di polizia, tese a rinforzare o temporaneamente sostituire le forze di polizia locali, al fine di contribuire al ripristino e/o al mantenimento dell'ordine e della sicurezza pubblica, dello Stato di diritto e della protezione dei diritti umani»[27]. Lo SP non è una capacità civile, ma una capacità militare di polizia che copre per intero lo spettro del conflitto[28], espandendo il proprio arco di interazione alla popolazione civile, nonché alle istituzioni governative e giudiziarie. Si tratta quindi di un insieme operativo di attività – diverse da quelle *combat* – volte sia alla sostituzione delle forze di polizia locali (laddove inesistenti o incapaci di svolgere il proprio mandato) sia al loro rafforzamento[29], nonché orientate a contribuire al mantenimento dell'ordine e della sicurezza pubblica, nonché di un *Safe and Secure*

---

[25] *2016 NATO Warsaw Summit Declaration, para 132 «…the imperative to protect civilians from the effects of armed conflicts…putting in place all the efforts to avoid, minimize, and mitigate the negative effects on civilians including a stability policing dimension*»;

[26] La pubblicazione, di cui la Difesa italiana, per il tramite dell'Arma dei Carabinieri, è C*ustodian*, è in corso di revisione, nell'ambito del processo di trasformazione governato dall'Alleanza che prevede la necessità di attualizzare ed implementare le proprie pubblicazioni di riferimento alla luce delle esigenze operative o dottrinali, adeguandosi al mutato contesto internazionale di riferimento.

[27] «*Police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights*» (AJP-3.22 *Allied Joint Doctrine for Stability Policing*, ed. 2016);

[28] «*The spectrum of conflict reflects the prevalence, scale, and intensity of violence ranging from stable peace to high intensity conflict. Overlaying the spectrum of conflict are four predominant campaign themes: Peacetime Military Engagement, Peace Support Operations, Security Operations, and Combat Operations. The spectrum of conflict can vary among, and within the campaign themes and can evolve over time*» (*AJP-3, Allied Joint Doctrine for the Conduct of Operations*, ed. 2019).

[29] Mediante attività di *monitoring, mentoring, advising, reforming, training e partnering.*

Environment (SASE). Sostituzione e rafforzamento sono missioni tra loro non alternative che spesso si sovrappongono temporalmente, nello sviluppo di un quadro coerente d'intervento che si propone di realizzare, in concreto, il *comprehensive approach to crisis management*. Lo SP non si confronta con un nemico convenzionale, ma si avvale di procedure, equipaggiamenti e forze appositamente strutturati per l'esigenza, al fine di contribuire al raggiungimento degli obiettivi della missione e dell'*end-state* pianificato. Ciò corrisponde al trasferimento della piena autorità alle forze di polizia, a un governo pienamente legittimo e ad autorità autosufficienti, ovvero a una missione di polizia internazionale. Lo *Stability Policing* è quindi un fattore essenziale di sicurezza e di sostegno alla *governance* nelle regioni instabili in un quadro di intervento sistematico e armonico con l'addestramento delle forze militari convenzionali e degli attori del *Rule of Law*. Ma l'obiettivo della funzione non si esaurisce nello svolgimento di attività di livello tattico od operativo, potendo svilupparsi anche attraverso attività di *advising* di livello strategico, volta a supportare le Istituzioni (*MoD/MoI/MoJ*) della *Host Nation* nel processo di sviluppo di autonome capacità. Tale obiettivo, certamente premiante nel medio-lungo termine, messo a sistema con la conduzione di operazioni tattiche, costituisce l'espressione concreta dell'approccio olistico che l'Alleanza si pone nella pianificazione di operazioni. Il *campaign design* ed il *campaign management* rappresentano i due fattori di successo di una operazione, laddove la conoscenza degli strumenti a disposizione del Comandante e l'integrazione/interazione degli stessi, consente il conseguimento di quegli obiettivi strategici che vanno ben oltre il singolo risultato tattico/operativo, ma mirano alla definizione di un *end state* armonico e strutturato, che ha, evidentemente, un ampio orizzonte geostrategico.

Lo sviluppo di una dottrina dello *Stability Policing* in ambito NATO muove di pari passo con la sempre maggiore consapevolezza di dover fronteggiare minacce di tipo ibrido[30], in contesti ambientali contraddistinti da totale o parziale assenza di istituzioni affidabili, forze armate e di polizia incapaci di operare, strutture giudiziarie e detentive inefficienti, nonché popolazione locale sbandata e priva di riferimenti, permeabile a influenze di natura criminale o terroristica. In tale quadro, caratterizzato da assenza di ordine e sicurezza pubblica, è emersa la necessità di espandere le capacità militari dell'Alleanza, acquisendo, oltre a esse, anche alcune delle capacità di polizia.

Dal 2014, la NATO è impegnata in un cammino di riposizionamento strategico verso funzioni di *Deterrence and Defence*, nel quadro della rinnovata assertività fra grandi potenze (USA, Federazione Russa e Repubblica Popolare Cinese), con uno spostamento del

[30] Bosnia, Kosovo, Libano, Iraq, Afghanistan tra tutti.

baricentro dell'Alleanza verso il fianco Est (proiezione inevitabilmente accentuata dopo l'invasione della Crimea). Con differenti nomi, visioni e ampiezza d'intervento, lo *Stability Policing* è stato condotto, nel tempo, dalle Nazioni Unite, dall'Unione africana, dall'Alleanza atlantica e dall'Unione europea, e ha maturato una solida esperienza nel campo dello *Stability Policing*, cui essa si riferisce genericamente con il termine di missioni CSDP di polizia, rientrando nell'ambito della *Common Security and Defence Policy*. Proprio il confronto con la NATO – che ha adottato ufficialmente il termine *Stability Policing*, dotandolo di una definizione – fa emergere alcuni aspetti distintivi della funzione SP di concreta importanza per la risoluzione delle crisi. Lo *Stability Policing* della NATO abbraccia tutto lo spettro del conflitto ed è un'area delle operazioni militari. Gli assetti di SP sono parte integrante della forza militare schierata e i compiti da essi assolti contribuiscono al raggiungimento degli obiettivi militari dell'Operazione. La fase operativa, a cui l'Alleanza lo incardina dottrinalmente, è quella della stabilizzazione e ricostruzione (*stabilization & reconstruction*), con specifico riferimento al processo di riforma del settore della sicurezza (*security sector reform*) che inizia già durante la fase del conflitto. L'UE, diversamente, inquadra le missioni CSDP di polizia nel contesto del contributo civile al c.d. *comprehensive approach* alla gestione delle crisi. Le missioni sono gestite operativamente dalla *Civilian Planning and Conduct Capability* (CPCC), risalendo all'autorità dell'Alto Rappresentante dell'Unione per gli Affari esteri e la politica di sicurezza, nonché e al controllo politico e alla direzione strategica del *Political and Security Committee* (PSC). L'intervento di polizia costituisce strumento privilegiato di prevenzione avanzata delle minacce, in grado di iniettare elementi di *governance* utili a ricomporre le fratture interne e rafforzare la coesione sociale, ottenendo – con dispendio di energie inferiore a quello richiesto da contingenti più strutturati – risultati efficaci sul piano operativo e informativo. Lo spettro delle missioni di polizia della UE include sia le missioni di sostituzione (c.d. *substitution*) che di ricostruzione delle capacità delle forze di polizia (c.d. *strengthening*), previste anche dalla NATO. Lo SP è, quindi, lo strumento d'elezione che l'Alleanza condivide con le altre maggiori Organizzazioni Internazionali, UE, ONU e UA, sebbene con nomi e visioni differenti, per colmare il *policing gap*. La NATO è caratterizzata da una visione militare di tale strumento mentre l'ONU e l'UA condividono l'idea che lo schieramento di polizia appartiene alla componente civile della missione schierata. La UE, infine, si pone in una posizione intermedia, ma orientata verso le posizioni ONU.

L'UE, infatti, possiede una solida esperienza nella polizia di Stabilità ma ha una visione diversa da quella dell'Alleanza e un concetto d'impiego più articolato. Le missioni di polizia (cosi l'UE chiama lo SP) sono inquadrate tra le capacità civili di gestione della crisi della

Common Security and Defence Policy (CSDP) e sono gestite operativamente dalla *Civilian Planning and Conduct Capability* (CPCC), risalendo all'autorità dell'Alto Rappresentante dell'Unione per gli Affari esteri e la politica di sicurezza, nonché al controllo politico e alla direzione strategica del *Political Policing and Security Commitee* (PSC).

Diversamente dalla NATO, per la quale lo SP è una componente delle operazioni militari (e potrebbe sostanziare, in linea teorica, anche una operazione stand-alone) e del contributo militare al cd. *Comprehensive approach* alle crisi, nell'ambito della UE, la polizia di stabilità è parte del contributo civile allo stesso. La visione dell'impiego e della finalità dello strumento di polizia è quindi differente.

La denominazione, le capacità e la catena di comando e controllo degli assetti di polizia schierati dall'Unione Europea, tuttavia, sono diversificati in relazione al livello di instabilità. In particolare, le *Integrated Police Units* (IPU) rappresentano la componente di polizia "robusta", idealmente riconducibile alle Gendarmerie, da schierare nella fase iniziale delle operazioni e in ambiente a più elevato livello di instabilità per la conduzione di una molteplicità di compiti, incluse le attività addestrative, di *mentoring* e *monitoring* a favore delle forze di polizia della *Host Nation*, anche sotto temporaneo comando e controllo militare. Per contro, le *Formed Police Units* (FPU), mutuate dall'ONU e principalmente riconducibili alle forze di polizia civile degli Stati Membri, costituiscono la componente di polizia più leggera, con compiti, di massima, limitati al mantenimento dell'ordine pubblico e al controllo del territorio, da impiegare sotto comando e controllo civile, nelle aree in cui già esiste una cornice di sicurezza. La UE, con costante coerenza, ha sempre considerato la Polizia di Stabilità un'area funzionale non militare e non ha mai costituito una capacità militare di polizia dedicata, assegnabile al comandante della Forza schierata per il perseguimento degli obiettivi militari della missione. Le stesse IPU, quando schierate sotto comando e controllo militare, perseguono obiettivi che non sono ritenuti militari. La differente impostazione europea, tuttavia, ha lo svantaggio di sottrarre al Comandante della Forza militare UE uno strumento essenziale per ampliare il ventaglio delle opzioni a sua disposizione finalizzate alla gestione della minaccia ibrida e alla stabilizzazione dell'area di crisi. Essa, quindi, implica un potenziale indebolimento della componente militare della missione, rendendo la componente di polizia della missione UE schierabile solo in contesti di intensità conflittuale minore rispetto a quello in cui la NATO schiera la componente di *Stability Policing*. L'impostazione europea, inoltre, non valorizza l'opportunità offerta dall'appartenenza delle GTF (di cui diversi Stati Membri sono dotati) ai rispettivi strumenti militari nazionali.

3. SP e Multi-Domain Operations

L'evoluzione degli scenari operativi, caratterizzati da contesti fragili e variabili, nonché segnati da minacce ibride dai centri di gravità mobili e mutevoli trova un ulteriore strumento di presidio nel concetto di *Multi-Domain Operations*. Sviluppato inizialmente per codificare un approccio alle operazioni militari integrante i domini tradizionali di Terra, Mare ed Aria con quelli nuovi di *Cyber* e Spazio, nonché con il crescente ruolo dell'ambiente elettromagnetico e della dimensione informativo-cognitiva, esso aveva la finalità di fronteggiare efficacemente strategie d'azione lungo il *continuum of competition* da parte di potenziali *peer-competitors*. La proliferazione e democratizzazione delle tecnologie, insieme alla frammentazione delle risorse di potere ha, però, poi contribuito ad estenderne la valenza anche nei confronti di *near-peer-competitors* e di attori non statuali. L'approccio multi-dominio si ispira sostanzialmente all'esigenza di generare effetti (letali e non) allo scopo non di avere la supremazia in un singolo dominio, bensì di mantenere la libertà d'azione producendo effetti in tutte le dimensioni del confronto, favorendo una maggiore comprensione degli obiettivi e delle condotte dei potenziali avversari (*enhanced strategic anticipation and situational awareness*) e limitandone l'azione. Il concetto di operazioni multi-dominio travalica, inoltre, il solo ambito prettamente militare, ampliandosi ad includere tutti gli strumenti del potere (Diplomatico, Informativo, Militare ed Economico – DIME) nell'ambito del *continuum of competition* per influenzare gli avversari, contrastarne le azioni e tutelare i propri interessi, coniugando sinergicamente il ricorso al *Military Instrument of Power* (MIoP) e agli altri *Instruments of Power* (IoP). Gli effetti di tali azioni sono poi orientati ad incidere selettivamente o diffusamente sulle tre dimensioni: fisica, virtuale e cognitiva al fine di raggiungere l'obiettivo dell missione.

Nell'ambito delle *Multi-Domain Operations*, lo *Stability Policing*, proprio per il suo carattere intrinsecamente ibrido di attività di polizia preventiva e repressiva in contesti securitari degenerati, condotto da forze dell'ordine ad ordinamento militare (*Gendarmerie Type Forces*), può fornire un contributo centrale, costituendo una capacità pregiata in grado di produrre efficaci effetti non letali trasversalmente a tutte tre le dimensioni e lungo almeno quattro dei cinque domini operativi (escludendo ragionevolmente quello spaziale), e crescentemente soprattutto nel nuovo dominio cibernetico. Al contempo, l'attività di SP può beneficiare, interfacciandosi ed integrandosi con le altre componenti di un'eventuale *Joint Force* in teatro per moltiplicare e rafforzare i risultati del processo di stabilizzazione, svolgendo un ruolo di coordinamento nell'impiego sinergico delle risorse e degli assetti disponibili al fine di contrastare minacce sotto-soglia ed intervenire sulle cause fondamentali di insicurezza caratterizzanti contesti fragili.

Lo SP tradizionalmente è considerato parte della componente terrestre e si sostanzia in una funzione militare di polizia ordinaria e di addestramento professionale delle forze di sicurezza interne dello Stato ospitante (questo, indipendentemente dalla natura militare o civile di queste ultime). Quella dello SP si può immaginare come una costante fase operativa, dottrinalmente incardinata nel processo di stabilizzazione e ricostruzione, con specifico riferimento al procedimento di riforma del settore della sicurezza, che inizia già durante la fase del conflitto. L'idea alla base ruota intorno ai due principi di inclusività e di gradualità: tutto lo strumento militare, pertanto, può contribuire allo SP secondo le proprie specifiche abilità e capacità. È sotto tale prisma ottico che occorre leggere la possibilità di inglobare, oltre al terrestre, anche altri domini (su tutti marittimo e aereo) che possono rivestire un ruolo di valido e qualificato supporto per le attività militari finalizzate alla riduzione del *policing gap*.

Il dominio aereo può, ad esempio, risultare cruciale per la condotta di attività di sorveglianza del territorio, consentendo di coprire vaste aree, contribuendo soprattutto alla vigilanza sulle zone rurali o di confine, sia con il ricorso ad assetti ad ala rotante, sia con l'impiego di UAS (*Unmanned Aerial System*). Queste capacità possono essere non solo progressivamente integrate nei dispositivi di SP, ma possono anche divenire oggetto di formazione specialistica per le forze locali, contestualmente al loro processo di ricostituzione ed approntamento. In uno scenario segnato da minacce ibride, inoltre, lo sviluppo e l'acquisizione di capacità *counter*-UAS può dimostrarsi di significativa importanza alla luce della sempre maggiore facilità di accesso a prodotti commerciali adattabili alla condotta di azioni malevole di natura terroristica o criminale, dal trasporto di piccoli ordigni esplosivi, ad attività di contro-sorveglianza, fino all'impiego dei droni come corrieri per il contrabbando di materiale di provenienza o natura illecita. L'occasionale presenza di una componente aeronautica appartenente ad una *Joint Force*, può poi attivamente contribuire allo sviluppo di tali capacità, potendo svolgere, inoltre, funzioni di intercettazione e disturbo di comunicazioni VHF o GSM impiegate da attori malevoli, attraverso i propri sistemi EW (*Electronic Warfare*), assistendo fattivamente le aliquote di SP nelle attività di controllo del territorio.

Nel dominio marittimo, invece, dove le fasce costiere sono notoriamente permeabili ad attività illecite, lo SP può fornire gli elementi informativi abilitanti all'efficace attuazione di attività di polizia d'alto mare da parte di una componente marittima, svolgendo, inoltre, una valida azione di filtraggio attraverso la sorveglianza delle zone portuali e/o di approdo. Gli stessi dispositivi di SP possono contribuire al controllo diretto delle zone immediatamente antistanti il litorale al fine di individuare e reprimere comportamenti criminosi, dal traffico di

esseri umani, al contrabbando di sostanze stupefacenti, le quali possono avere riflessi diretti sul processo di stabilizzazione. Queste capacità possono poi essere oggetto di trasmissione e formazione alle forze dell'ordine locali, anche agendo di concerto con la componente navale. Questa, a sua volta, può svolgere un ruolo di sostegno all'attività di SP tramite il persistente presidio delle aree più prossime a quelle portuali, con il ricorso a mezzi sotto e sopra la superficie, nonché ad Unità equipaggiate con sistemi di EW. La specificità infatti degli assetti navali, consistente nella possibilità di permanere in un dato settore assicurando continuità di azione per un tempo praticamente indefinito, rafforza infatti da un lato il controllo di una determinata area e dall'altro garantisce una più difficile penetrazione dalle aree costiere di agenti destabilizzanti esogeni.

Relativamente al *cyber*spazio infine, le minacce da esso provenienti si configurano precipuamente come una fonte multilivello di cyber-instabilità dove gli strumenti di risposta più idonei possono anche provenire dallo SP. In *primis*, la natura pervasiva e non solo tecnologica del dominio *cyber* postula di per sé un coinvolgimento dell'intera *Joint Force* al suo presidio nel rispetto delle specificità proprie di ogni componente, con lo SP particolarmente idoneo a vigilare, prevenire e reprimere le minacce a bassa intensità e sotto-soglia. Essendo, inoltre, il *cyber* una componente tipica delle operazioni ibride proprio per l'assenza di confini fisici e sfruttando l'assenza di distinzioni tra contesto puramente militare ed ambiente civile, lo SP rappresenta uno strumento particolarmente attagliato al suo contrasto, offrendo ai Comandanti soluzioni alternative ed adattabili per espandere le opzioni di intervento. I compiti di stabilire e mantenere sia un *Safe And Secure Environment* (SASE), sia la *Freedom Of Movement* (FOM) sono, in aggiunta, progressivamente estesi anche al dominio cibernetico, in quanto la comprensione dell'ambiente operativo e della minaccia, proprie delle considerazioni di pianificazione di una missione di SP, non possono prescindere da esso. Infine, adeguate ed efficaci attività di pubblica sicurezza a supporto della *Host Nation* non possono mancare di fornire un contributo, sia in termini di addestramento delle forze dell'ordine locali, sia di azione diretta degli assetti schierati, nella conduzione di azioni di contrasto tradizionale o di operazioni cibernetiche, volte soprattutto ad impedire lo sviluppo di santuari *cyber* all'interno di Stati fragili, che potrebbero minacciare la sicurezza e stabilità di altri Paesi.

Capitolo III: LA LAW ENFORCEMENT INTELLIGENCE (LEINT)

Nuovi scenari, nuove minacce e nuove attività di presidio dell'instabilità postulano la necessità di nuovi strumenti integrati. Se infatti i contesti in cui si dispiegano molte delle operazioni contemporanee si caratterizzano per una policromia di minacce fluide, frequentemente sotto soglia, molte capacità tradizionali faticano a fornire autonomamente risposte adeguate. Proprio alle crescenti e mutate esigenze preventive ed informative funzionali ad un'adeguata consapevolezza situazionale dell'ambiente operativo, nonché alle necessità di supporto o sostituzione alle azioni di polizia repressiva delle forze locali, la *Law Enforcement Intelligence* (LEINT) può fornire un valido ausilio. Il presente Capitolo mira dunque a definire e delineare le specificità proprie di questa peculiare forma di raccolta, analisi e disseminazione informativa, sottolineandone le differenze rispetto all'attività investigativa, prima di approfondire le sue potenzialità nel dominio cibernetico entrando nel dettaglio degli strumenti di *Web Intelligence* e *Social Media Intelligence*, nonché delle potenzialità offerte in quest'ambito dalla convergenza di *Big Data* ed Intelligenza Artificiale.

1. Definizione, Strumenti e Finalità

Il concetto di LEINT afferisce al più vasto settore dell'intelligence ampiamente intesa e può, pertanto, venire preliminarmente definito come il prodotto finale di un processo analitico di: valutazione delle informazioni raccolte da una molteplicità di fonti, integrazione di queste in un formato logico e produzione di conclusioni, stime o previsioni concernenti un fenomeno criminale, attraverso l'impiego di un approccio scientifico alla risoluzione dei problemi. Ne consegue che essa è un prodotto sinergico inteso a fornire conoscenze significative, affidabili e pragmatiche alle forze dell'ordine in riferimento ad attività e caratteristiche di delinquenza comune, organizzazioni criminali, associazioni estremiste e gruppi terroristici.

Le funzioni della LEINT possono generalmente venire circoscritte da un lato alla prevenzione e dall'altro alla pianificazione ed allocazione delle risorse. In riferimento al primo, esso implica l'acquisizione e l'accrescimento di un quadro informativo concernente minacce terroristiche o criminali, al fine di impiegare questo per individuare, perseguire ed eventualmente arrestare i possibili perpetratori, proteggere obiettivi sensibili e dispiegare strategie atte ad eliminare o mitigare impatti e vulnerabilità. In particolare, nell'ambito della LEINT, sono individuabili tre diverse linee d'azione aventi un primario orientamento alla prevenzione. Una prima riguarda l'analisi informativa in supporto ad una contemporanea indagine penale, una seconda fa riferimento all'intelligence relativa a minacce imminenti, disseminata tra le aliquote delle forze di polizia al fine di sviluppare ed implementare piani

ed azioni preventive di mitigazione e/o risposta, mentre una terza linea d'azione concerne le minacce di lungo periodo quali sospette organizzazioni a delinquere o complesse reti criminali transnazionali. La seconda funzione assolta dalla LEINT, consiste nel fornire informazioni ai decisori nel contesto di riferimento, in relazione all'emergere e mutare delle minacce, nonché alle loro caratteristiche e metodologie, allo scopo di pianificare strategie ed allocazioni di risorse (materiali, umane, tecnologiche…) aderenti ad un'efficace prevenzione nel medio-lungo termine. Nell'ambito della LEINT, questo è anche definito come Intelligence Strategica e consente una valutazione dell'evoluzione degli spettri di minaccia a beneficio dei responsabili delle forze dell'ordine, con la finalità di sviluppare piani ed assegnare anticipatamente risorse idonee a rispondere alle minacce emergenti.

Le attività di LEINT non vanno, in particolare, confuse con quelle investigative. Infatti, benché queste ultime siano strettamente correlate alla raccolta di informazioni e al processo di intelligence in sé, la funzione di intelligence è propriamente più esplorativa e diffusamente orientata di quanto non possa esserlo una specifica indagine penale. A titolo di esempio, una forza di polizia potrebbe avere un ragionevole sospetto che un soggetto o un gruppo di persone abbia l'intenzione, la capacità e la determinazione di commettere un atto criminale o terroristico, ma potrebbe mancare di un quadro probatorio sufficiente per provvedere all'attuazione di una misura cautelare. In un simile scenario si osserva come non sussista un'identità tra attività di intelligence volte a prevenire la minaccia e standard investigativi diretti a procedere penalmente contro degli individui. In un'altra prospettiva, un'indagine con molti sospettati ed un'ampia gamma di elementi probatori, magari contradditori, potrebbe beneficiare di un processo analitico di intelligence volto ad indirizzare la composizione coerente del quadro accusatorio.

Similarmente all'interazione intercorrente tra attività investigativa e *Law Enforcement Intelligence*, sussiste anche un rapporto tra quest'ultima ed il più ampio ambito dell'intelligence derivante dalla dottrina anglosassone. Questa infatti generalmente riguarda l'analisi di informazioni grezze per produrre una conoscenza sinergica relativa ad una minaccia ed è usualmente differenziata in due classi interrelate: la disciplina di intelligence, concernente concetti, regole, procedure e norme della funzione di intelligence, e le applicazioni di intelligence. In relazione alla prima classe, la LEINT condivide contemporaneamente similitudini e profonde differenze con altre due discipline di intelligence: l'intelligence per la sicurezza interna o *Homeland Security Intelligence* (HSI) e l'intelligence per la sicurezza esterna o *National Security Intelligence* (NSI). La HSI è anche definita intelligence multi-minaccia/multi-rischio (*all-threat all-hazard*), occupandosi della raccolta ed analisi di informazioni relative a minacce non criminali verso infrastrutture

critiche, salute e sicurezza pubblica, al fine di prevenirne il verificarsi o mitigare gli effetti di eventi malevoli. Benché la HSI non si occupi di attività criminali, essa è tuttavia naturalmente sottoposta ad una parziale sincronia bidirezionale con la LEINT in conseguenza del ricorso della prima a risorse operative ed informative fornite dalle stesse forze dell'ordine (si pensi alla pandemia da Covid-19). La NSI riguarda invece la raccolta ed analisi di informazioni concernenti la relazione e l'omeostasi di uno Stato con le altre Nazioni, Organizzazioni Internazionali governative e non, nonché singoli individui, in riferimento a fattori politici ed economici, oltre che di mantenimento e tutela della propria sovranità e dei propri interessi nazionali. Essa include sia l'intelligence politica su azioni o attività minacciose attuate da soggetti ostili al Paese in oggetto, sia l'intelligence militare sulle capacità belliche, tecniche ed organizzative, di entità avverse. Rispetto alla NSI, concentrata primariamente su minacce provenienti dall'estero, la LEINT ha un focus locale e presenta profonde divergenze nelle tecniche operative e nei limiti normativi a cui le due sono sottoposte. Infatti, se la raccolta di informazioni a fini di sicurezza nazionale opera in un ambito giuridico frequentemente permissivo, le attività di *Law Enforcement Intelligence* sono condotte nel contesto di una società civile, essendo legate da vincoli di privacy e tutela dei diritti civili sostanzialmente analoghi a quelli delle altre attività di polizia. Al contempo, le discipline di NSI e LEINT possono, tuttavia, presentare un punto di intersezione nella prevenzione e disarticolazione di reti terroristiche, sia con riferimento al possibile concretarsi di minacce provenienti da gruppi internazionali nel contesto locale, sia in relazione alle linee di finanziamento illecito del terrorismo, non di rado mediante attività criminali. Questo pone notevoli sfide in termini di accessibilità, trasmissione, compatibilità legale ed azionabilità delle risorse informative provenienti dalle entità praticanti le rispettive discipline di intelligence.

Sotto il profilo della seconda classe di intelligence, ossia l'applicazione dell'intelligence, la LEINT si rivolge allo sviluppo di conoscenze specifiche sulle differenti tipologie di crimine. Questa concerne, ad esempio, la produzione di informazioni su nuovi metodi ed indicatori afferenti all'uso di armi da fuoco in azioni criminali o le caratteristiche di attività di riciclaggio di denaro sporco. Essenzialmente dunque essa mira a fornire una comprensione della natura e degli elementi costitutivi di un fenomeno criminale di interesse. Esemplificativo può essere il caso di comunità minacciate da attività di gang operanti come organizzazioni criminali, dove la conoscenza di culture, segni, simboli, gerarchie ed altre caratteristiche specifiche delle singole gang può essere centrale, per analisti e funzionari delle forze di polizia, allo scopo di attuare un'adeguata azione repressiva.

Non diversamente dalle altre attività di intelligence, anche la LEINT implica il ricorso ad un ciclo di intelligence rivolto a garantire un metodo sistematico, scientifico e logico per

processare le informazioni in modo completo. Questo assicura infatti la produzione e la disseminazione di intelligence fruibile ed accurata ai soggetti incaricati di fornire risposte operative volte a prevenire il realizzarsi di minacce criminali. Nello specifico, questo si concretizza nelle sei fasi di: Pianificazione e Direzione, Raccolta, Elaborazione e Collazione, Analisi, Disseminazione, Rivalutazione. Se la maggior parte dei passaggi non diverge significativamente da un comune ciclo di intelligence, la fase di raccolta presenta specificità proprie dell'attività di polizia poggiando, soprattutto, su notifiche di attività sospetta (SARs-*Suspicious Activity Reports*) osservate o riportate da funzionari degli organi di polizia, elementi probatori ed indizi provenienti da indagini penali, accesso a database delle forze dell'ordine ed infine analisi *open source,* tra cui i *social media* (a cui saranno dedicati vastamente i paragrafi successivi).

Nel complesso, ed alla luce di tutti gli elementi caratterizzanti summenzionati, la *Law Enforcement Intelligence* può essere dunque più circostanziatamente definita come il prodotto di un processo analitico atto a fornire una prospettiva integrata di informazioni disparate afferenti i crimini, trend criminali e minacce alla sicurezza, nonché a condizioni associate con la delinquenza[31]. Dalla LEINT deriva, inoltre, il concetto di *Intelligence-Led Policing* (ILP), consistente nella raccolta ed analisi di informazioni relative al crimine ed alle condizioni che vi contribuiscono, risultante in prodotti di intelligence fruibile intesi a supportare le forze dell'ordine nello sviluppare risposte tattiche a minacce e/o pianificazioni strategiche riguardanti i rischi securitari emergenti o mutevoli[32]. L'ILP integra sostanzialmente la funzione LEINT nelle attività di polizia preventiva e repressiva attraverso un'essenziale parte di raccolta informativa grezza incentrata ad individuare e comprendere fenomeni criminosi all'interno di una determinata giurisdizione. Questa prima parte dell'attività si basa su un'aderenza tra le informazioni raccolte e parametri prestabiliti dalle forze di polizia in una fase di pianificazione e direzione. In particolare, i requisiti di intelligence sono dedotti sulla base di rapporti provenienti da funzionari di polizia, fonti confidenziali e membri della comunità locale sottoforma di denunce anonime, indizi e segnalazioni di attività sospette. La successiva analisi sottopone ad un esame sistematico gli elementi raccolti, impiegando metodi quantitativi e qualitativi, deduttivi ed induttivi al fine di identificare fatti significativi e inferirne conclusioni funzionali alla caratterizzazione e previsione delle minacce. Se dunque le informazioni grezze forniscono avvio al processo e generano consapevolezza, l'intelligence derivante dall'analisi produce conoscenza, riduce

[31] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Michigan State University, Institute for Intergovernmental Research, 2022, p.7.
[32] Ibid., p. 103.

le incertezze e consente decisioni accurate. Il processo analitico infatti, sinergicamente provvede a sviluppare e derivare conoscenze dai fatti contribuendo ad individuare ulteriori requisiti e deficit informativi. Concentrandosi l'ILP sulle minacce, esso si fonda su una fondamentale identificazione delle variabili interne alla comunità di riferimento, nonché dell'area geografica circostante in funzione di origini, sviluppi ed interazioni criminose (si pensi all'influsso di confini internazionali su attività di traffico illecito o all'effetto della presenza di più organizzazioni criminali o violente operanti in uno stesso settore). Il contemporaneo focus sulle condizioni ingeneranti le minacce alla sicurezza postulano, inoltre, un'attenzione particolare a fattori che possono contribuire ad un esacerbarsi degli episodi delinquenziali o alla presenza di soggetti strumentali allo sfruttamento di particolari situazioni politiche, sociali o economiche per condurre attività di natura criminale o terroristica. Il perno di congiunzione tra gli elementi menzionati ed il risultato delle attività di ILP è costituito dalla concreta fruibilità del prodotto di intelligence, il cui fine ultimo dovrebbe essere il supporto alle forze dell'ordine nell'assumere decisioni, fornendo utili direzioni per lo sviluppo e l'attuazione di prevenzione, contrasto e repressione del crimine. Ad esempio, il risultato analitico potrebbe descrivere alternativamente minacce imminenti per una comunità o una specifica area, soggetti ricercati costituenti potenziali rischi securitari o metodologie criminali di cui le forze dell'ordine necessitano di venire a conoscenza. Essenzialmente, il prodotto di intelligence deve essere disseminato ai soggetti istituzionali competenti sotto il profilo operativo, garantendo un'utilizzabilità pratica delle informazioni. Gli effetti dell'attività di ILP sono infine rivolti sia a risposte tattiche, sia strategiche. Le prime, spazianti dall'aumento dei controlli di sicurezza in aree di transito, alla presa di coscienza di attività sospette presso un potenziale obiettivo, sono incentrate sulla prevenzione, impiegando le informazioni relative a fenomeni terroristici o criminali per eliminare o ridurre le minacce a breve termine e immediate. Le seconde coinvolgono invece il cambiamento delle minacce all'interno di una comunità nel tempo, fornendo informazioni sulla natura, le caratteristiche e le metodologie mutevoli delle condotte antisociali, allo scopo di sviluppare strategie di lungo termine implicanti la riallocazione di risorse operative per prevenire la maturazione di una minaccia o per mitigarne gli effetti qualora questa dovesse emergere. Attraverso l'ILP, la funzione di *Law Enforcement Intelligence* abilita l'adozione di decisioni concrete e funzionali a conseguire misurabili effetti sul campo, creando un'efficace integrazione tra sviluppo della consapevolezza situazionale ed effetti sulla condotta degli attori malevoli e criminali.

Un'ultima specificità riguardante la LEINT concerne il quadro giuridico-normativo di riferimento in cui esse si svolgono. Come precedentemente anticipato, infatti, le forze

dell'ordine non possono conservare informazioni su individui per attività di intelligence a meno che non vi sia un presupposto criminale. Ne consegue che le forze di polizia devono disporre di elementi affidabili e basati sui fatti che consentano di inferire che il soggetto sottoposto a raccolta ed analisi di intelligence ha commesso, sta commettendo o sta per commettere un crimine. In particolare, tutte le attività di raccolta informativa su un individuo a fini di intelligence devono essere condotte coerentemente con le norme di procedura penale. Ne deriva che gli elementi raccolti non possono essere conservati a tempo indeterminato, se non in presenza di indizi probatori che consentano di dedurre la sussistenza di un presupposto criminale. Le forze dell'ordine hanno infatti la responsabilità di proteggere la privacy delle informazioni che raccolgono nel corso delle operazioni di intelligence. Questo include la limitazione della loro diffusione solamente a funzionari che hanno il diritto o la necessità di conoscerle al fine di promuovere un'indagine penale, consistentemente con i precetti del segreto investigativo, provvedendo al contrario, in assenza di accertate condotte criminali, alla loro distruzione. A questo fine le funzioni di LEINT devono essere presidiate da fattori di controllo orientati a stabilire standard, aspettative e limiti decisionali sulle singole attività, implicando un'adeguata formazione degli operatori e funzionari coinvolti ai fini di trasmettere le conoscenze, abilità e capacità necessarie, nonché specificando metodi esecutivi, incluso cosa deve essere fatto, come dovrebbe essere fatto e cosa non dovrebbe essere fatto.

Nonostante, come osservato, la LEINT presenti diversi spazi applicativi tradizionali, lo sviluppo di moderne tecnologie ha ampliato, proprio per le maggiori possibilità di aderenza ai summenzionati limiti normativi e di accessibilità, le opportunità di implementazione. A questo fine i paragrafi successivi approfondiscono la natura e le caratteristiche delle attività di intelligence nel dominio cibernetico.

2. LEINT e Dominio Cibernetico

La LEINT ha utilizzato nel corso dei decenni varie forme di tecnologia per raccogliere informazioni, ricorrendo a strumenti spazianti dai registri a penna alle intercettazioni, dalla videosorveglianza alle immagini ad infrarossi, dai dispositivi di ascolto avanzati a quelli di localizzazione GPS (*Global Positioning Satellite*). Negli anni, le forze dell'ordine hanno iniziato ad adottare computer *mainframe* alla fine degli anni '60 e *personal* computer (PC) già dai primi anni '70, mentre oggi questi possono contare anche su tablet e smartphone per archiviare, analizzare e condividere informazioni.

Contestualmente al nuovo vigore dato all'intelligence dopo l'11 Settembre 2001, l'ambiente e la tecnologia digitale hanno svolto un ruolo sempre più importante. Nello

specifico, l'ambiente *cyber* ha visto probabilmente lo sviluppo più consistente, con un sempre maggiore impiego di fonti aperte online per gli scopi più disparati: dal conoscere le ideologie estremiste, al carpire informazioni sugli indagati e cercare indizi. Le applicazioni tecnologiche in campo informatico hanno reso maggiormente disponibili e facilmente accessibili le risorse informative, compresi i prodotti della *Global Justice Information Sharing Initiative* e dei suoi vari gruppi di lavoro. La condivisione delle informazioni tra le diverse forze di polizia di un Paese e tra quelle di diversi Paesi è diventata più facile e veloce, e c'è stato un crescente uso di video digitali, non solo da telecamere di sorveglianza, ma da una vasta gamma di fonti, in testa gli smartphone. La tecnologia offre agli analisti l'accesso alle informazioni grezze in modo rapido, semplice e sicuro. Con l'evoluzione dell'informatica, nonché con la recente introduzione dell'intelligenza artificiale, gli strumenti analitici stanno diventando, inoltre, più robusti e con capacità via via crescenti.

Nel complesso, quindi, l'uso degli strumenti nati dagli sviluppi in campo *cyber* nella LEINT come nel campo delle indagini penali, di per sé, non ha guidato lo sviluppo di nuove dottrine di prevenzione del crimine o di svolgimento delle indagini penali, né ha modificato la logica di fornitura di servizi di intelligence o di pubblica sicurezza. Tuttavia, lo sviluppo tecnologico in generale, e in ambiente *cyber* in particolare, ha favorito l'implementazione di risorse abilitanti e/o ausiliarie per rendere operative queste dottrine in modo più efficiente ed efficace.

Praticamente tutto ciò che fa un analista di intelligence è reso più veloce, più facile e più completo utilizzando la tecnologia. A titolo di esempio si pensi all'*Integrated Criminal Apprehension Program* degli anni '70, grazie al quale fu sviluppato *CompStat* (un database computerizzato). Questo ha fornito un'analisi dettagliata della criminalità su base statistica, fornendo una risposta tempestiva utile a valutare e/o sviluppare reazioni operative per anticipare, identificare ed interrompere le tendenze della criminalità organizzata. L'evoluzione degli strumenti informatici ha, quindi, permesso di condurre analisi del crimine più dettagliate, più precise e più rapide. Grazie ad un meccanismo di *feedback*, e quindi capitalizzando l'esperienza maturata, è stato possibile, inoltre, perfezionare e implementare il *CompStat* per migliorarne l'accuratezza e l'aderenza informativa.

Attualmente, le società stanno vivendo una vera e propria rivoluzione tecnologica: velocità di rete più elevate, archiviazione di un consistente volume di informazioni a basso costo e in condivisione su *cloud*, velocità di elaborazione dati elevatissime, mezzi di comunicazione alternativi come i *social media* e l'integrazione di immagini digitali audio e video che possono essere facilmente condivise tra i dispositivi e manipolate in modo quasi non rilevabile (come nel caso dei *deep fake*). A questo si sommano le comunicazioni

crittografate, come quelle di applicazioni di messaggistica che consentono, inoltre, la scomparsa dei messaggi, le comunicazioni nascose facendo ricorso alla steganografia[33], le possibilità di tracciamento dei telefoni cellulari con dati geografici e temporali, nonché l'accesso biometrico agli smartphone, che di per sé memorizzano un tesoro di dati, sono all'ordine del giorno. Una quantità significativa di tali informazioni è correlata alle piattaforme di *social media* e all'*e-commerce*. Anche veicoli a motore, elettrodomestici e articoli per la casa, come frigoriferi, apriporta per garage, televisori e forni possono essere connessi per comunicare e archiviare informazioni come parte dell'*Internet of Things* (IoT). Ad esempio, sussiste una crescente applicazione nella medicina legale dei dati digitali scambiati dai veicoli: si cercano in rete prove utili per le indagini penali o nell'esame delle dinamiche di un incidente stradale, che possono includere i dati GPS di bordo di un veicolo, i dati della console multimediale di bordo, la connettività Wi-Fi e i dati della scatola nera del veicolo. Il campo include anche l'esame di app per smartphone che sono direttamente interattivi con i sistemi del veicolo o scaricati nella console multimediale. Queste fonti possono fornire una grande quantità di informazioni sul movimento del veicolo e persino identificare il conducente, data la connettività dello smartphone, che potrebbe essere un'informazione preziosa per indagini e intelligence.

La connettività tra diverse tecnologie è diventata un importante punto focale, l'Intelligenza Artificiale (IA), l'apprendimento automatico e gli algoritmi predittivi stanno infatti cambiando il volto dell'analisi dei dati. Sempre più spesso, tutte queste tecnologie vengono fuse in flussi di informazioni condivisibili sui *social media* e utilizzate in tutto, dal marketing, all'*e-commerce*, alla fornitura di servizi.

Anche l'economia ha assunto nuove dimensioni attraverso l'uso delle criptovalute. Queste e altre tecnologie stanno cambiando il carattere sociale, economico e politico delle società globali. Forniscono grandi promesse per l'evoluzione umana, ma possono anche servire come via per nuove forme di criminalità, molte delle quali di natura transnazionale.

La linfa vitale del processo di intelligence sono le informazioni grezze, e le nuove tecnologie forniscono una varietà di metodi per raccoglierle in modo accurato, completo e aggiornato. Droni in grado di registrare persone e oggetti in cortili recintati o tetti, anche di notte, utilizzando i sensori a infrarossi, dati delle torri cellulari in grado di identificare la presenza di un telefono in una determinata data, ora e posizione, telecamere di

[33] La steganografia è una tecnica che si prefigge di nascondere la comunicazione tra due interlocutori. A differenza della crittografia, consente di nascondere un messaggio all'interno di un vettore che possa consentirne il trasporto senza destare sospetti, ad esempio mediante l'occultamento di informazioni all'interno di file di computer. Nella steganografia digitale, le comunicazioni elettroniche possono includere la codifica steganografica all'interno di un livello di trasporto, come un file di documento, un file di immagine, un programma o un protocollo.

videosorveglianza in grado di documentare la data, l'ora e la posizione di una persona e potenzialmente identificarla attraverso il riconoscimento facciale: queste sono tutte illustrazioni della raccolta di informazioni basate sulle tecnologie attualmente disponibili.

L'uso di queste risorse può tuttavia ingenerare problemi legati al rispetto delle libertà civili (come la privacy) e di questioni etiche. Le norme sui diritti civili stabiliscono infatti i confini in cui è legalmente consentito raccogliere informazioni tramite una tecnologia, mentre l'etica affronta se è "giusto" o "appropriato" utilizzare una determinata tecnologia in un certo modo. Nessuno dei due fornisce risposte chiare. Le prove raccolte nel dominio *cyber* sono sempre più utilizzate nelle indagini penali, in particolare e-mail, documenti, messaggi e cronologia di ricerca su Internet. La questione legale più frequente derivante dall'uso di prove digitali è costituita dalla correttezza della procedura di perquisizione e sequestro. Le questioni etiche sono ancora più difficili da affrontare, in quanto riflettono gli standard morali e sociali di ciò che è "giusto", concetto soggettivo, che varia tra le comunità. La liceità infatti non è di per sé garanzia di aderenza ai canoni etici di riferimento. Lo standard etico è quello di utilizzare il potere non solo in modo lecito ma anche responsabile.

Fino a quando non ci sarà una solida base di sentenze, che esemplifichino le possibili casistiche, la LEINT nel dominio cibernetico continuerà crescentemente a svolgere un compito fondamentale per l'indirizzo e l'impostazione delle indagini penali tradizionali. Essendo, infatti, questa disciplina volta a prevenire ed evitare i fatti criminosi, la sua peculiarità di poter lavorare "sotto traccia", fornisce alle forze dell'ordine il vantaggio informativo necessario a costruire l'impianto accusatorio raccogliendo solo le informazioni necessarie in modo che queste possano utilmente venire usate in sede processuale.

3. Web Intelligence

Negli anni '90, Internet e la nascita del World Wide Web (WWW) diedero un impulso eccezionale alla rivoluzione digitale in corso dal '900. È inizialmente utile accennare alle differenze tra queste due infrastrutture. L'attuale Internet è l'evoluzione di un progetto della *Defence Advanced Research Projects Agency* (DARPA) del Dipartimento della Difesa statunitense ed era, inizialmente, una rete di macchine interconnesse in ambito universitario e di ricerca scientifica. Questo network si è allargato sino a diventare l'attuale rete globale che conosciamo. Il WWW, o semplicemente il web, è una parte della rete internet e consiste nell'insieme di siti pubblicamente raggiungibili, incluse le macchine utili al suo accesso. Queste stesse macchine condividono documenti rappresentati dalle pagine web che possono contenere semplice testo, immagini, video e sono accessibili attraverso software di *web browsing*. La rete è oggi il *mass media* più accessibile al mondo e veicola ogni tipo

di formato di comunicazione in esistenza con una quantità di dati creati giornalmente pari a 2,5 quintilioni di byte[34]. Tale mole di informazioni è stata spesso sottovalutata dalla comunità dell'intelligence mondiale, soprattutto per la difficoltà di gestione di una tale quantità di informazioni, per la maggior parte non di interesse informativo. Grazie, però, all'avanzare di tecnologie di computazione sempre più rapide, hanno preso piede software di analisi dei *Big Data* che, servendosi anche dell'intelligenza artificiale hanno reso l'*Open Source Intelligence* (OSINT) un valido strumento nelle mani della comunità dell'intelligence e del *law enforcement*. L'uso del web nella *Web Intelligence* (WEBINT) è un caso particolare di OSINT. Quest'ultima, secondo il *NATO Open Source Intelligence Handbook*, è un prodotto informativo, derivante da fonti pubblicamente disponibili e da altre non classificate che hanno una distribuzione o un accesso pubblico limitato, deliberatamente ricercato, selezionato, analizzato e diffuso ad un'*audience* selezionata, generalmente di livello direttivo e di Comando, al fine di soddisfare uno specifico requisito informativo. Essendo *open source*, l'informazione può essere raccolta al di fuori di un procedimento legale che descriva quale sia l'obiettivo di ricerca sia esso una persona, un comportamento, un gruppo o un evento. Tale informazione può essere reperita, inoltre, attraverso una ricerca effettuata sul web o sul *dark web* ed è accessibile a chiunque. L'OSINT è stata utilizzata dai governi nazionali, dalle difese e dal mondo dell'industria per fini istituzionali e di mantenimento del vantaggio strategico nei confronti dei competitori. Vi è quindi una bivalenza strategica e tattica nell'OSINT, anche quando questa è applicata al LEINT. Generalmente le fonti sono la stampa online, pubblicazioni accademiche, paper di ricerca, i forum di conversazione e i blog, i database pubblici, i documenti ufficiali governativi e d'agenzia, tutti i tipi di file e documenti, i social media (come vedremo in seguito nello specifico), agenzie di vendita di dati a terzi, fermo restando che tutto ciò che è condiviso sulla rete da una macchina o un server può essere raggiunto. Il pronto accesso al web rende l'OSINT una risorsa primaria di facile e rapido accesso che può fornire un efficiente ed efficace sguardo d'insieme sull'inchiesta futura o in itinere. Gli operatori coinvolti nel ciclo intelligence del LEINT seguono il ciclo standard di identificazione dell'esigenza informativa, raccolta di dati e informazioni grezze, trattamento delle informazioni, analisi, produzione e disseminazione. Volendo catalogare le applicazioni OSINT di *law enforcement* possiamo identificare le seguenti macro categorie: supporto agli interventi di polizia giudiziaria, profilazione dei soggetti, investigazioni sul web aperto e *dark web*, investigazioni sotto copertura (*undercover*), antiterrorismo. Il supporto agli interventi è indirizzato a fornire intelligence in

[34] *How to manage complexity and realize the value of big data*, https://www.ibm.com/blogs/services/2020/05/28/how-to-manage-complexity-and-realize-the-value-of-big-data/

tempo reale a fini operativi per stabilire, ad esempio, luogo e caratteristiche di un obiettivo, punti di accesso e rischi (una foto postata su un social potrebbe far presagire la presenza di armi da fuoco) o nelle fasi successive allo scoppio di una crisi o incidenti gravi per interpretare la situazione contingente e sviluppare una risposta. Nella profilazione dei soggetti, la WEBINT permette la raccolta di fotografie, nomi, abitazioni, contatti, luoghi frequentati, precedenti penali e abitudini generali di un individuo. Un'altra importante applicazione è l'approfondimento e la profilazione dei gruppi criminali, anche transnazionali, caratterizzati da una dimensione ideologica, che molto spesso utilizzano il web sia per la diffusione del proprio ideale sia ai fini proselitistici. La raccolta sul web aperto, inoltre, abilita un'investigazione a 360° per lo sviluppo di una *picture* completa di intelligence e l'acquisizione di elementi probatori ad esempio attraverso la raccolta di dichiarazioni pubbliche di soggetti o gruppi criminali che spesso lasciano dietro a se tracce della condotta illegale perpetrata. Trafficanti di droga, estremisti di stampo politico e criminalità organizzata utilizzano sovente il web ed il *dark web* rilasciando affermazioni incriminanti, che ancorché possano non costituire reato, forniscono all'operatore di polizia utili spunti di indagine. La consultazione dei mezzi di informazione facilita l'identificazione di peculiari *modus operandi* e lo studio dei trend di crimine in una determinata area o su una scala più ampia. Ma il web permette l'accesso a una vasta gamma di dati utili alle indagini come informazioni sulle caratteristiche demografiche di una determinata area, tracciamento diretto dei voli commerciali e privati, accesso a immagini satellitari e non, compilazione di *link analysis*. Come accennato, i forum e i mercati online del *dark web* possono venire scandagliati per far emergere attività illegali che includono lo scambio di beni illegali. Il *dark web* viene poi investigato per ricercare crimini e terrorismo cibernetici, generalmente non facilmente perseguibili con metodi di polizia tradizionali. Un ulteriore categoria è costituita dalla modalità investigativa *undercover* di WEBINT applicato al *law enforcement*. Queste attività non convenzionali prevedono l'impiego di un ufficiale di polizia giudiziaria che, utilizzando il web, nasconde la propria identità infiltrandosi all'interno di organizzazioni criminali allo scopo di guadagnare la fiducia dei malviventi e raccogliere elementi utili all'investigazione o incastrare i partecipanti. Infatti, l'art. 14 l. 3 Agosto 1998, n. 269 autorizza, per le fattispecie elencate in norma, l'organo di polizia giudiziaria a svolgere attività in un vero e proprio ruolo di agente provocatore[35] anche, ad esempio, con la creazione di siti "civetta", noti anche con il termine *honeypot*, per cogliere in flagranza il criminale. Ad esempio, potrebbero essere creati profili virtuali che grazie all'AI siano in grado di simulare l'identità di un bambino, con

[35] Cfr. L. Luparia e G. Ziccardi, *Investigazione Penale e Tecnologia Informatica*, Giuffrè, 2007.

le caratteristiche linguistiche e comportamentali dei minori ricompresi tra gli otto e i tredici anni[36]. Gli accessi e le interazioni sui siti "civetta" permettono di identificare e tracciare le attività web di soggetti interessanti sul piano investigativo, sui quali poi orientare indagini più mirate attraverso controlli incrociati su altri siti web (nelle *chat* e nei *newsgroup*, in particolare)[37]. Il LEINT, infine, si avvale del web svolgendo attività di OSINT quale importante risorsa per l'antiterrorismo. Come per il crimine organizzato, le indagini sul web permettono di intercettare le dinamiche di radicalizzazione, reclutamento, addestramento, finanziamento e incitamento al terrorismo. Non solo, possono essere altresì poste in essere misure difensive di *counter-intelligence* in funzione aggressiva o dissuasiva al fine di proteggere le infrastrutture critiche come i nodi delle telecomunicazioni, della finanza, dell'energia. In più, soggetti di interesse a rischio spionaggio o sovversione possono essere identificati, monitorati e localizzati. Gli analisti di intelligence, avvalendosi dei già menzionati strumenti di AI possono individuare siti terroristici e *network* per abilitare la condotta di operazioni di arresto e confisca. Concludendo, al netto di un controllo qualità successivo, l'accesso a informazioni potenzialmente vitali per le indagini è considerevolmente facilitato. Tra i compiti dello *Stability Policing* supportati, troviamo quelli esplicitati nella AJP-3.22 e possiamo annoverare *border control*, *criminal investigation*, *surveillance*, *counter-smuggling*, *counter human trafficking*, *war crime investigations* e *assistance to international courts*. Queste funzioni ricadono in quello che la dottrina definisce *Advanced Police Skills* da sviluppare nello *Specialised Training*.

4. Social Media Intelligence

La attività di *Law Enforcement Intelligence* nel dominio cibernetico, come anticipato, possono assumere numerose forme differenti, ma una delle più facilmente accessibili è l'*Open Source Intelligence* (OSINT), consistente nella ricerca, raccolta ed analisi di dati e di notizie rinvenibili su fonti aperte al fine di produrre intelligence fruibile. Benché non esistano categorizzazioni condivise della disciplina, questa è a sua volta distinta in base alla tipologia di risorse verso cui è rivolta la raccolta informativa iniziale ed in particolare risulta possibile effettuare una bipartizione tra il settore della *Social Media Intelligence* (SOCMINT) e quello più generale della *Web Intelligence*. Il presente paragrafo ed il successivo indagano appunto nel dettaglio queste due forme.

---

[36] Cfr. M. Delle Donne, *Tecniche d'Indagine della Polizia Postale nell'ambito dei reati informatici e nella pornografia online*, in Diritto e Diritti, 2017.

[37] Cfr. F. Buffa, *Profili penali del commercio elettronico*, Giuffrè, 2006, pag. 104.

La SOCMINT si riferisce a tecniche, strumenti e soluzioni che consentono di raccogliere, in modo più o meno intrusivo, elaborare, estrarre ed analizzare informazioni ai fini di intelligence dalle multiformi interazioni che si verificano su *social network* aperti o chiusi. Il termine venne formalmente coniato in un *paper* del 2012 scritto da Sir David Omand, Jamie Bartlett e Carl Miller ed intitolato *Introducing Social Media Intelligence (SOCMINT)*[38]. Il documento, nell'esprimere l'assoluta rilevanza raggiunta dalle piattaforme online nelle dinamiche sociali, faceva appello ad uno sviluppo di capacità di intelligence in quest'ambito, in particolare ai fini di sicurezza ed ordine pubblico. Significativamente, l'analisi partiva proprio da un episodio di cronaca verificatosi nel Regno Unito, nell'agosto 2011, quando in seguito all'uccisione di un individuo da parte di un funzionario di polizia, diffusi disordini colpirono la città di Londra, venendo fomentati, anticipati e testimoniati sui *social media*. La successiva indagine interna alle forze dell'ordine per l'inefficace risposta rilevò come la polizia non avesse canali e competenze atte a sfruttare le risorse informative provenienti da tali fonti, richiamando l'apparato securitario ad adattarsi rapidamente per evitare il ripetersi di simili episodi[39]. Se la crescita delle piattaforme online non ha conosciuto tregua nel successivo decennio fino ad oggi, la consapevolezza dell'opportunità di un loro sfruttamento, per finalità di prevenzione e repressione dei crimini nonché le capacità e le tattiche per realizzarlo, hanno avuto notevoli progressi.

Precisamente, l'ambito in cui vengono condotte le attività di SOCMINT è circoscritto, come intuibile dal nome stesso, ai *social media*. Questi sono definibili come un insieme di applicazioni software e piattaforme online intese a fornire informazioni, interazione umana, comunicazione e più diffusamente condivisione di contenuti in qualsiasi forma (testuale, grafica, audio e video), includendo forme di *social networking*, *social bookmarking* (ad esempio il *tagging*), *social curation* (condivisione e marketing), nonché forum di discussione virtuale, blog e microblog variamente orientati e specifici. Sotto un profilo di pubblica sicurezza, queste realtà offrono alle forze dell'ordine sia uno strumento di comunicazione diretta con i cittadini, sia una fonte di raccolta informativa. In particolare, i *social media* possono essere un utile strumento per monitorare minacce, tendenze antisociali e modelli criminosi, fornendo indicatori relativi ad intenzioni malevole, possibili obiettivi e potenziali perpetratori di condotte illecite, o addirittura elementi probatori per lo svolgimento e finalizzazione di indagini penali.

---

[38] Sir David Omand, Jamie Bartlett e Carl Miller, *Introducing Social Media Intelligence (SOCMINT)*, Intelligence and National Security, Vol. 27, n.6, pp. 801-823, Dicembre 2012.

[39] Her Majesty's Inspectorate of the Constabulary (HMIC), *The Rules of Engagement: A Review of the August 2011 Disorders*, London.

Parallelamente alle piattaforme online generalmente note al grande pubblico (Facebook, Twitter, Telegram…) ne esistono molte altre di più piccole dimensioni e considerabili di nicchia, spesso monotematiche o ideologicamente orientate. Se i grandi *social network* possono fornire valevoli elementi ai fini investigativi e di intelligence, le piattaforme più contenute e meno note, spesso situate nel *Deep Web*e nel *Dark Web*, rappresentano non di rado dei veri e propri collettori informativi ai fini delle esigenze di ordine pubblico. Frequentemente infatti alcune di queste tendono a concentrarsi su tematiche suprematiste, fondamentaliste, anarchiche o antigovernative, oppure mettono in contatto soggetti con un'alta propensione alla violenza o impegnati in analoghe attività criminali, dalla pedopornografia alle truffe. La maggioranza di esse richiede, inoltre, il ricorso ad un browser Tor, divenendo difficili da trovare ed ancor più da infiltrare, ma quando queste operazioni hanno avuto successo, i risultati informativi hanno generato ricadute di intelligence ed investigative significativamente rilevanti.

Il monitoraggio dei forum di discussione e dei mercati del *darknet*[40]*,* legati a gruppi estremisti e criminali, consente infatti di individuare tendenze e minacce, con effetti particolarmente importanti per la dimensione di LEINT strategica. Esaminare i temi di discussione, identificare possibili conflitti tra gang o metodologie di compravendita su siti del *darknet* può infatti fornire informazioni grezze da analizzare al fine di ridefinire il quadro di sicurezza od orientare la raccolta di elementi di prova durante attività investigative. Ad esempio, la diffusione di droghe sintetiche come il fentanyl ha avuto in molti casi un impatto sui proventi illeciti dei trafficanti di eroina, portando ad un aumento della sua produzione e ad un abbassamento dei prezzi sia nelle strade, sia nel *darknet*. Le attività di SOCMINT in quest'ultimo ambito possono consentire di ottenere dettagli aggiuntivi sui trafficanti, le reti di distribuzione e gli spostamenti geografici dettati dal cambiamento nel mercato degli stupefacenti. Un ulteriore esempio è costituito dal processo di ridenominazione affrontato intorno al 2015 da molti gruppi di estrema destra negli Stati Uniti d'America, dove i termini "supremazia bianca" e "destra bianca" iniziarono ad essere sostituiti da quello di "nazionalismo bianco". Il linguaggio di questi movimenti, nonché la loro apparenza esteriore, progressivamente normalizzatasi, è stata ampiamente anticipata nelle discussioni su blog e forum dei diversi gruppi. La SOCMINT ha consentito di comprendere le tendenze interne a queste realtà estremiste attraverso l'analisi di una moltitudine di *post* su diversi *social media*.

[40] Una *darknet* è una rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano, nel suo significato più generale, essa può essere qualsiasi tipo di gruppo chiuso e privato di persone che comunicano, ma il nome è spesso usato per reti di condivisione di file.

A fianco di finalità strategiche, la *Social Media Intelligence* permette anche di collezionare prove di reati e minacce, in quanto le piattaforme sono diffusamente impiegate da delinquenti ed estremisti. Se infatti non è raro che membri di gruppi criminali postino sui *social media* immagini con armi, stupefacenti o denaro, spesso essi ricorrono a strumenti online per pianificare azioni violente, reclutare membri o sfidare organizzazioni rivali. Similarmente, come numerosi casi di radicalizzazione hanno dimostrato, alcune associazioni terroristiche (si pensi ad Al-Qaida, ISIS…) impiegano i *social network* per fare proselitismo e persuadere altri individui ad agire o unirsi alla causa. Infine, i mercati del *darknet* forniscono luoghi virtuali anonimi dove si ritiene, e numerose operazioni di polizia lo confermano, vengano smerciati beni e servizi di natura o provenienza illecita, dalle armi agli stupefacenti, dai documenti falsi ai *ransomware*.

I vantaggi apportati dalla SOCMINT possono dunque venire raggruppati in tre ambiti principali: sviluppo di una consapevolezza situazionale quasi istantanea, acquisizione di punti di osservazione interni ad organizzazioni malevole ed individuazione di intenti o elementi criminali nel corso di un'indagine sia per la prevenzione, sia per la repressione del reato. In riferimento al primo, la raccolta ed elaborazione di dati aggregati provenienti dai *social media* consente spesso di ottenere indicatori e descrizioni degli eventi che si stanno sviluppando in una determinata area. Ad esempio, diversi studi relativi a Twitter hanno dimostrato come, nonostante la maggioranza dei *tweet* faccia generalmente seguito alla diffusione di notizie sui media convenzionali, una piccola parte di essi tende sistematicamente ad anticipare la pubblicazione di notizie significative. L'analisi del traffico dati può consentire dunque una più rapida individuazione di eventi emergenti, anticipando metodi classici di notifica o segnalazione. Il ricorso a tecniche di geolocalizzazione può, inoltre, permettere di sviluppare mappe evolutive che riportino i picchi di *post* o *tweet* legati ad episodi o contenuti violenti, facilitando risposte più rapide, efficaci ed agili. Relativamente al secondo aspetto, la SCOMINT può incrementare la comprensione di attività e comportamenti di determinati gruppi di interesse o noti alle forze dell'ordine. In presenza di adeguata autorizzazione legale a procedere, la polizia può infatti sfruttare i *social media* per individuare nuovi ed emergenti tematiche sviluppantesi internamente alle conversazioni di fazioni specifiche o apprendere come queste reagiscono al verificarsi di determinati episodi. Il ricorso a simili tecniche può consentire di stimare i livelli di rabbia o aggressività di gruppi criminali o violenti, nonché quali preoccupazioni ed interessi animano le discussioni loro interne. Ancora più precisamente, le informazioni raccolte ed analizzate possono contribuire ad identificare quando sono in corso di pianificazione azioni o dimostrazioni che potrebbero avere risvolti violenti o aumentare i livelli di tensione in una comunità, come incontri di ultras

calcistici che possono causare disordini, o contro-dimostrazioni che incrementano le risorse necessarie a mantenere l'ordine pubblico. Rispetto al terzo ed ultimo ambito, le forze di polizia, su autorizzazione delle autorità competenti, possono effettuare attività di sorveglianza digitale di individui sospettati di essere coinvolti in crimini o associazioni a delinquere, consentendo, attraverso attività incrociata sulle diverse piattaforme, di collegare eventuali complici, svelare identità fittizie, individuare reti criminali e preservare contenuti da impiegarsi come elementi probatori in un procedimento giudiziario.

Sebbene la SOCMINT apporti notevoli vantaggi, essa richiede una serie di attenzioni al fine di preservare la qualità, correttezza e legalità del prodotto di intelligence. In *primis* è necessario assicurarsi dell'accuratezza delle informazioni raccolte evitando il rischio concreto di *fake news* o *fake facts* risalendo con scrupolo alle origini iniziali di ogni singolo *post* analizzato e verificandone in modo indipendente i contenuti. Risulta fondamentale, inoltre, la consapevolezza del rischio che le identità virtuali abbiano natura fittizia, richiedendo approfondimenti volti a determinare con sicurezza la reale fonte di dichiarazioni e condotte digitali. Non diversamente, anche immagini e video possono venire manipolati per apparire originali benché non lo siano, postulando la necessità di esercitare un approccio critico e sempre volto alla verifica. In aggiunta, la perpetuità delle informazioni online determina l'esigenza di ricercare costantemente una precisa collocazione temporale dei *post* e delle dichiarazioni, al fine di evitare travisamenti o inefficienze dell'attività di intelligence.

Infine, in linea con le restrizioni normative afferenti alla LEINT in generale, anche la SOCMINT richiede un'attenzione primaria al rispetto della disciplina sulla privacy e la libertà di espressione. In particolare è opportuno vigilare sull'eventuale presenza di informazioni personali in *post* o dichiarazioni che possano inficiare sulla legittima raccolta del dato, così come sul fatto che il *social media* che è stato individuato abbia accesso aperto e pubblico, altrimenti potrebbe essere necessaria un'autorizzazione. La presenza infatti di forti restrizioni d'accesso contribuisce a rendere applicabile i principi di privacy alle affermazioni riportate sull'eventuale piattaforma in oggetto. L'intera attività di SCOMINT deve dunque occuparsi di documentare minuziosamente le procedure seguite, ai fini di illustrare le precise finalità istituzionali delle attività svolte, i presupposti investigativi o di pubblica sicurezza e l'attuazione delle prescritte norme di conservazione degli elementi di prova digitali, nonché a testimonianza delle precauzioni attuate per prevenire abusi e violazioni dei diritti di privacy. Qualora si presentino situazioni dubbie, la richiesta di mandati o autorizzazioni da parte delle autorità competenti dovrebbe venire opportunamente osservata.

5. Il Ruolo di Big Data ed Intelligenza Artificiale

Le attività di *Social Media Intelligence* e quello più generale della *Web Intelligence* si basano senza dubbio sulle innumerevoli interazioni sui *social network* che quotidianamente si ripetono, oltre agli accessi continui sui siti web e all'uso ininterrotto di smartphone interconnessi. Tutto ciò genera una mole di dati incredibilmente più elevata di qualche decennio fa. Enormi volumi di dati eterogenei per fonte e formato, analizzabili in tempo reale, tutto questo sono i *Big Data.* Essi sono dotati di cinque caratteristiche fondamentali: volume (elevate moli di dati o in forte crescita), velocità (dati generati e acquisiti rapidamente), varietà e variabilità (dati eterogenei per fonte e formato), veridicità (qualità e affidabilità dei dati).

Analizzare la grande mole di dati permette di raccogliere informazioni e generare nuova conoscenza utile per prendere decisioni più consapevoli, dall'efficientamento dei processi produttivi in campo commerciale ad una migliore *situational awarness grazie* all'ottenimento di input utili all'intelligence nel campo della sicurezza nazionale. Una migliore consapevolezza della situazione in atto potrebbe influenzare i *decision-makers* in ambito di sicurezza nazionale soprattutto nel campo delle attività di polizia all'estero (come nella conduzione di operazioni di S*tability Policing)*. L'analisi dei *Big Data* ha infatti un impatto in tutti i processi e questo è reso possibile da tecnologie che permettono di gestire dati destrutturati e di processarne ampi volumi in tempo reale ma anche dalla diffusione di algoritmi e metodologie di analisi innovative, in grado di estrapolare autonomamente le informazioni nascoste nei dati. Le principali progettualità e metodologie *Analytics* sono le seguenti:

- *Descriptive Analytics*: strumenti orientati a descrivere la situazione sia attuale che passata di processi aziendali o di singole aree funzionali;
- *Predictive Analytics*: strumenti avanzati che effettuano l'analisi dei dati per rispondere a domande relative a cosa potrebbe accadere nel futuro;
- *Prescriptive Analytics*: strumenti avanzati capaci di proporre al *decision-maker* soluzioni strategiche sulla base delle analisi svolte;
- *Automated Analytics*: strumenti capaci di implementare autonomamente l'azione proposta in base al risultato delle analisi dati svolte.

Le metodologie di *Predictive, Prescriptive* e *Automated Analytics* si possono descrivere all'interno della categoria dei cosiddetti *Advanced Analytics*. Come suggerisce l'espressione stessa, si tratta di realizzare progettualità avanzate che hanno finalità almeno predittive e che possono avere un impatto molto rilevante su uno o più processi decisionali. Per realizzare un progetto di questo tipo è necessario considerare i diversi strumenti

tecnologici che si hanno a disposizione, gli assetti organizzativi e le competenze da mettere in campo.

Occorre, infatti, creare veri e propri team di professionisti volti alla gestione e alla valorizzazione di questa grande mole di dati. La *Data Science* (DS) è una materia complessa, i cui confini sono difficili da tracciare e pertanto i professionisti della DS devono provenire dai percorsi di formazione più disparati: dall'informatica all'economia, passando per la statistica, la matematica o la fisica. Le cinque professioni fondamentali individuate e a cui la LEINT deve rifarsi per formare un team esperto di *Big Data*, per gestire la cosiddetta DS*,* sono:

- *Data analyst*: è colui che esplora, analizza e interpreta i dati, con l'obiettivo di estrapolare informazioni utili al processo decisionale. In altre parole, l'obiettivo del suo lavoro è ricercare evidenze quantitative all'interno di grandi moli di dati, supportando in tal modo il *decision-maker*;
- *Data scientist*: è la figura professionale che comunemente si associa alla capacità di gestire i *Big Data* e trarne informazioni rilevanti. Si occupa delle fasi di sviluppo, *training* e *testing* di modelli statistici e algoritmi di apprendimento automatico;
- *Data engineer*: gestisce le fasi di raccolta, processamento e integrazione dei dati. Rende i dati disponibili per le analisi nel giusto formato;
- *Data science manager:* gestisce l'intero processo di DS, coordinando un team centralizzato o favorendo la crescita e la formazione di figure di DS distribuite nel campo della sicurezza nazionale;
- *Analytics translator:* "traduttore" tra la DS e il *core-business* della ricerca. Sa tradurre gli *use case* in linguaggio analitico ed è in grado di interpretare i risultati delle analisi.

Oltre ai team di professionisti volti alla gestione e alla valorizzazione di questa grande mole di dati utili alla gestione della DS, un altro elemento abilitante la valorizzazione dei *Big Data* è l'infrastruttura tecnologica. Infatti è necessaria la disponibilità di macchine che elaborino grandi quantità di dati in tempo reale e software con algoritmi innovativi che permettano lo sviluppo di analisi avanzate (abilitate dagli algoritmi di *Machine Learning*), l'*ingestion* e l'analisi dei dati in tempo reale e l'integrazione di tipologie di dati sempre più eterogenee. Entra in gioco l'Intelligenza Artificiale (IA), che con le sue tecnologie riesce a esaminare e rielaborare i dati per fornire analisi concrete e riutilizzabili. Grazie all'IA e alle sue innovative soluzioni, infatti, è possibile individuare dei trend utili, mettere in relazione delle variabili apparentemente sconnesse tra loro e trasformare la maggioranza dei *Big Data* in dati parlanti, da cui trarre conclusioni vantaggiose. Il vantaggio principale dell'IA è la possibilità di raccogliere informazioni con cui profilare gli utenti comprendendo, per esempio,

quali sono le loro abitudini, quali le preferenze personali o quali le attività svolte con più frequenza.

È importante, però, sottolineare che l'Intelligenza Artificiale non si limita ad accumulare dati e riconoscere tendenze, ma sa anche come apprendere da essi. Sa infatti come adattarsi ai cambiamenti e alle oscillazioni delle tendenze identificando i valori anomali nei dati capisce quali parti del *feedback* dei clienti sono da considerare significative, adattandosi di conseguenza. L'apprendimento automatico e l'apprendimento approfondito sono quindi caratteristiche chiave dell'IA e sono fondamentali per generare nuove regole per l'analisi dei dati. Grazie all'uso degli algoritmi, inoltre, si possono fare analisi predittive, ottimizzare automaticamente i sistemi informativi e creare nuovi contenuti sulla base di ciò che si è appreso. I *Big Data* e l'IA possono essere usati insieme in quasi ogni tipo di settore, ottenendo ottimi risultati in particolare in ambito LEINT ad esempio nel migliorare i processi decisionali, supportando le autorità nazionali a generare risposte più rapide ed efficaci.

Le *Big Data Analytics* hanno un ruolo significante nelle *predictive capability* per anticipare specifici incidenti in ambito sicurezza nazionale, in particolare possono favorire le seguenti piattaforme come valore aggiunto:

- Algoritmi: è possibile progettare algoritmi in grado di allertare le autorità sulla menzione, nelle varie fonti di informazione, di concetti come terrorismo, bombe o rivolte. È, inoltre, possibile rilevare video/contenuti relativi ad organizzazioni atte ad azioni sovversive o studiare qualsiasi escursione insolita nelle attività sociali in una specifica fonte di informazioni. Ad esempio, un'ondata di discussioni su Twitter relative a un argomento specifico o siti web che promuovono attività illecite possono essere identificati in tempo per agire;
- *Social Media Monitoring*: i principali argomenti discussi nei *social media* possono essere monitorati e studiati in modo specifico per geografia, persona e organizzazione. L'analisi delle fonti di informazione, ad esempio, e la loro affinità con uno specifico gruppo di utenti in una determinata area per intraprendere azioni proattive, se necessario;
- *Information Mining*: le informazioni nelle notizie/documenti relativi a una persona specifica possono essere cercate per scoprire le sue idee relative a un dato concetto. Si possono trovare documenti correlati che forniscono rappresentazioni diverse delle stesse informazioni, ad esempio, i diversi modi in cui gli esplosivi sono menzionati negli articoli. Nuove informazioni su un argomento specifico, ad esempio nuovi articoli, pubblicazioni, libri bianchi, brevetti relativi alla difesa missilistica, costituiscono input

che saranno di grande aiuto nella pianificazione della strategia di intelligence ad un livello superiore;

- *Social Network Monitoring*: si può intraprendere uno studio sulla correlazione tra persone basato sui social network. È possibile, inoltre, studiare diversi profili *social* di una persona su Twitter, Facebook e LinkedIn analizzandone i siti Web collegati alla stessa, in base al suo profilo *social*, al contenuto creato o alla cerchia di amici;
- *Document Analytics*: concetti discussi in una raccolta di documenti possono essere studiati. Ad esempio, gli argomenti su cui si concentra il Ministero degli Esteri del Pakistan, sulla base dell'analisi degli articoli/documenti sul suo sito web. I documenti possono essere raggruppati in segmenti separati: documenti che discutono di politica, sport, giochi o affari esteri al fine di trovare tendenze relative ad argomenti specifici;
- *Cyber Security*: l'analisi dei *Big data* può essere, infine, applicata per individuare minacce avanzate persistenti o attacchi progettati per rubare informazioni governative come è accaduto in passato. La maggior parte degli *hacker* ha un *modus operandi* che una volta identificato può essere utilizzato per prevedere la forma di futuri attacchi e mettere in atto adeguate misure difensive. È, inoltre, possibile profilare i gruppi di *hacker*, anche al fine di effettuare l'attribuzione degli attacchi, con risvolti non trascurabili in termini di capacità di *law enforcement*. L'applicazione può poi essere utilizzata per aspetti offensivi della sicurezza informatica. Nelle operazioni di controspionaggio/antiterrorismo i *Big Data* raccolti da droni, satelliti e intercettazioni tecniche possono essere analizzati automaticamente in base al quadro generale fornito dai dati ISR così da consentire di eseguire operazioni di risposta in tempo reale.

Tutto questo proliferare di dati, metodologie, competenze e tecnologie pone davanti, ancora una volta, il problema della privacy. L'analisi e la gestione dei *Big Data* comportano infatti enormi criticità dal punto di vista del trattamento dei dati personali e della tutela della privacy. È dunque necessario un adattamento alle linee guida di trasparenza e liceità raccomandate a livello internazionale in materia di normativa di *Big Data Analytics*.

Capitolo IV: UNA PROPOSTA CONCRETA: *SP LEINT TEAM*

Le peculiarità che contraddistinguono la LEINT rendono questa una nuova ed importante risorsa, non solo per le attività di sicurezza interna, ma sempre di più anche nei contesti di operazioni militari all'estero, indipendentemente dalla loro natura e configurazione. Se, infatti, contesti fragili segnati da minacce ibride sono l'elemento caratterizzante la contemporanea instabilità internazionale, uno strumento flessibile e tipicamente orientato all'individuazione di attività malevole sotto-soglia come la LEINT può costituire un assetto estremamente utile all'arricchimento e raffinamento del quadro informativo. È infatti opportuno ricordare come, al di là delle intersezioni possibili con la comune attività investigativa, la LEINT si distingua chiaramente da questa, orientandosi a sviluppare prodotti di intelligence volti ad incrementare la conoscenza dell'ambiente operativo e delle minacce ivi presenti, abilitando il processo decisionale di Comandanti e *decision makers*. Benché la sensibilità verso i vantaggi da essa apportati si siano progressivamente consolidati negli ambiti nazionali, ed in particolare nel supporto alle attività di prevenzione e repressione delle attività criminali, la LEINT non ha ancora trovato una collocazione determinata nel quadro di operazioni all'estero. In ambito NATO, nello specifico, nonostante stia progressivamente emergendo una riflessione sull'argomento, la *Law Enforcement Intelligence* sostanzialmente non esiste, mancando riferimenti dottrinali in materia ed una definizione della stessa nel contesto dell'Alleanza.

Il presente capitolo tenta appunto di colmare questo *gap*, offrendo una proposta concreta in merito ed elaborando capacità, criticità ed impieghi della LEINT a vantaggio di dispositivi militari schierati in missione. Nello specifico, partendo dalla constatazione dell'assenza di riferimenti in dottrina, il primo paragrafo offre un'inedita definizione di *Law Enforcement Intelligence* attagliata al quadro NATO, approfondendo il concetto con particolare riferimento alle attività di *Stability Policing*. Le sezioni successive affrontano poi i principali *costraints* che complicano l'integrazione della LEINT con le esistenti strutture di intelligence, prima di delineare un prospetto dettagliato dell'implementazione di questo strumento sia a livello di staff G2/J2, sia all'interno di un assetto di SP, dettagliando poi le applicazioni della LEINT nel contesto di operazioni multi-dominio e presentando una sua applicazione teorica a partire dal *case study* dell'Afghanistan.

1. LEINT come Nuovo Strumento nelle Operazioni di Stability Policing

Secondo quanto indicato dalla dottrina dell'Alleanza Atlantica, le attività di *Stability Policing* (SP) *«are conducted with the aim of establishing a safe and secure environment*

(SASE), restoring public order and security, and establishing the conditions for meeting longer term needs with respect to governance and development (in particular through Security Sector Reform)»[41]. Più prosaicamente, la *Stability Policing* è una capacità militare di polizia ordinaria che contribuisce, nei Teatri Operativi, a ristabilire l'ordine e la sicurezza pubblica contrastando terrorismo, guerriglia e criminalità, mediante la sostituzione delle forze di polizia locali ovvero il loro addestramento per migliorarne l'efficienza. Dal punto di vista strettamente dottrinale, le attività di SP collegano gli obiettivi strettamente militari con quelli più politici di stabilizzazione finalizzati a ristabilire le condizioni necessarie al funzionamento delle Istituzioni locali.

Sulla scorta delle esperienze fatte in operazioni e delle prospettive aperte dal progresso tecnologico, la NATO sta analizzando e valutando l'opportunità di includere la LEINT nel proprio corpo dottrinale, con una particolare attenzione al suo inserimento nell'ambito dello *Stability Policing*. Infatti, è stato proposto e approvato di inserire alcuni riferimenti a questo strumento all'interno dell'AJP 3.4.*1 Allied Joint Doctrine for the Military Contribution to Peace Support.* Secondo l'approccio indicato nel testo, le forze di sicurezza presenti in teatro dovrebbero impiegare la *Law Enforcement Intelligence* e diffondere con gli altri attori le informazioni derivanti dall'uso di questa (ad esempio informazioni derivanti da investigazioni criminali) per contribuire a una maggiore *comprehensive approach* della situazione nell'area di operazioni. Si può quindi definire la *Law Enforcement Intelligence* come una capacità rientrante nella funzione intelligence che in teatro funge da raccordo fra la cellula J2 e le Forze di Gendarmeria dedicate alle operazioni di *Stability Policing*, con il fine di contribuire alla *comprehesive approach* attraverso la condivisione con gli altri attori interessati delle informazioni derivanti dal suo uso.

Il NATO *Stability Policing Centre of Excellence* (NSPCoE) di Vicenza, ha in merito svolto nel mese di Marzo 2023 un *workshop* finalizzato a coinvolgere i principali *stakeholder*, esperti in materia e funzionari appartenenti sia alla NATO *Intelligence Enterprise*, sia alla *Stability Policing Community* al fine di individuare punti di convergenza da cui avviare la riflessione sull'utilità di promuovere il concetto di LEINT all'interno dell'Alleanza. Nello specifico, alla luce delle sfide delineate dal NATO *Strategic Concept 2022* ed a sostegno dell'approccio a 360° dell'Alleanza stessa, il NSPCoE ha identificato l'esistenza di un *gap* di intelligence e dunque la necessità di esplorare le modalità di massimizzazione degli effetti della LEINT a beneficio sia dello *Stability Policing* e della *Law Enforcement Community*, sia dell'*Intelligence Community*.

[41] AJP 3.22, *Allied Joint Doctrine for the Stability Policing Edition A Version*, 1° Luglio 2016.

2. LEINT e Multi-Domain Operations

La *Law Enforcement Intelligence* può rappresentare uno strumento aggiuntivo ed intrinsecamente trasversale e flessibile per il sostegno alla condotta di operazioni multi-dominio. Il contributo da essa apportato abilita, infatti, sia una maggiore incidenza delle capacità di *Stability Policing*, a vantaggio di un'eventuale *Joint Force*, sia rafforza la consapevolezza situazionale dell'intero dispositivo, integrando la definizione del quadro informativo e favorendo sinergie tra le diverse componenti. Configurandosi come un assetto di intelligence schierato sul campo all'interno delle aliquote di SP ed interfacciantesi con specifiche posizioni addette a livello di staff J2, la LEINT può contribuire a delineare un prodotto informativo maggiormente dettagliato, preciso e completo. In particolare, essa ha la capacità di intercettare tempestivamente ed analizzare l'emergere di minacce sotto-soglia, individuando al contempo quei fattori socio-economico-culturali che favoriscono il persistere e proliferare di insicurezza ed instabilità nel teatro d'operazione.

Fenomeni illegali locali, traffici illeciti di varia natura e connivenze tra entità criminali ed attori malevoli di più alto profilo possono infatti sfuggire o non risultare superficialmente rilevanti ad altri elementi della Forza, ma se meticolosamente e sistematicamente sorvegliati possono fornire informazioni utili per incrementare e coordinare l'efficacia dell'azione in tutti i domini operativi. Le rilevanze di *intelligence* prodotte grazie all'attività LEINT, possono non solo guidare una più incisiva e consapevole attività di prevenzione e contrasto in sostegno o in sostituzione alle forze di polizia locali, ma permettono, inoltre, di influenzare positivamente l'azione delle altre componenti militari del contingente, discriminando meglio carattere e natura delle fonti di minaccia e coordinando eventuali azioni volte a produrre risultati decisivi sull'intero teatro. La LEINT, in virtù della sua provenienza dal settore della sicurezza interna e del perseguimento di attività criminali, offre infatti una sensibilità a specifiche fonti informative ed un punto d'osservazione sostanzialmente inedito ai dispositivi militari tradizionali, garantendo un ampliamento dello spettro di analisi ed una maggiore probabilità di cogliere indici di mutamento del contesto operativo, magari sintomatici o prodromici al manifestarsi di minacce ibride. La possibilità di operare sia nell'ambito fisico, raccogliendo informazioni dall'attività di controllo del territorio e di cooperazione con le forze dell'ordine locali, sia in quello virtuale, implementando un'analisi pervasiva delle risorse digitali attraverso attività di WEBINT e SOCMINT, nonché la capacità di generare effetti incisivi nella dimensione cognitiva prevenendo e mitigando condotte anti-sociali, rendono la LEINT uno strumento particolarmente attagliato al multi-dominio.

Al fine di comprendere le sinergie possibili grazie al menzionato strumento, si immagini una *Joint Force* schierata in un'area di crisi rivierasca soggetta ad un persistente fenomeno

di insorgenza anti-governativa di difficile eradicazione e ricorrente a tattiche di guerriglia. In assenza di una componente LEINT e del relativo *expertise* dispiegato negli assetti di SP, gli strumenti di *intelligence* convenzionali potrebbero avere la tendenza a concentrarsi primariamente sulla dimensione politico-militare della crisi, ingenerando conseguenti attriti e correlazioni instabili tra le strategie di contrasto ed i risultati delle stesse. Il ricorso alla LEINT consentirebbe invece di conseguire una visione più dal basso dei fattori di insicurezza affliggenti la società, individuando i collegamenti tra gli insorti e le comunità locali ed abilitando azioni di contrasto mirate alle fonti di finanziamento derivanti da attività illecite, ad esempio informando le azioni di polizia d'alto mare volte al contrasto di traffici illegali da parte della componente navale della Forza. È dunque osservabile il ruolo che la LEINT può assolvere a favore della condotta di ciascun elemento di una *Joint Force*, orientandone l'azione, integrandone l'efficacia o proteggendone l'operatività.

Nel dominio terrestre, *in primis*, lo strumento LEINT, inserito nelle aliquote di SP, può sostenere un più efficace controllo del territorio, garantendo un SASE ed assicurando FOM alla componente di terra facilitando la condotta di azioni cinetiche e non. L'accesso informativo ai *database* delle forze di polizia locali può inoltre ampliare la consapevolezza delle dinamiche di potere "occulte" nel settore di intervento, rendendo più efficaci operazioni di *counterinsurgency* (COIN) o di *counter-terrorism* (CT). La LEINT può in aggiunta contribuire in modo privilegiato alla valutazione delle implicazioni a livello sociale ed economico delle azioni e della presenza della Forza, fornendo elementi utili per adeguare o valorizzare la percezione della stessa.

Relativamente al dominio marittimo, essa è in grado di offrire uno strumento cruciale per la sorveglianza dei traffici nelle aree portuali e per la vigilanza di attività criminali lungo le zone litoranee. Una simile attività potrebbe infatti incrementare la profondità della consapevolezza situazionale degli assetti navali, supportando un coordinamento sinergico volto a limitare la permeabilità dei confini marittimi alla penetrazione di fattori di instabilità inficianti sulla condotta dell'intera *Joint Force*. L'analisi dei fenomeni evolutivi afferenti attività criminali nelle aree costiere permette inoltre il tracciamento di fenomeni migratori o di natura economico-commerciale che possono determinare un mutamento delle condizioni di sicurezza nel teatro o una variazione rilevante degli spettri di minaccia. Infine, le informazioni raccolte ed elaborate in attività di *law enforcement* possono contribuire ad incrementare l'accessibilità alle aree litoranee e rafforzare la protezione della componente marittima della Forza.

Nel dominio aereo, invece, la LEINT può essere un utile strumento volto ad orientare l'impiego di assetti aerei, individuando siti di particolare interesse da sottoporre a

sorveglianza dall'alto, nonché integrando, verificando ed avvalorando le informazioni raccolte da questi. Al contempo essa può supportare l'attività di individuazione e repressione alle minacce di bassa quota provenienti dalla progressiva diffusione di droni commerciali e dal loro adattamento da parte di entità criminali e terroristiche per azioni di contro-sorveglianza ed interferenza alle attività della Forza. Lo strumento LEINT può inoltre svolgere un ruolo essenziale nell' incrementare la cornice di sicurezza attorno alle infrastrutture di supporto della componente aeronautica, prevenendo attività criminose e predatorie sull'indotto delle basi e favorendo una migliore integrazione ed accettazione delle stesse da parte delle comunità locali.

Relativamente al dominio *cyber*, infine, la LEINT costituisce un assetto altamente modulare e centrale nell'individuazione di condotte criminose coinvolgenti la rete, con la possibilità di valorizzare specificamente le risorse informative offerte da tale dominio a favore dell'intera *Joint Force*. Sia le attività di WEBINT, sia quelle di SOCMINT generano infatti un incremento della consapevolezza situazionale sull'evoluzione del teatro, rilevando variazioni del dibattito pubblico all'interno di diverse piattaforme, sintomatici di cambiamenti di postura degli attori presenti nel teatro o adeguamento di queste in funzione delle attività della Forza. La vigilanza costante dell'ambiente cibernetico, in cui la LEINT può offrire un contributo agli sforzi attuati dagli assetti specializzati delle altre compagini militari, consente interventi anticipati di mitigazione delle vulnerabilità dei sistemi informatici delle forze dell'ordine locali e del dispositivo, fornendo un valido supporto alla prevenzione e repressione di condotte malevole, anche di natura criminale, afferenti alla sfera *cyber*. Proprio la LEINT può svolgere un ruolo primario nell'impedire lo sviluppo di zone grigie per attività cybercriminali, nel cui sedime potrebbero originarsi minacce securitarie più significative a detrimento della stabilità del teatro, della protezione della Forza o del funzionamento di infrastrutture critiche in altri Paesi della regione.

Nel suo complesso, l'implementazione di strumenti e funzioni LEINT non solamente in missioni a *lead* SP, ma anche ad integrazione di dispositivi interforze in scenari di *Stabilization & Reconstruction*, così come di *Crisis Management* o addirittura di *Full Conflict*, può determinare vantaggi significativi e trasversali, contribuendo ad un più rapido e facile conseguimento dell'obiettivo di missione. La produzione di risultati in tutte e tre le dimensioni ed il ruolo abilitante alle molteplici componenti della *Joint Force* rendono dunque la LEINT funzionale alla produzione di effetti in tutti i domini, costituendo difatti un elemento di vantaggio per la condotta di *Multi-Domain Operations*.

3. Integrare la LEINT

Lo strumento del *Law Enforcement Intelligence* nelle operazioni di *Stability Policing*, connesse all'ambito cibernetico, è inquadrabile nell'ordinamento nazionale ai sensi dell'art. 37 del decreto legge del 9 Agosto 2022, n. 115, c.d. decreto "Aiuti bis". In particolare, è attribuito al Presidente del Consiglio dei Ministri, acquisito il parere del Comitato interministeriale per la sicurezza della Repubblica (CISR) e sentito il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), il potere di emanare disposizioni per l'adozione di particolari misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o emergenza a fronte di minacce che interessano aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale. Tali disposizioni prevedono la cooperazione del Ministero della Difesa e quindi il ricorso alle garanzie funzionali previste all'art. 17, comma 7, della legge 3 Agosto 2007, n. 124. Alla raccolta informativa posta in essere dall'Agenzia informazioni e sicurezza esterna (AISE) e dall' Agenzia informazioni e sicurezza interna (AISI), sono affiancate quindi ulteriori capacità di difesa proattiva/controffensiva con un'adeguata cornice di garanzie e nel rispetto dei principi che formano l'azione dell'Intelligence.

Con l'intento di potenziare la capacità informativa del Comparto *Intelligence*, sono state adottate le seguenti disposizioni di legge: l'ampliamento della disciplina d'impiego all'estero del personale dell'AISE *ex* art. 42 sexies del decreto legge 9 Agosto 2022, n. 115, nonché la modifica con la legge 29 Dicembre 2022, n. 197, in particolare del decreto legge 27 Luglio 2005, n. 144, c.d. "Decreto Pisanu", in materia di intercettazioni preventive/acquisizione di metadati delle comunicazioni elettroniche per i Servizi di Intelligence, volta ad una maggiore autonomia in termini di attività e di gestione delle risorse finanziarie.

Un ulteriore impulso al contrasto delle azioni criminose informatiche potrà esser fornito, inoltre, a seguito dell'adozione del 12 Maggio 2022, del Secondo Protocollo Addizionale[42] alla Convenzione sulla Criminalità Informatica (c.d. Convenzione di Budapest del 2001), voluto da 22 Paesi del Consiglio d'Europa, compreso l'Italia. Con l'autorizzazione alla ratifica dell'Unione Europea avvenuta con la decisione n. 436[43] del 14 Febbraio 2023, riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche, si assicurano strumenti efficaci al fine di ottenere informazioni sugli abbonati e i dati relativi al traffico, ed una

[42] *Secondo Protocollo Addizionale alla Convenzione sulla Criminalità Informatica Riguardante la Cooperazione Rafforzata e la Divulgazione di Prove Elettroniche*, Gazzetta ufficiale dell'Unione europea, 28 Febbraio 2023.

[43] *Decisione (UE) 2023/436 del Consiglio* del 14 Febbraio 2023, Gazzetta ufficiale dell'Unione europea, 28 Febbraio 2023.

cooperazione immediata con i *service provider* in caso di emergenza o indagini congiunte. In attesa della ratifica, sono emerse questioni di compatibilità del suddetto Protocollo con gli ordinamenti interni degli Stati firmatari, per i quali secondo il parere del Consiglio d'Europa, è necessario individuare e porre riserve, dichiarazioni, notifiche e comunicazioni anche in virtù dei loro rapporti reciproci con altri Paesi terzi, parte del Protocollo. Il quadro normativo sopracitato non tralascia i *constraints* che la LEINT dovrà considerare quali le regole auree del *need to know* e *del need to share* volte a prevenire la probabile compromissione, la perdita di integrità o riservatezza dei dati e delle informazioni veicolate. Al riguardo, concentrandosi sulla fruibilità ed accessibilità delle informazioni afferenti le questioni di sicurezza pubblica, relazioni internazionali, nonché eventuali crimini commessi, le embrionali linee guida per un processo di integrazione devono propendere ad una fusione delle informazioni tra le forze dell'ordine (che partecipano alla fase preliminare di acquisizione dati per la parte di precipua competenza) ed il settore privato/istituzionale (incluse le Agenzie di Sicurezza Interna ed Esterna). In tal modo al fine di agevolare tale osmosi*,* si potrebbe convogliare l'unicità della fonte informativa ad appositi *fusion center* (progetto non ancora concretizzato) che supererebbero i limiti normativi ai quali il personale appartenente all'AISE/AISI deve attenersi (non obbligatorietà del *need to share* e possibilità di posticipare l'osmosi informativa con l'Autorità Giudiziaria competente su informazioni che possono costituire elementi di prova ai fini investigativi, se non a seguito di una postuma valutazione tecnica da parte del DIS ai sensi del comma 8 dell'art. 23 della legge 124/2007). Per quanto attiene quest'ultima procedura tecnica, è doveroso evidenziare che, contrariamente all'AISE/AISI, le forze di polizia ad ordinamento militare impiegate al di fuori della territorialità Nazionale possono condividere informazioni/atti tutelati da *segreto investigativo* con altri organi istituzionali a seguito di autorizzazione degli organi della Magistratura competente, insistente nella *Host Nation*, se presente, ovvero di un'Autorità Giudiziaria *ad hoc*, a cui specifici *Technical Agreement* hanno delegato la competenza in materia giudiziaria.

Nel comparto intelligence, in ottica di perfezionamento delle capacità nazionali per individuare, prevenire e contrastare la minaccia ibrida proveniente dal cyberspazio, era stato inizialmente istituito, con il DPCM 17 Febbraio 2017 (c.d. "Decreto Gentiloni") il Nucleo Sicurezza Cibernetica collocato in seno al DIS. Successivamente, la sua riconfigurazione, con il decreto legge 14 Giugno 2021, n. 82, in Agenzia per la Cybersicurezza Nazionale (ACN) ha portato ad una nuova architettura nazionale cibernetica, inquadrante l'ACN al di fuori della comunità intelligence tra quelle attività nazionali definite di *cyber-resilience*, volte a rafforzare le capacità di difesa cibernetica delle infrastrutture sensibili nazionali, c.d.

infrastrutture critiche. Le operazioni condotte da un possibile LEINT team, non sarebbero quindi riconducibili all'ambito di cybersicurezza, ove trovano invece collocazione il Nucleo per la Cybersicurezza e il CSIRT-Italia, ma attribuibili agli Organismi di Informazione e Sicurezza a mente della legge 124/2007, successivamente modificata dalla legge 133/2012. Le operazioni di *cyber-intelligence*, atte a rilevare tempestivamente e a monitorare, prevenire e contrastare in maniera sistematica le minacce cibernetiche, rimangono quindi di peculiare ed esclusiva competenza del Comparto informativo.

4. J2 LEINT ed SP LEINT Team

L'applicazione della dottrina SP si fonda oggi sulla presenza di SMEs/specialisti a livello di Comando operativo e strategico in tempo di pace, crisi o conflitto e, come nei recenti teatri operativi (ad esempio Bosnia Herzegovina e Kosovo) di nuclei a livello tattico quali ad esempio le *Multinational Specialised Units* (MSU) dove il Comandante fungeva, nella prassi, da SP *advisor* del Comandante di Teatro e, con le proprie risorse svolgeva i compiti precipui di questa funzione. Nell'alveo dello sviluppo della dottrina LEINT, in ambito internazionale (NATO, ONU, UE), deve essere quindi compreso dove questa capacità si debba inquadrare negli staff dei Comandi ai vari livelli e immaginare, inoltre, la struttura di una capacità LEINT proiettabile nella forma di un LEINT team, flessibile e interoperabile e che svolga i compiti della funzione del ciclo intelligence "raccolta delle informazioni". Tale sviluppo è necessario per poter fronteggiare un conflitto di natura ibrida dal livello sotto la soglia della guerra (ad esempio in contesto di Difesa delle infrastrutture nazionali o di art. 3[44] della NATO), nel caso in cui il Paese ricorra all'uso delle Forze Armate contro un soggetto statuale (ad es. art. 5[45] della NATO) o ancora in operazioni di risposta alle crisi (ad esempio NA5CRO nella nomenclatura della NATO).

In quest'ottica, contestualmente ad un *Collection Plan* comprensivo degli *Essential Elements of Information* (EEI), gli analisti LEINT possono formulare *information requirements* funzionali a soddisfare specifici *gap* informativi, a cui seguirà, contestualmente alla funzione IRM&CM una loro possibile esplicitazione in *Request For Information* (RFI) o *Request For Clarification* (RFC). La raccolta informativa sul terreno sarà coordinata e gestita, pertanto, dal *Collection Management* anche sopperendo alle deficienze di *expertise* in materia delle unità. La fase di raccolta può infatti venire svolta sia da componenti

[44] Art. 3 (Resilienza): «Allo scopo di conseguire con maggiore efficacia gli obiettivi del presente Trattato, le parti, agendo individualmente e congiuntamente, in modo continuo ed effettivo, mediante lo sviluppo delle loro risorse e prestandosi reciproca assistenza, manterranno e accresceranno la loro capacità individuale e collettiva di resistere ad un attacco armato».

[45] Art. 5: «Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti […]».

specialistiche (HUMINT, IMINT, SIGINT…), sia da assetti non specialistici (ad esempio unità di manovra), operando, però, sempre in coerenza al *Collection Plan*, convertente le esigenze informative (IR-I*nformation Requirements*) in esigenze di raccolta (CR-*Collection Requirements*).

Nell'organigramma di un HQ di livello operativo nazionale o internazionale in BACO (*Baseline Activities and Current Operations*) troviamo generalmente una sezione dedicata allo SP che ne raccoglie gli SMEs e la cui Divisione di inquadramento dipende dalla specifica organizzazione del Comando. Alternativamente può essere adottata una divisione *cross-functional* che ripartisce gli SME SP nelle diverse branche su uno schema per funzione ovvero presso il J5 per il *planning*, J3 per il *refinement*, J2 per l'intelligence e così via in relazione alle esigenze specifiche. Quale che sia l'organizzazione, gli specialisti SP della LEINT saranno inquadrati all'interno della branca J2 con due configurazioni possibili, una robusta che potrebbe essere adottata dai JFC (*Joint Forces Command*) della NATO *Command Structure* (NCS), ed una leggera, più adatta ai comandi della NFS (NATO *Force Structure*) i quali sono chiamati a ricoprire anche i ruoli di unità di livello tattico e di Comando di Componente. La configurazione robusta vedrebbe un SO1 (*Staff Officer* 1) con compiti di coordinamento e *liaison* avente alle dirette dipendenze uno o due SA (*Staff Assistant*) LEINT con l'incarico di analisti di intelligence. Diversamente, nella configurazione leggera il nucleo LEINT non costituirebbe una sezione a sé all'interno del J2, e di conseguenza la funzione LEINT perderebbe la posizione di SO1, inquadrando esclusivamente una o due posizioni da SA con incarico di analista J2 nella sezione di analisi e produzione Intel. L'incaricato quale SO1 LEINT, nella configurazione robusta, è responsabile delle risultanze della fase di identificazione del fabbisogno informativo (collabora alla comprensione dell'ambiente operativo), del coordinamento, della supervisione in esecuzione di tutte le attività LEINT della forza, nonché di quelle condotte a supporto delle forze di polizia dell'*Host Nation* (HN), in operazioni. Egli definisce le priorità delle esigenze informative al fine della prevenzione e identificazione delle minacce di natura ibrida, in chiave di mantenimento della legge, dell'ordine, della sicurezza pubblica e della forza e assicura l'integrazione della LEINT nel ciclo intelligence del Comando Operativo.

Lo SA LEINT si coordina con la cellula di gestione delle richieste di intelligence e di gestione della raccolta (IRM&CM) al fine di coadiuvare il J2 *Production* Manager nella definizione delle prerogative di raccolta che soddisfino i requisiti informativi critici del Comandante (CCIR che oltre alle PIR potrebbero includere le *Host Nation Information Requirements* in prospettiva SP) inerenti la produzione di un quadro informativo strumentale alla stabilizzazione del contesto (ad es. profilazione di personalità e/o specifici gruppi

criminali a titolo di prevenzione, statistiche sui trend criminali). L'analista LEINT provvede alle fasi di trattamento delle informazioni e analisi e produzione sviluppando *assesment* inerenti le minacce individuate sulla base dei dati provenienti dalla raccolta svolta al livello tattico, da attori nazionali ed internazionali statuali e non statuali appartenenti alle comunità intelligence e *law enforcement*.

Per guidare una più incisiva e consapevole attività di prevenzione e contrasto in sostegno o in sostituzione alle forze di polizia locali, ed influenzare positivamente l'azione delle altre componenti militari del contingente, è necessario implementare nel dispositivo SP a livello tattico nuove figure e risorse. In particolare, nel contesto generale della capacità LEINT, è possibile sviluppare un assetto precipuamente orientato al dominio *cyber*. In quest'ottica, gli apparati organizzativi e le competenze da mettere in campo nelle MSU per la gestione della *Data Science* devono costituire un team esperto LEINT che integri le funzioni della cellula G2 così di seguito composto[46]:

- Nr. 1 *Liaison Officer* (OF-2) dedicato alla gestione e condivisione delle informazioni reperite tramite organizzazioni governative e non, il *Multinational CIMIC Group* impiegato nei teatri operativi e le infrastrutture critiche della *Host Nation*; svolge quindi il compito di *Information Mining* con la raccolta di informazioni in documenti reperibili a livello locale relativi ad una persona o argomento specifico (nuovi articoli, pubblicazioni, libri bianchi, brevetti militari) che costituiscono input che per la pianificazione della strategia di intelligence ad un livello superiore;
- Nr. 1 Ufficiale (OF-2) ingegnere informatico o delle telecomunicazioni per l'implementazione dell'infrastruttura tecnologica per l'elaborazione di grandi quantità di dati in tempo reale e software con algoritmi innovativi di intelligenza artificiale; ricopre i compiti di *Data analyst* (per ricercare evidenze quantitative all'interno di grandi moli di dati), *Data scientist* (per lo sviluppo, training e testing di modelli statistici e algoritmi di apprendimento automatico) e *Data engineer* (per rendere i dati disponibili per le analisi nel giusto formato). Inoltre ottimizza le analisi predittive degli algoritmi di Intelligenze artificiali e controllano l'apprendimento automatico di tali algoritmi;
- Nr. 1 Ufficiale (OF-3) che ricopra l'incarico di *Data science manager* per gestisce l'intero processo di Data Science. Ha il compito di interfaccia con la cellula G2. È responsabile delle acquisizioni delle informazioni necessarie al ciclo di intelligence così da consentire operazioni di risposta ad un eventuale controspionaggio o terrorismo in

[46] Si noti come il numero e la professionalità delle figure indicate si fondi su un'ipotesi di massima aderenza dell'assetto LEINT ai requisiti ed alle esigenze individuate nel presente studio, pur nella consapevolezza degli inevitabili vincoli di risorse e difficile reperibilità di competenze a cui attingere nei contesti reali.

tempo reale. Formula, inoltre, le proposte dell'IA da avanzare, tramite il Comandante del Reggimento, alle istituzioni locali al fine di migliorare il supporto alle forze di polizia locali ed il supporto alle autorità nazionali a generare risposte più rapide ed efficaci.

5. Un *Case Study*: Afghanistan

Al fine di evidenziare gli effetti positivi dell'integrazione di capacità LEINT all'interno di aliquote di *Stability Policing* nel contesto di operazioni fuori area, è utile analizzare retrospettivamente le *lessons learned* di un caso studio specifico quale quello relativo all'Afghanistan. Dopo l'intervento in Afghanistan, per quasi 20 anni la NATO ha infatti fornito un significativo sostegno alle Forze di Sicurezza Nazionale afghane, con l'obiettivo di creare una forza di polizia legittima, responsabile ed efficace in grado di proteggere la popolazione dai criminali e far rispettare lo stato di diritto del Paese, supportando la formazione di un apparato statale.

L'intervento in Afghanistan ha presentato una elevata complessità, il vasto spettro di problemi di sicurezza riscontrati durante l'intervento internazionale (terrorismo e insurrezioni che si basavano su tattiche asimmetriche, criminalità organizzata, criminali, sommosse, ecc.) avrebbe suggerito il dispiegamento di una forza di polizia versatile come quella dello *Stability Policing*, in grado di calibrare diversi livelli di potenza per affrontare queste minacce, come la NATO ha fatto nei Balcani.

La decisione di procedere invece con il cosiddetto *light footprint* ha portato a un peggioramento delle condizioni di sicurezza che ha reso poi necessario lo sviluppo urgente di una forza di polizia afghana in grado di essere professionale, efficace e rappresentativa della diversità etnica del paese.

Trovare la giusta relazione tra elementi militari e civili durante la riforma delle forze di polizia in regioni di conflitto e post-conflitto è difficile e varia in considerazione di molteplici variabili sociali, culturali, storiche e politiche. I principi della Riforma del Settore della Sicurezza (SSR) civile e democratica sottolineano la necessità di separare l'esercito e la polizia, tuttavia, la realtà quotidiana in molti luoghi non lo consente. La polizia deve adottare una posizione decisa per chiudere le lacune di sicurezza e procedere contro criminali armati o insorti ben organizzati. Nel contesto di riforma della polizia in Stati fragili, è necessario che la polizia sia il più possibile civile e il più possibile militare per quanto riguarda attrezzatura, approccio, struttura e compiti. La rapida militarizzazione della polizia può causare problemi portando a una frattura con la popolazione che impedirebbe lo sviluppo di una relazione di fiducia fondamentale per le azioni di polizia.

La Riforma del Settore della Sicurezza in Afghanistan (SSR) è stata avviata nel 2002 con l'obiettivo di creare un comparto della sicurezza costituzionale, efficace ed efficiente, legittimato democraticamente. La Riforma mirava a riorganizzare le forze armate, la polizia, le autorità giudiziarie e i servizi di intelligence basandosi su principi come la trasparenza, la professionalità e l'efficienza.

Uno dei principali problemi è la mancanza di chiarezza concettuale, il che rende difficile identificare quali *stakeholder* della sicurezza dovrebbero avere la priorità. Ciò ha portato alla necessità di coinvolgere tutti gli *stakeholder* importanti nei processi di riforma.

Gli *stakeholder* della SSR hanno riconosciuto il pericolo di sottovalutare il contenuto politico della SSR, dove l'ignoranza dei contesti locali spesso impedisce loro di adottare un approccio mirato alle specifiche esigenze del posto. Dalla fine del 2007, gli *stakeholder* internazionali si sono concentrati sul Programma di Sviluppo del Distretto Focalizzato (FDD). Questi sono stati organizzati in Team di *Mentor* della Polizia (PMT) e in Team di *Mentoring* e di Collegamento Operativo della Polizia (POMLT).

Tuttavia, nonostante gli sforzi della comunità internazionale, la riforma ha avuto scarso impatto sui problemi istituzionali più ampi, come la corruzione e la mancanza di responsabilità, anche per la mancanza di una visione strategica unificata che ha limitato gli effetti di tale riforma.

Nel corso di un *workshop*, tenutosi a Vicenza nel Luglio 2022, organizzato dal NATO *Stability Policing Centre of Excellence,* sono stati analizzati tre diversi aspetti dell'intervento NATO e individuate le relative *lesson learned.*

Il primo *syndacate* si è concentrato specificatamente sul livello strategico, nello specifico, idealmente, la riforma del settore della sicurezza nei Paesi post-conflitto è lineare. In primo luogo, l'esercito assume i compiti di polizia, in particolare se la situazione della sicurezza è precaria, segue poi una graduale transizione verso un modello di polizia civile. Gli interventi internazionali non sono riusciti ad aiutare a stabilire l'ordine pubblico e lo stato di diritto nei decisivi primi anni coordinando i loro approcci. Sul lato afghano, l'escalation del conflitto armato, la scarsa leadership governativa, l'assenza di una tradizione di lavoro di polizia civile e lo stato desolante della polizia hanno favorito la deriva militare della riforma della polizia. Il collasso del governo afghano e delle forze di difesa e sicurezza nazionale afghane nel 2021 sottolinea l'importanza di stabilire un servizio di polizia affidabile ed efficace nella stabilizzazione dei Paesi post-conflitto. Senza un servizio di polizia affidabile per far rispettare le leggi della nazione e proteggere i suoi cittadini, un paese è costantemente a rischio di instabilità e di ritornare nuovamente al conflitto.

Il secondo *syndacate* ha analizzato il livello operativo. È stato evidenziato come, nonostante gli ingenti sforzi economici, la Comunità Internazionale non sia riuscita a costruire forze di polizia responsabili ed efficaci. Al contrario, lo spreco di finanziamenti, il nepotismo e la corruzione hanno aggravato la percezione negativa della popolazione civile verso le forze di polizia locali, che sono diventate le organizzazioni più odiate e corrotte in Afghanistan, e gli attori internazionali coinvolti nella stabilizzazione del Paese. La maggior parte della formazione e del *mentoring* delle forze di polizia locali è stata svolta, inoltre, da *asset* NATO non dotati di mentalità di polizia, creando così una ANP sbilanciata militarmente. I moduli di formazione dedicati all'attività investigativa e alla raccolta di informazioni hanno avuto un impatto decrescente sui programmi addestrativi svolti, sottovalutando l'importanza che una LEINT integrata con le forze di SP avrebbe potuto avere sull'effettivo controllo del territorio.

Infine, il terzo *syndacate* si è concentrato sul livello tattico. A partire dalla fine del 2007, la NATO ha creato team di mentoring di polizia chiamati *Police Operational and Mentoring Liaison Teams* (POMLT), per distinguerli dai team di mentoring militari degli Stati Uniti.

Gli Stati membri hanno investito molto nei POMLT, contribuendo con circa 400 ufficiali impiegati in team di *mentoring* composti da 15-20 persone ognuno, provenienti da polizia militare o dalle forze terrestri o dalle unità di gendarmeria come la *Guardia Civil* spagnola, la *Gendarmerie Nationale* francese o i Carabinieri italiani.

Oltre a fornire assistenza in termini di formazione ed equipaggiamento, i partner internazionali hanno anche aiutato l'ANP migliorandone le infrastrutture, in particolare costruendo Stazioni di Polizia. Sebbene l'inclusione della NATO nella missione di assistenza di polizia abbia coordinato meglio il supporto militare internazionale, non ha migliorato il coordinamento con le agenzie civili influenzando la missione a livello di strategia, pianificazione e finanziamento.

I corsi di formazione hanno posto maggiormente l'accento sulle abilità militari come la gestione delle armi, l'istituzione di posti di blocco e l'identificazione di dispositivi esplosivi improvvisati (IED). Circa sette delle otto settimane di formazione di polizia sono state dedicate all'apprendimento di abilità militari. Solo circa una settimana rimaneva per imparare questioni come la Costituzione dell'Afghanistan, il processo penale o i diritti umani. Il contenuto civile della formazione di base della polizia è stato ulteriormente ridotto a partire da Novembre 2008. La formazione di tipo militare ha sostituito le lezioni sul lavoro di polizia orientato alla comunità, la violenza domestica e i diritti delle donne.

Quando la Comunità Internazionale (IC) si appresta ad entrare in un Paese come l'Afghanistan, o in altri, dovrebbe sapere che ogni Paese è unico nella sua modalità di fare

polizia come pure nella cultura, nella storia e nel tipo di criminalità a medio termine. Una polizia efficace è necessaria per stabilizzare un Paese in quanto sarà in grado di fornire lo stato di diritto e l'applicazione della legge.

La NATO non ha ancora individuato uno standard per l'assistenza internazionale alla polizia e su come dovrebbe essere organizzata. Non fare niente è destabilizzante, come si è visto in Afghanistan, non intervenire nella *golden hour* permetterà in ogni circostanza, alle persone che competono per il potere e per l'influenza, di usare le forze di polizia per rafforzare posizioni di potere dal punto di vista politico, ed in tali condizioni gli *advisor* di polizia vedranno le loro possibilità di riformare quella forza di polizia diminuire drasticamente al loro arrivo.

L'attività di *mentoring* alle forze di polizia deve essere coordinata con altri componenti della giustizia al fine di sviluppare in maniera coordinata il rispetto delle regole e la certezza della pena in uno Stato in fase di costruzione. Ciò non è avvenuto in Afghanistan destabilizzando di fatto entrambe le istituzioni e diminuendone la legittimità agli occhi della popolazione.

Affinché la *leadership* della polizia in fase di formazione possa sentirsi seguita nel processo di maturazione professionale, sarebbe necessario che la *partnership* con i *mentors* fosse a lungo termine. Questo è un grande problema nell'ambiente NATO, in cui gli *advisors* sono stati dispiegati per 6 mesi senza poter dare continuità al loro lavoro. Tale rotazione, unita alla mancanza di direttive comuni e condivise, portava la formazione a continue rivoluzioni a cadenza periodica. Prevedere rotazioni più lunghe per le figure apicali, o rotazioni non contestuali di intere unità aumenterebbe la consistenza dell'attività formativa con indiscusse ripercussioni positive sull'efficacia dell'addestramento e la razionalizzazione delle risorse impiegate.

I diversi Paesi della NATO hanno approcci disuguali ed è evidente quanto la creazione di un centro congiunto per il coordinamento delle attività di *mentoring*, nell'ambito SP, non possa essere ritardato, per il fine comune di tutte le Nazioni di razionalizzare la spesa quando impiegate all'estero. Tale centro potrebbe fornire supporto tecnico, sviluppo di capacità, consulenza, condivisione di intelligence e coordinamento di attività investigative. Ciò permetterebbe, in una missione NATO, di definire chiaramente gli obiettivi intermedi e l'*end state* desiderato dai diversi *stakeholders*, stabilendo, inoltre, chiaramente compiti e responsabilità. Al di fuori del contesto NATO, la definizione di standard condivisi offrirebbe invece una linea guida utile per evitare duplicazioni e sprechi di risorse.

La nuova ascesa dei talebani in Afghanistan è stata possibile anche per l'incapacità dell'apparato statale del governo di Kabul di fornire sicurezza alla popolazione. È quindi

fondamentale per la CI comprendere quali siano state le lacune nell'attività di mentoring, affinchè in una futura attività similare si possa assistere al raggiungimento dei risultati politici prefissati, a fronte di un così importante investimento economico. Ampliare l'uso del LEINT, in una missione di *peace-keeping* o *peace-enforcement,* consentirebbe di mantenere un legame più stretto con la popolazione civile e di comprenderne meglio le dinamiche e le correlazioni interne. L'intelligence sulle attività criminali e terroristiche potrebbe, inoltre, aiutare a identificare le fonti di finanziamento delle organizzazioni criminali o dei gruppi terroristici, consentendo di interrompere le loro attività illegali e di indebolirne la capacità di sostenere azioni violente. In questi ambiti, il dominio cibernetico potrebbe essere utilizzato per monitorare le attività online dei gruppi terroristici, seguendone i flussi finanziari anche al fine di comprenderne i finanziatori esterni, o intercettandone le comunicazioni criptate.

In terzo luogo, l'uso dell'intelligence potrebbe anche contribuire a migliorare la cooperazione tra le forze di polizia internazionali e le forze di mantenimento della pace locali, consentendo loro di lavorare insieme per risolvere le questioni legate alla sicurezza. Fondamentale, in tal caso, la protezione delle infrastrutture critiche dalle minacce cibernetiche e l'utilizzo del dominio *cyber* per la raccolta di informazioni sensibili, gestendolo con cautela e nel rispetto dei diritti umani e delle libertà civili.

In generale, l'intelligence applicata al *law enforcement* potrebbe fornire informazioni essenziali per prevenire e gestire situazioni di crisi, aumentando la capacità delle forze di mantenimento della pace di stabilizzare un Paese e garantire la sicurezza della popolazione locale, prevenendo il ritorno ai regimi precedenti. L'opportunità di applicare le lezioni dell'Afghanistan a future missioni di assistenza e ricostruzione della polizia non dovrebbe essere sprecata.

CONCLUSIONI

Lo scenario internazionale contemporaneo è caratterizzato più che mai da crescente instabilità, insicurezza e frammentazione, associata ad una diversificazione ed ibridazione delle minacce che pongono sfide inedite alla pianificazione e condotta di operazioni militari all'estero, indipendentemente dalla natura delle stesse. Dalle missioni di supporto alla pace, a quelle di stabilizzazione e ricostruzione, dal *crisis management* fino al ritorno di conflitti convenzionali ad alta intensità, in ogni contesto si assiste ad una progressiva compenetrazione degli strumenti di potere e ad un processo di *weaponisation of everything*[47]*,* mostrando limiti e vulnerabilità degli assetti militari tradizionali. Il presente lavoro ha cercato di sviluppare, sottolineandone le specificità ed i vantaggi, ma anche le sfide e le criticità, di una possibile proposta volta ad adeguare, integrandole, le capacità normalmente schierate in un teatro. La *Law Enforcement Intelligence*, vastamente approfondita nei capitoli precedenti può infatti costituire uno strumento particolarmente adatto a contribuire allo sviluppo di una consapevolezza situazionale dettagliata e precisa dell'ambiente operativo, soprattutto in un'ottica di *comprehensive approach* ed in funzione della produzione di effetti trasversali alle dimensioni fisiche, virtuale e cognitiva in un *framework* di *multi-domain operations*.

Sviluppatasi originariamente con finalità di sicurezza interna e di prevenzione delle minacce all'ordine pubblico, l'integrazione della LEINT nella condotta di operazioni militari, in particolare attraverso la valorizzazione delle capacità peculiari offerte dalle aliquote di *Stability Policing*, può oggi rappresentare una risposta estremamente adatta ad individuare, prevenire, contrastare e reprimere minacce ibride sotto-soglia. L'esistenza di queste è, difatti, non solo causa di attriti per le forze convenzionali, pregiudicane e ritardandone i risultati delle loro azioni, ma è, soprattutto, alla base per lo sviluppo e l'espansione di spazi di insicurezza ed instabilità, anche con caratteri transnazionali. La LEINT offre uno strumento versatile e polivalente idoneo ad ampliare ed approfondire il quadro di intelligence, favorendo una comprensione più estensiva dei fattori avversi alla missione e delle minacce attive nel teatro, contribuendo, contemporaneamente, a sostenere le istituzioni locali, in particolare quelle di polizia, attraverso l'analisi dei fenomeni criminali locali e la condivisione biunivoca di informazioni. La pervasività delle attività nel dominio cibernetico, così come la sua accessibilità e predisposizione alla condotta di attività malevole sotto-soglia, rendono poi il *cyber* un ambito di precipuo interesse per il contrasto

[47] Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 15 Febbraio 2022.

alle minacce ibride, dove le attività di raccolta, analisi e diffusione informativa sviluppati dalle forze dell'ordine possono garantire un presidio persistente e funzionale volto a sostenere ed abilitare il processo decisionale dei Comandanti.

Definire la LEINT all'interno del perimetro dottrinale della NATO e determinarne caratteri e concetti, come ambiziosamente tentato nell'ultimo capitolo, è un essenziale passo avanti nel diversificare ed arricchire gli strumenti di cui l'Alleanza Atlantica dispone per adempiere ai suoi compiti. Configurandosi come una funzione, la LEINT può beneficiare dell'apporto di molteplici e diversificati assetti, valorizzando concretamente soprattutto l'apporto capacitivo e di *expertise* che Unità, dalla natura intrinsecamente bicefala, come le *Gendarmerie Type Forces,* possono offrire in tutti i teatri ed in tutte le tipologie di operazioni. Il dettaglio ordinativo della configurazione di un assetto tattico di *Stability Policing* con capacità LEINT e le corrispondenti figure da inquadrare a livello operativo all'interno dello *staff* J2 costituisce, infine, un utile punto di partenza per fissare dei riferimenti reali volti alla pragmatica implementazione di queste capacità all'interno di una *Joint Task Force* da dispiegarsi in un teatro. Inserire la dimensione di *Law Enforcement* all'interno di operazioni militari appare in linea con un approccio a 360° ed una prospettiva di *Multi-Domain Operations*. In quest'ottica, la LEINT può apportare un significativo e rilevante contributo alla NATO *Intelligence Enterprise* nell'identificazione e contrasto alle minacce ibride e, pertanto, lo *Stability Policing* è, per definizione, uno *stakeholder* chiave.

In conclusione, se, come anticipato, negli scenari operativi contemporanei tutto può diventare un'arma, allora la conoscenza più ampia possibile di tutte le potenziali fonti di minaccia diviene essenziale per anticipare l'azione di attori malevoli e mantenere l'iniziativa. Integrare la LEINT nell'attuale quadro di intelligence si orienta a questo cruciale obiettivo.

BIBLIOGRAFIA

Libri

- Alexandru Herciu, *Adapted Strategies for Countering Hybrid Threats: Consideration on Hybrid Conflict*, LAP LAMBERT Academic Publishing, 31 Gennaio 2019.
- Brin Najzer, *The Hybrid Age: International Security in the Era of Hybrid Warfare*, I.B. Tauris, Londra 2020.
- F. Buffa, *Profili Penali del Commercio Elettronico*, Giuffrè, 2006.
- L. Luparia e G. Ziccardi, *Investigazione Penale e Tecnologia Informatica*, Giuffrè, 2007.
- Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 15 Febbraio 2022.
- Mark Phythian, *Understanding the Intelligence Cycle*, Routledge, 2013.
- Mikael Weissmann, Niklas Nilsson e Björn Palmertz, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, I. B. Tauris, Londra 2021.

Pubblicazioni e documenti

- AJP-3.22 NATO *Allied Joint Doctrine for Stability Policing*, Luglio 2016.
- AJP-3.4.1 NATO *Allied Joint Doctrine for the Military Contribution to Peace Support*, Dicembre 2014.
- AJP-3.4.5 NATO *Allied Joint Doctrine for the Military Contribution to Stabilization and Reconstruction*, Dicembre 2015.
- Aldo Rosa, *Cyber: A New Domain for Stability Policing?*, CoESPU Magazine, 11 Aprile 2022.
- Alessandro Colombo, Paolo Magri e Giampiero Massolo, *Ritorno al Futuro*, Rapporto ISPI 2023.
- Anders Åslund, *Europe can win Putin's gas war but must learn Nord Stream lessons*, Atlantic Council, 6 Settembre 2022.
- *Approccio della Difesa alle Operazioni Multidominio* ed.2022, Stato Maggiore della Difesa.
- David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Michigan State University, Institute for Intergovernmental Research, 2022.
- David L. Carter, *Law Enforcement Intelligence Operations: Concepts, Issues & Terms*, School of Criminal Justice, 1990.

- *Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber*, Camera dei Deputati, XVIII Legislatura, Servizio Studi-Documentazione e ricerche, 24 Settembre 2019.
- *Libro bianco per la difesa e la sicurezza internazionale*, Ministero della Difesa, 2015.
- M. Delle Donne, *Tecniche d'Indagine della Polizia Postale nell'ambito dei reati informatici e nella pornografia online*, in Diritto e Diritti, 2017.
- Marco Codispoti, *SP in Supporting Fragile Countries' Resilience*, CoESPU Magazine, 25 Luglio 2022.
- MC 0655 *Military Concept for Projecting Stability*, 24 Aprile 2018.
- NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Febbraio 2013.
- NATO SP COE, *Stability Policing in Afghanistan: did NATO miss an Opportunity? Lessons from a 20-year Campaign*, 2022 LL Branch – Final Report, Settembre 2022.
- NATO *Strategic Concept* 2022.
- *Secondo Protocollo Addizionale alla Convenzione sulla Criminalità Informatica Riguardante la Cooperazione Rafforzata e la Divulgazione di Prove Elettroniche*, Gazzetta ufficiale dell'Unione europea, 28 Febbraio 2023. Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023, Gazzetta ufficiale dell'Unione europea, 28 Febbraio 2023.
- Sir David Omand, Jamie Bartlett e Carl Miller, *Introducing Social Media Intelligence (SOCMINT), Intelligence and National Security*, Vol. 27, n.6, pp. 801-823, Dicembre 2012.
- Her Majesty's Inspectorate of the Constabulary (HMIC), *The Rules of Engagement: A Review of the August 2011 Disorders*, London.
- UK Ministry of Defence, *Cyber primer*, Ottobre 2022.

Articoli Internet

- Alessandro Burato, SocMInt: un nuovo spazio per la raccolta di informazioni rilevanti, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/socmint-un-nuovo-spazio-per-la-raccolta-di-informazioni-rilevanti.html (accesso effettuato il 20/02/2023).
- *How to manage complexity and realize the value of big data*, https://www.ibm.com/blogs/services/2020/05/28/how-to-manage-complexity-and-realize-the-value-of-big-data/ (accesso effettuato il 10/12/2022).

- Marco Lombardi, Alessandro Burato e Marco Maiolino, Dalla SocMInt alla Digital HumInt, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/dalla-socmint-alla-digital-humint.html (accesso effettuato il 22/02/2023).
- Mario Caligiuri, Cyber intelligence, la sfida dei data scientist, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html (accesso effettuato il 26/02/2023).
- Saverio Setti, Intelligence e indagine penale in Italia, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligence-e-indagine-penale-in-italia.html (accesso effettuato il 15/03/2023).
- Saverio Setti, La tutela del segreto di Stato nella procedura penale, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-tutela-del-segreto-di-stato-nella-procedura-penale.html (accesso effettuato il 13/03/2023).
- Stefano Mele, Matteo Faini e Carmine America, Social media intelligence e sicurezza nazionale, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/social-media-intelligence-e-sicurezza-nazionale.html (accesso effettuato il 24/02/2023).

Altri siti

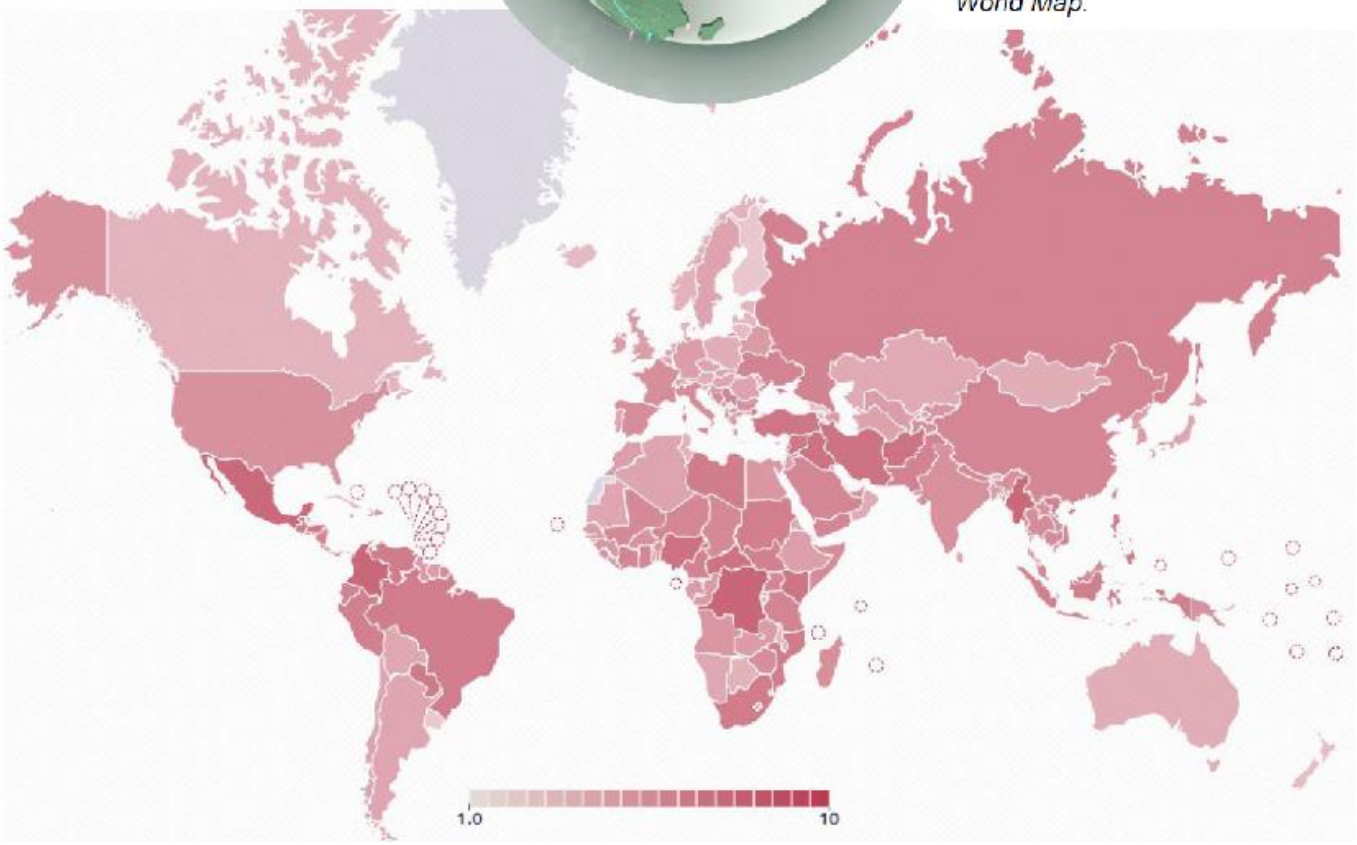
- Agenzia per l'Italia Digitale, www.agid.gov.it (accesso effettuato il 14/02/2023).
- Arma dei Carabinieri, www.carabinieri.it (accesso effettuato il 19/01/2023).
- EUROPOL, www.europol.europa.eu (accesso effettuato il 16/02/2023).
- Esercito Italiano, www.esercito.difesa.it (accesso effettuato il 21/12/2022).
- INTERPOL, www.interpol.int (accesso effettuato il 13/03/2023).
- Sistema di Informazione per la Sicurezza della Repubblica, www.sicurezzanazionale.gov.it (accesso effettuato il 17/02/2023).
- NATO, www.nato.int (accesso effettuato il 24/01/2023).
- NATO SP COE, www.nspcoe.org (accesso effettuato il 29/03/2023).

Un Mondo Instabile di Minacce Multilivello

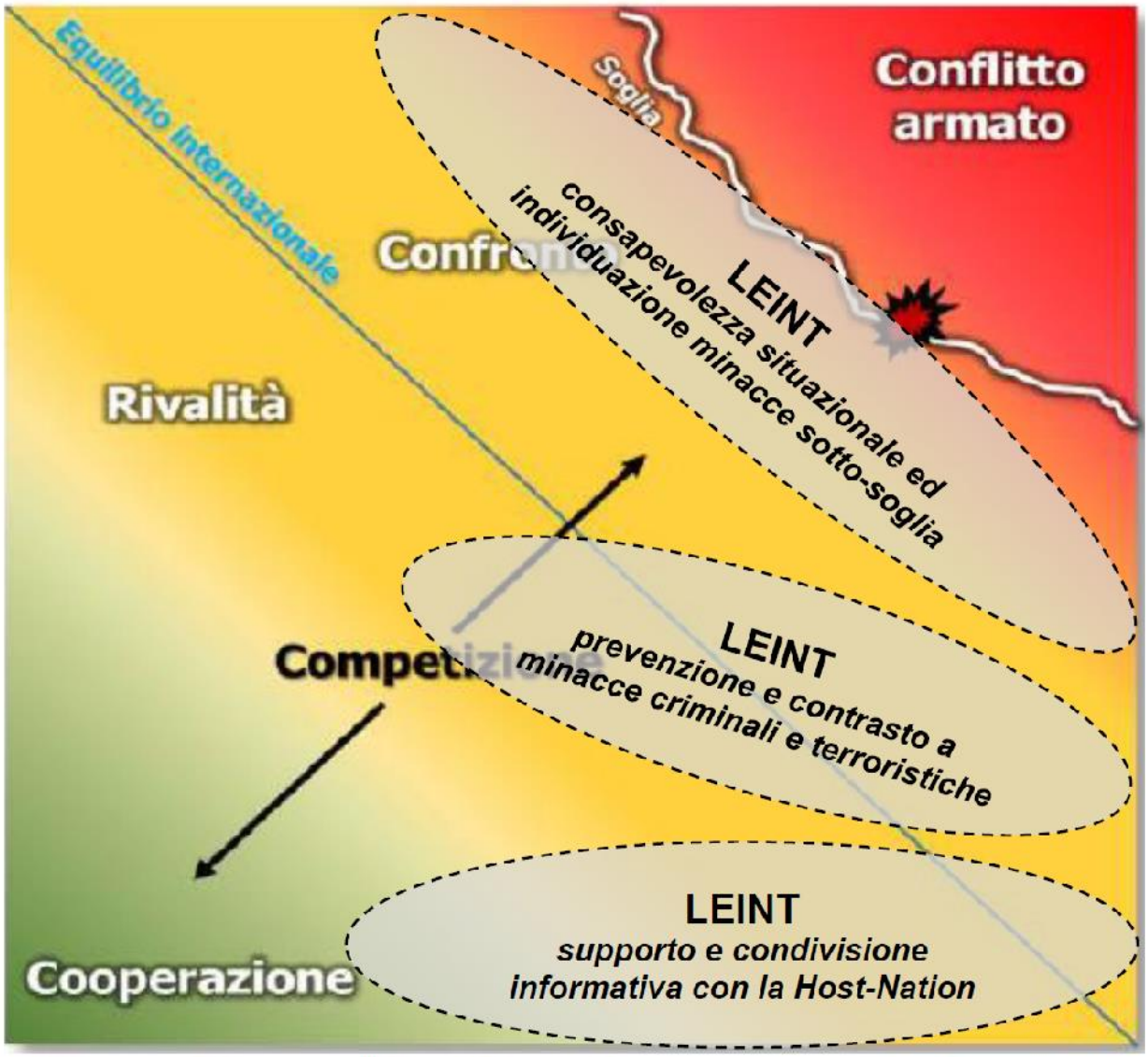
Uppsala Conflict Data Program, *fatal events in 2021 by type of violence, World Map.*

Kaspersky, *Cyberthreat Real-Time Map.*

Global Organized Crime Index, *World Map.*

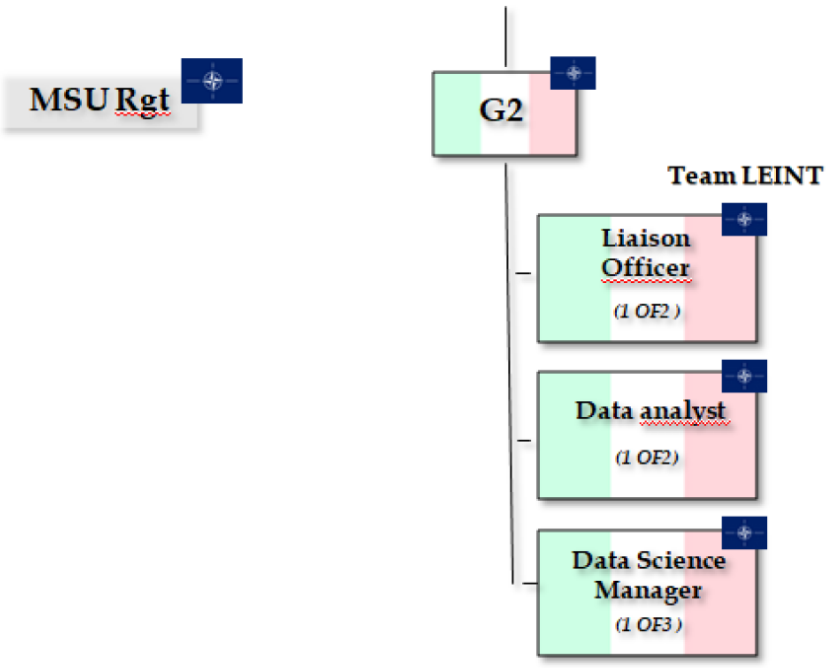


La LEINT nel Continuum of Competition



Rielaborazione degli autori sulla base del Grafico *Il Continuum of Competition*, *Approccio della Difesa alle Operazioni Multidominio* ed.2022, Stato Maggiore della Difesa.

Organigramma di un *SP LEINT Team*



Job Description

- *Liaison Officer (Information Mining Specialist)*: raccogliere informazioni in documenti reperibili a livello locale relativi ad una persona o argomento specifico (nuovi articoli, pubblicazioni, libri bianchi, brevetti militari) che costituiscono input che per la pianificazione della strategia di intelligence ad un livello superiore;
- *Data analyst*: implementare l'infrastruttura tecnologica per l'elaborazione di grandi quantità di dati in tempo reale e software con algoritmi innovativi di intelligenza artificiale; ricerca evidenze quantitative all'interno di grandi moli di dati; sviluppo, training e testing di modelli statistici e algoritmi di apprendimento automatico; rendere i dati disponibili per le analisi nel giusto formato; ottimizzare le analisi predittive degli algoritmi di Intelligenze artificiali e controllare l'apprendimento automatico di tali algoritmi;
- *Data science manager*: gestire l'intero processo di *Data Science*. Interfaccia con la cellula G2 nel formulare proposte dell'IA da avanzare alle istituzioni locali al fine di migliorare il supporto alle forze di polizia locali ed il supporto alle autorità nazionali a generare risposte più rapide ed efficaci.

ISBN 979-12-5515-045-9