



UNICA

UNIVERSITÀ
DEGLI STUDI
DI CAGLIARI

DOTTORATO DI RICERCA IN

Storia, Beni Culturali e Studi Internazionali

Indirizzo Studi d'Area e Internazionali, Storia, Spazi e Società

Ciclo XXXV

TITOLO TESI

Lo sviluppo della Politica di Sicurezza e di Difesa Comune dell'Unione Europea e la condivisione dell'intelligence quale opportunità per il rilancio di una nuova Difesa europea

Settore scientifico-disciplinare di afferenza

SPS/06 Storia delle Relazioni Internazionali

Presentata da

Dott. Pietro Lucania

Supervisore/a

Prof. Christian Rossi

Esame finale anno accademico 2021/2022

Tesi discussa nella sessione d'esame di aprile 2023

Ringraziamenti

Trascorsi tre anni dall'applicazione nella ricerca è arrivato il momento di dare un tocco finale a questo paziente lavoro. Piacevolissima la sensazione di accrescimento sia sotto il profilo professionale e sia sotto il profilo personale ma più di ogni altra cosa mi preme sottolineare l'impagabile percezione che un obiettivo, a lungo cercato e desiderato, sta per realizzarsi. Si tratta di un impegno portato avanti in un periodo in cui sono state riscritte le regole del vivere in società e in cui gli stessi cardini del diritto hanno subito scossoni sui quali si parlerà ancora per parecchio tempo e che costituiranno, essi stessi, materiale per future attività di ricerca; future, perché solo tra molti anni sarà possibile individuare, decrittare e discutere in maniera pacifica di questo stravolgimento epocale vissuto. Nonostante tutto, questo percorso è stato concluso e, un grandissimo merito va a voi: Ornella, Edoardo e Ludovico che mi avete consentito di definirlo con successo, supportandomi in ogni circostanza, facendovi carico di impegni e questioni anche complesse, per tutto questo tempo. Un ringraziamento speciale a chi mi ha esortato sin dall'inizio, credendo in me, in questo progetto, con tanta grinta e caparbia, tra mille difficoltà, proprio per questo: importante. Sincera gratitudine rivolgo alla Prof. Cecilia Tasca, già coordinatrice, per la sua professionalità e lo spirito di comprensione che mi hanno consentito di completare un percorso non certo facile; al Prof. Lorenzo Tanzini, attuale coordinatore, nonché al tutor Prof. Christian Rossi, sempre attento, prodigo di consigli: chiari efficaci ed essenziali in questo lavoro.

INDICE

Introduzione

Obiettivo della tesi

Materiali e Metodi

Cronologia di interesse

Capitolo 1: la Politica di Sicurezza e Difesa dell'Unione Europea

1.1 Le origini

1.1.1 Le esigenze di sicurezza e il Trattato di Bruxelles

1.1.2 Il Trattato Nord Atlantico

1.1.3 La CECA

1.1.4 La presenza militare nel continente, il Piano Marshall

1.2 La CED: il progetto di un esercito europeo

1.2.1 Le origini e le perplessità dei francesi

1.2.2 La visione europea, gli interessi USA e la posizione italiana

1.2.3 Il rifiuto francese, l'assetto NATO e il Piano Fouchet

1.2.4 Il Trattato dell'Eliseo

1.3 La nuova Politica di Sicurezza e Difesa

1.3.1 Il concetto di Foreign and Security Policy

1.3.2 Nascita ed evoluzione della PESD

1.3.3 Rapporti UE-NATO

1.3.4 Il Trattato di Lisbona e la PSDC

1.4 Dal Trattato di Lisbona alla PESCO

1.4.1 Il Trattato di Lisbona e le sue implicazioni

1.4.2 La nuova Strategia Globale

1.4.3 La Cooperazione Strutturata Permanente PESCO

1.4.4 La Revisione Strategica della PESCO

1.5 La PSDC nell'Europa dei 27

1.5.1 La Brexit

1.5.2 Il Trattato di Aquisgrana/Aachen (Francia-Germania)

1.5.3 L'era Covid-19

1.5.4 Il Trattato del Quirinale (Francia-Italia)

Capitolo 2: L'Intelligence nell'ambito dell'Unione Europea

2.1 L'idea di una intelligence europea

2.1.1 La situazione nel dopoguerra

2.1.2 I presupposti storici per una intelligence comune

2.1.3 La visione NATO

2.2 Il SitCen (EU Situation Centre)

2.2.1 Le origini del centro

2.2.2 Evoluzione e nuove collaborazioni

2.3 L'IntCen (EU Intelligence and Situation Centre)

2.3.1 Il Centro: struttura e compiti

2.3.2 Le sfide attuali

2.3.3 Evoluzione e nuove direttrici

2.4 L'intelligence sharing nell'Unione Europea

2.4.1 Le nuove piattaforme di condivisione

2.4.2 Le strutture già esistenti

2.4.3 Efficacia e criticità

2.5 L'UE tra status quo e maggiore autonomia

2.5.1 Obiettivi futuri

2.5.2 La dimensione giuridica, economica e psicologica.

2.5.3 La prospettiva di maggiore autonomia.

Capitolo 3: Difesa e Intelligence comuni: uno sguardo al futuro

3.1 La collaborazione UE NATO nella Difesa e la sfida alle minacce ibride.

3.1.1 Terminologia e aspetti

3.1.2 La pianificazione delle politiche

3.1.3 Le principali iniziative e implicazioni nelle politiche di Difesa

3.2 La collaborazione UE-NATO nell'intelligence

3.2.1 L'esigenza di maggiore cooperazione

3.2.2 Spinte endogene, spinte esogene e slancio cooperativo

3.2.3 *Intelligence warning system*

3.3 Intelligence e grey zone

3.3.1 *Sfida alle funzioni principali*

3.3.2 *Percorsi di ottimizzazione*

3.3.3 *La trasformazione digitale*

3.4 La dimensione dello spazio e quella dei fondali marini

3.4.1 *Spazio e supremazia*

3.4.2 *Tecnologie e sistemi antisatellite*

3.4.3 *Geopolitica dei fondali marini*

3.5 Processi decisionali ed esigenze di sicurezza

3.5.1 *Difesa totale e processi di resilienza*

3.5.2 *Resistance Operating Concept*

3.5.3 *L'intelligence tra vecchi e nuovi schemi*

Annessi:

Annesso 1: Intervista al generale di Divisione Massimo Mingiardi

Annesso 2: Intervista a S.E. Amb. Giampiero Massolo

Annesso 3: Intervista al Prof. Cesare La Mantia

Conclusioni

INTRODUZIONE

Il tema della sicurezza e difesa dell'Unione europea è stato a lungo trattato come un aspetto marginale nello scenario della politica d'integrazione europea. Le criticità sperimentate dai governi europei nella creazione di una politica di sicurezza condivisa, unitamente alle difficoltà nell'assumere decisioni concordate in merito all'utilizzo delle capacità militari hanno inciso negativamente sulla percezione dell'Unione come attore internazionale. Il dibattito sulla difesa europea e le relative politiche adottate a livello nazionale rappresentano una sintesi tra gli obiettivi raggiunti in ambito europeo e gli interessi particolari degli stati membri. I risultati ottenuti in materia di sicurezza restano, pertanto, legati alla convergenza o alla divergenza degli approcci nazionali sui principali temi che la difesa europea dovrebbe affrontare per garantire gli interessi comuni dell'Unione. Pertanto, si è resa necessaria un'analisi delle prospettive nazionali e del ruolo assunto dai principali paesi europei rispetto alla creazione della difesa europea. Oltre al ruolo decisivo degli stati, una valutazione particolare merita la figura dell'Alto Rappresentante per la politica estera e di sicurezza, nonché il rapporto tra Unione europea e NATO, con particolare riferimento alle problematiche che hanno contraddistinto la cooperazione tra le due Organizzazioni. Nonostante le criticità presenti nel settore della difesa europea, un notevole passo avanti è stato compiuto attraverso l'istituzione della Cooperazione Strutturata Permanente. In questo contesto, è di cruciale importanza analizzare sia il processo decisionale che ha portato alla nascita della PESCO, sia i principali aspetti istituzionali e le motivazioni che ne hanno favorito lo sviluppo. Un ruolo decisivo è stato svolto da Francia e Germania, che rappresentano i maggiori promotori dell'iniziativa. I due paesi, nonostante le differenti posizioni di partenza, hanno raggiunto, a seguito di una lunga concertazione, una sintesi efficace dei loro obiettivi. Più controversa risulta la posizione assunta dagli altri stati europei, e, in particolare, dagli stati dell'est Europa, da sempre scettici rispetto al processo di integrazione europea in materia di difesa, ma che, nonostante questo, hanno aderito all'iniziativa. L'Unione europea rimane un'entità ibrida, caratterizzata da una commistione di elementi intergovernativi e sovranisti, la cui proiezione esterna si traduce in un'ampia

gamma di politiche e strumenti di soft e hard power. Nel corso degli anni, l'Ue si è affermata come attore di sicurezza a livello internazionale, utilizzando i mezzi tipici di una potenza "civile". Più recentemente, ed in particolare dopo la definizione della Politica europea di sicurezza e difesa (PESD), l'Unione si è progressivamente dotata di strutture e mezzi militari di difesa, inaugurando una nuova fase "operativa" della sua presenza nel contesto di sicurezza globale. Il quadro europeo è parzialmente cambiato con l'adozione della PESCO che rappresenta un primo passo per ripensare la politica di difesa all'interno dell'architettura europea. Questo progetto ha aperto grandi aspettative circa la possibilità di creare un sistema di sicurezza europeo più efficiente, fermo restando che l'istituzione della Cooperazione Strutturata Permanente non ha come obiettivo la creazione di un sistema militare unificato, né tantomeno, la creazione di un esercito europeo. Si tratta comunque di un impegno notevole che cerca di dare maggiore omogeneità a scelte finora incomprensibilmente divisorie tra i partner. Attualmente, nel quadro della PESCO sono stati sviluppati 60 progetti che coprono vari settori: strutture di formazione, sistemi di formazione terrestre, servizi di intelligence, sorveglianza e riconoscimento (ISR), sistemi marittimi avanzati, sistemi aerei a pilotaggio remoto (drone europeo), trasporto aereo strategico, cyberdifesa, servizi multipli congiunti di sostegno e infrastrutture spaziali. La decisione relativa ad un elenco iniziale di 17 progetti è stata adottata il 6 marzo 2018 e uno di questi è stato poi chiuso nel 2020. Successivamente, il Consiglio ha adottato un secondo gruppo di progetti il 19 novembre 2018 e il 12 novembre 2019. I progressi fatti nell'ambito della sicurezza, per quanto encomiabili, non sono sufficienti a superare le criticità che ancora permangono all'interno dell'Unione. In particolare, l'assenza di una visione strategica condivisa degli stati membri ha creato grossi problemi nella definizione di un indirizzo politico univoco per la gestione delle crisi internazionali. Al contempo, i limiti operativi delle forze militari hanno reso difficile il controllo delle (modeste) risorse militari messe a disposizione dagli stati membri. Infine, vi è da considerare che il trasferimento di sovranità in materia di difesa, da sempre osteggiato dagli stati comunitari, ha reso il processo integrativo molto più complicato che in altri settori. Gli ambiti affrontati dalla ricerca evidenziano un punto cruciale costituito dalla divergenza che molti Paesi hanno su molteplici aspetti. Queste difficoltà sembrano destinate a rimanere immutate nel prossimo

futuro, lasciando la politica di sicurezza e difesa in un limbo ancora non definito. Su piani diversi ma che spesso si intersecano, scorre la tematica dell'intelligence europea, ancor di più astratta, complessa e di difficile collocazione. La nozione di intelligence sharing per certi versi sembra quasi incomprensibile, rappresentando per taluni, quasi un ossimoro. Le attività di intelligence sono tradizionalmente pensate per essere al centro della sicurezza nazionale e dei prerequisiti per una sfera di sovranità alla quale difficilmente si pongono delle deroghe. Gran parte della cooperazione in materia di intelligence avviene su base bilaterale, anche se non mancano elementi che portano a una cooperazione multilaterale e ciò che può apparire un compromesso alle citate visioni, in realtà può essere spiegato dal fatto che così facendo si ha la possibilità di ottenere più informazioni e guadagni politici riducendo al minimo i costi in termini di autonomia e di maggiore vulnerabilità.

OBIETTIVO DELLA TESI

Il punto di partenza è quello di accertare quali siano i passi finora fatti nel campo della Difesa Europea, se le politiche di Difesa siano state in grado di assolvere ai compiti che inizialmente le sono state affidate ma soprattutto se gli sforzi fatti in questi lunghi anni siano funzionali a un progetto unitario molto spesso invocato. Nonostante l'evoluzione cronologica abbia imposto nuove e diverse sigle e siano subentrati nuovi e diversi profili giuridico-istituzionali all'interno dell'UE, il dato oggettivo è costituito dal livello di capacità di difesa raggiunto in questi anni, sicuramente molto alto, proprio grazie al comune sforzo politico, economico e di tecnologia messi a disposizione da tutti, che ha di fatto superato i numerosi limiti che i singoli paesi avevano e continuano ad avere in certi settori. Si tratta di uno sforzo comune di portata storica, che continua ad essere espresso migliorando le capacità di difesa, razionalizzando risorse umane ed economiche dei singoli, dettando le principali priorità e i passi successivi per adeguare lo strumento ai tempi. Tuttavia, non è possibile ipotizzare una Difesa europea se non si dispone di una struttura unitaria di intelligence, attualmente surrogata da una serie di centri ed organizzazioni che tentano di svolgere quella *mission* essenziale per la prevenzione delle minacce agli interessi comunitari. Il più importante di questi è il centro di analisi INTCEN¹ con sede a Bruxelles, che trova la sua genesi nella politica di sicurezza e di difesa europea del 1999, ma è successivamente ai fatti dell'11 settembre 2001 che l'allora Alto Rappresentante UE decise di dare al Centro di Situazione Congiunto (o *Joint Situation Centre*) una connotazione tipica da dipartimento di analisi con scambi di informazioni classificate e non, tra le diverse strutture preposte nei vari Paesi.² Ulteriori incrementi alle attività vennero apportate negli anni successivi con l'istituzione di altri Dipartimenti e Centri, tutti dipendenti dal SEAE che hanno ampliato la sfera di analisi anche nei settori delle minacce ibride e nell'analisi dei dati satellitari. È questo il secondo degli ambiti affrontati in questa ricerca, svolta nel settore dell'intelligence e più precisamente nell'intelligence sharing ovvero nell'approccio sempre esistito ma incrementato negli ultimi, tendente allo scambio informativo seppure tale prassi sia solitamente legata a singole situazioni o risulti essere meglio apprezzata per singoli contesti

¹ EEAS website, https://www.eeas.europa.eu/_en

² <https://www.statewatch.org/media/documents/news/2009/aug/SitCen2009.pdf>

(prevenzione criminalità attività, oppure nell'azione di contrasto al terrorismo). Fino a che punto però i singoli Paesi siano disponibili a condividere le proprie informazioni classificate, resta comunque un problema di non facile soluzione: lo scambio di informazioni classificate nell'intelligence spesso può contrastare con l'esigenza di proteggere i propri interessi strategici. La condivisione di intelligence meglio nota come *intelligence sharing* procede verso una nuova direttrice; difficoltà a vari livelli e criticità spesso rilevati potrebbero far desistere dal proseguire in uno sforzo sicuramente complesso. L'obiettivo finale è quello di stabilire se i due ambiti (Difesa/Intelligence) procedano nella prospettiva di un adeguamento ai tempi e alle emergenze in atto, al di là delle ritrosie dei singoli paesi e se l'elemento derivante da una condivisione dell'intelligence, possa costituire la chiave di volta per una maggiore coesione e una visione della sicurezza scevra da campanilismi dannosi, pur nel rispetto delle logiche derivanti dai principi di sovranità nazionale. Il dato certo è che l'auspicata condivisione può rilevarsi determinante: una più efficace collaborazione in questi settori strategici si tradurrebbe in maggiori vantaggi per i singoli Paesi e consentirebbe all'UE di presentarsi nell'arena globale quale attore di un piano ben più elevato di quello attuale. È doveroso sottolineare che la presente attività di ricerca ha quale suo ultimo periodo esaminato quello immediatamente antecedente al 24 febbraio 2022, data che coincide con un conflitto, tutt'ora in corso, che ha ovviamente determinato mutamenti e scelte differenti nei settori oggetto della ricerca. La ricerca, focalizzata sulla fase storica che precede la data indicata, punta a evidenziare un dato concreto, ovvero che all'interno della PSDC vi sia ampio spazio non soltanto per azioni nuove in materia di sviluppo congiunto di capacità di difesa, ma anche per iniziative significative volte a determinare una maggiore coesione delle politiche diversificate di difesa (adozione di sistemi d'arma compatibili, sviluppo di procedure in termini di cybersicurezza, adozione di standard di livello organizzativo e operativo comuni, scelta di strategie condivise). Parallelamente è innegabile che Paesi come Francia e Germania mentre dialogano e si adoperino per portare avanti uno o più progetti in tal senso, procedono parallelamente su iniziative bilaterali o multilaterali che automaticamente ricreano una differenziazione progettuale, strutturale, economica e finanziaria.

MATERIALI E METODI

L'ambito di ricerca è stato affrontato attraverso uno studio dei processi di governance e dei rapporti di collaborazione, sia in prospettiva storica e comparata e sia in relazione alle recenti evoluzioni, con riferimento ai differenti interessi geopolitici e al disallineamento (qualche volta efficacemente rimodulato da comuni necessità, altre volte decisamente voluto), che alcuni dei paesi membri operano, tra interessi di sovranità e esigenze globali. Lo studio nella sua prima parte ha riguardato l'approfondimento di fonti aperte "open source"; successivamente è stato svolto un accurato esame sulle strutture esistenti nei comparti "difesa" e "intelligence" attraverso l'analisi di documentazione su fonti primarie costituite da documentazione governative declassificate (archivi USA e UE). Altro materiale di ricerca è stato reperito in archivi di centri studi e di ricerca, quali il Centro Studi Internazionali Roma (Ce.S.I. Italia) centro di analisi geopolitiche. Analoga ricerca è stata eseguita in archivi istituzionali esteri quali l'Università di Oxford, ricerca consentita attraverso l'affiliazione al circuito studentesco OUSSG (Oxford University Strategic Studies Group), e nell'ambito della quale è stato possibile seguire conferenze e riunioni sulle tematiche oggetto di ricerca, riservate in esclusiva ai membri del College e dell'OUSSG citato. Il progetto è stato arricchito da interviste scritte, richieste e ottenute da professionisti dei settori trattati che, in esclusiva, hanno acconsentito a rispondere a domande vertenti sulle tematiche oggetto della ricerca, fornendo in tal modo un qualificato contributo, come da annessi allegati. In particolare sono stati intervistati:

- Generale di Divisione Massimo Mingiardi, già Mission Commander missione EUTM Somalia 2014/2015 (con riferimento alle missioni UE coordinate dal SEAE e con il coinvolgimento delle strutture della Difesa Comune);
- S. E. Amb. Dott. Giampiero Massolo, già Direttore del Dipartimento delle Informazioni per la Sicurezza (DIS), relativamente all'intelligence, alle nuove minacce e alla possibilità di una visione comune in ambito UE;
- Prof. Cesare La Mantia, Professore associato presso l'Università degli Studi di Trieste; docente Storia dell'Europa orientale e Storia della politica estera

russa contemporanea (relativamente alla Politica di Sicurezza e Difesa UE, rapporti NATO-UE e relazioni internazionali).

Alcuni approfondimenti collegati alla presente ricerca hanno trovato spazio, sulla rivista Brainfactor, testata giornalistica scientifica italiana in elenco Anvur valida per l'abilitazione scientifica nazionale del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR), costituendo così singole pubblicazioni scientifiche. Si tratta di specifici approfondimenti su intelligence sharing, new capabilities in warfare, aspetti di infowar e psyops, nonché di guerra cognitiva. Altri invece, faranno parte di una monografia di prossima pubblicazione, incentrata sulle forme ibride/asimmetriche dei nuovi conflitti e sulle strategie di cyber difesa internazionali. Nel complesso, il processo di analisi utilizzato si è sviluppato attraverso un utilizzo sistemico delle informazioni disponibili, contestualizzate nel periodo di riferimento, connesse alle esigenze strategiche dei vari attori internazionali e avuto riguardo alle diverse prospettive egemoniche degli stessi. L'elaborazione analitica è stata altresì integrata in parte da una conoscenza empirica derivante da esperienze maturate in ambiti connessi a quelli individuati dalla ricerca e, parallelamente, da una conoscenza dei processi cognitivi, con particolare riguardo ai bias cognitivi³ che, nel determinare mutevoli errori, possono compromettere l'intero processo di analisi affrontato.⁴

³ I bias cognitivi sono automatismi mentali dai quali si generano credenze e da cui si traggono decisioni veloci. Si tratta, il più delle volte di errori di giudizio che impattano, nella quotidianità, non solo su decisioni e comportamenti ma anche sui processi di pensiero.

⁴ Lucania P.: *"The Use of Artificial Intelligence to Combating Disinformation"*, in Beyond Fake News – Governments, Press and Disinformation through International History, Franco Angeli Editore, EAN-9788835121794 ISBN-8835121795, pagg. 145-162 – dicembre 2021)

CRONOLOGIA DI INTERESSE

La Politica di sicurezza e di difesa comune: cronologia significativa

Prima fase: dal 1947 al 1960

marzo 1947, Trattato di Dunkerque. Il patto siglato da Francia e Regno Unito consiste in un accordo di alleanza e mutua assistenza contro un eventuale attacco da parte della Germania.

marzo 1948, Trattato di Bruxelles. L'accordo di autodifesa collettiva viene firmato da Francia, Regno Unito, Belgio, Paesi Bassi e Lussemburgo.

maggio 1952, Trattato che istituisce la Comunità europea di difesa (CED). proposto da Francia, Germania, Italia, Belgio, Paesi Bassi e Lussemburgo sulla scorta del Piano Pleven, prevede la creazione di un esercito europeo formato da sei divisioni, collegato al North Atlantic Treaty Organization (Nato) e gestito da un ministro della difesa europeo. L'accordo crea inoltre delle istituzioni simili a quelle della Comunità europea per il carbone e l'acciaio (Ceca).

agosto 1954, bocciatura del Trattato che istituisce la Comunità europea di difesa. Il testo del trattato non entra in vigore perché non ratificato dall'Assemblea Francese.

23 ottobre 1954, creazione dell'Unione dell'Europa occidentale (UEO). In seguito al fallimento della CED, gli atti internazionali che modificano il Trattato di Bruxelles del marzo 1948 danno vita ad un'organizzazione internazionale regionale di sicurezza militare e cooperazione politica della quale sono pertanto membri Francia, Regno Unito, Belgio, Paesi Bassi e Lussemburgo, ai quali si aggiungono anche l'Italia e la Germania.

25 marzo 1957, Trattato istitutivo della Comunità economica europea (Cee). Firmato a Roma da Belgio, Francia, Germania, Italia, Lussemburgo e Paesi Bassi, il trattato istituisce una Comunità con l'obiettivo dell'integrazione economica e la dota di strutture istituzionali proprie.

Luglio 1970, Cooperazione politica europea (CPE). Nelle intenzioni del rapporto Davignon, approvato a Lussemburgo dalla Conferenza dei ministri degli Esteri degli stati membri, la CPE "consente agli stati membri della Comunità europea di discutere e coordinare le loro posizioni sugli affari esteri e, ove appropriato, agire di concerto".

Seconda fase: inizia a costituirsi un fronte di Paesi che intendono consultarsi per il contrasto alle principali insidie sulla sicurezza e per la partecipazione ad interventi in aree sensibili.

febbraio 1986, Atto unico europeo (AUE). L'Atto unico istituzionalizza il coordinamento politico prevedendo la consultazione sistematica tra gli stati membri in merito alle questioni afferenti alla politica estera. Nel suo ambito gli stati membri devono tenere conto del punto di vista del Parlamento europeo e difendere, nei limiti del possibile, le posizioni comuni in seno alle organizzazioni internazionali.

7 febbraio 1992, Trattato sull'Unione europea (TUE). Firmato a Maastricht, trasforma la CPE nella **Politica estera e di sicurezza comune (PESC)** conservandone il carattere intergovernativo ed introduce strumenti normativi quali azioni comuni e posizioni comuni. Prevede il futuro sviluppo di una politica di difesa comune e richiede "all'UEO di elaborare e di porre in essere le decisioni e le azioni dell'Unione aventi implicazioni nel settore della difesa".

giugno 1992, Dichiarazione di Petersberg. Il Consiglio dei ministri dell'UEO, riunitosi a Petersberg, presso Bonn, definisce le "Missioni di Petersberg" e decide di mettere a disposizione dell'UE e della Nato unità militari provenienti dalle forze armate degli stati membri.

giugno 1996, Vertice della Nato a Berlino. La Nato decide di sviluppare un'Identità europea in materia di sicurezza e difesa (European Security and Defence Identity, Esdi) che consente ad ufficiali europei della Nato di occupare in parallelo posizioni di comando nella struttura dell'UEO. Viene inoltre deciso che le strutture e i mezzi della Nato siano disponibili per future missioni militari dirette dall'UEO.

2 ottobre 1997, Trattato di Amsterdam. Il trattato incorpora le Missioni di Petersberg dell'UEO, crea la figura dell'Alto rappresentante per la PESC, attribuendone le funzioni al segretario generale del Consiglio ed introduce un altro strumento normativo, le strategie comuni. Inoltre, al fine di temperare la rigidità del metodo di adozione delle decisioni per consenso, il trattato introduce "l'astensione costruttiva", uno strumento che consente ad uno stato membro di astenersi dal partecipare ad un'iniziativa comune nel settore della PESC senza impedire agli altri stati membri di portarla avanti. La Danimarca ricorre alla

clausola dell'opting-out al fine di non partecipare alle iniziative aventi implicazioni militari e/o nel settore della difesa.

Dicembre 1998, Vertice franco-britannico di Saint-Malo. Considerato il vero e proprio punto di partenza dell'allora **Politica europea di sicurezza e di difesa (PESD)**, sancisce su iniziativa del presidente della Repubblica francese Jacques Chirac e del primo ministro britannico Tony Blair la volontà dell'Unione europea di dotarsi di una "capacità autonoma di azione, basata su forze militari credibili" per permettere all'Unione europea di rispondere alle crisi internazionali.

Terza fase: si apre il decennio di coordinamento da parte di Javier SOLANA; nuove prospettive e nuovo ruolo internazionale

aprile 1999, Vertice Nato a Washington. In occasione dell'incontro per il cinquantesimo anniversario della Nato, i capi di stato adottano un nuovo concetto strategico ed un'iniziativa per promuovere le capacità militari. Si dichiarano inoltre disposti a sostenere le missioni dell'Unione europea e ribadiscono il principio delle "forze separabili, ma non separate", già enunciato nel Consiglio di Berlino del 1996.

giugno 1999, Consiglio europeo di Colonia. La **PESD** viene ufficialmente istituita. Javier Solana viene nominato Segretario generale/Alto rappresentante per la PESC (Sg/Ar) ed inoltre viene sancito il trasferimento di alcune competenze dell'UEO all'Unione europea. Una volta ultimato tale processo, "l'UEO avrà concluso la sua missione in quanto organizzazione".

dicembre 1999, Consiglio europeo di Helsinki. Oltre alla formulazione dell'Helsinki Headline Goal il Consiglio europeo giunge ad un'intesa sulle modalità di una cooperazione completa tra l'Unione europea e la Nato e sulle condizioni di consultazione con i paesi candidati all'adesione all'Ue, i paesi europei non membri della Nato ed i partners dell'UEO. Vengono create nuove strutture *ad interim*: il Comitato politico e di sicurezza interinale (Comité politique et de sécurité intérimaire, Copsi), il Comitato militare interinale dell'Unione europea (European Union Military Committee, Eumc) e lo Stato maggiore interinale dell'Ue (EU Military Staff, Eums).

giugno 2000, Consiglio europeo di Santa Maria da Feira. I capi di stato e di governo decidono di istituire quattro comitati *ad hoc* Ue/Nato su: sicurezza e obiettivi di capacità; modalità di utilizzo dei mezzi della Nato; meccanismi permanenti di consultazione. Essi definiscono inoltre il Civilian Headline Goal.

novembre 2000, Consiglio UEO di Marsiglia. Il Consiglio sancisce il processo di trasferimento delle capacità dell'organizzazione UEO relative alla gestione delle Missioni di Petersberg (gestione delle crisi) all'Unione europea. La UEO resta operativa per funzioni residuali relative alla clausola di difesa collettiva (Art. V del Trattato di Bruxelles modificato) e all'attività dell'Assemblea parlamentare UEO (Art. IX).

26 febbraio 2001, Trattato di Nizza. Il trattato introduce nuove strutture politiche e militari, rende permanenti quelle già esistenti ed estende il metodo delle "cooperazioni rafforzate" alla PESC, pur escludendo dal loro campo di applicazione le questioni aventi implicazioni militari o nel settore della difesa.

dicembre 2001, Consiglio europeo di Laeken. La PESD viene dichiarata parzialmente operativa.

marzo 2002, Azione comune del Consiglio Affari generali e relazioni esterne (Cagre) sulla missione di polizia dell'Unione europea in Bosnia Erzegovina (European Union Police Mission, Eupm). Con la prima missione PESD, l'Ue si impegna ad assumere dal 31 dicembre 2002 il comando della forza di polizia internazionale operante in Bosnia Erzegovina sotto l'autorità dell'Organizzazione delle Nazioni Unite (Onu). Si tratta dunque di un'operazione civile il cui organico conta inizialmente 531 funzionari di polizia e 400 civili.

giugno 2002, Consiglio europeo di Siviglia. Gli obiettivi della PESD vengono ampliati per includere la lotta al terrorismo.

dicembre 2002, Dichiarazione comune Ue-Nato sulla PESD. Superata l'impasse dovuta all'opposizione della Turchia, l'Unione europea e la Nato ufficializzano il raggiungimento degli accordi denominati "Berlin Plus", che consentono all'Unione di avere accesso ai mezzi della Nato per la gestione delle crisi, mentre da parte sua l'Unione accetta di integrare al massimo nell'ambito della PESD i paesi non europei della Nato.

gennaio 2003, Azione comune del Cagre sulla missione Concordia nell'Ex Repubblica jugoslava di Macedonia. I ministri degli Esteri degli stati membri

dell'Ue approvano la prima operazione militare europea. Si tratta inoltre della prima missione che utilizza le strutture e mezzi della Nato sulla base degli accordi "Berlin plus". Il personale in organico raggiunge inizialmente le 350 unità.

giugno 2003, Azione comune del Cagre sull'operazione Artemis nella Repubblica democratica del Congo. Il Cagre lancia la prima operazione militare dell'Unione europea realizzata senza utilizzare i mezzi della Nato nonché la prima al di fuori del continente europeo. Con i suoi 1.800 militari, l'operazione si prefigge l'obiettivo del ristabilimento delle condizioni di sicurezza nella città di Bunia, capitale della provincia d'Ituri.

settembre 2003, Dichiarazione congiunta sulla cooperazione tra le Nazioni Unite e l'Ue nell'ambito della gestione delle crisi. Le Nazioni Unite e l'Unione europea firmano una dichiarazione in base alla quale si impegnano a migliorare il coordinamento delle attività di pianificazione, addestramento, comunicazione e buone pratiche nell'ambito della gestione delle situazioni di crisi.

dicembre 2003, Strategia europea in materia di sicurezza (European Security Strategy, Ess). Il Consiglio europeo di Bruxelles adotta la versione finale della Ess, proposta dall'allora Alto rappresentante per la PESC, Javier Solana, "Un'Europa sicura in un mondo migliore".

luglio 2004, Agenzia europea per la difesa (European Defence Agency, Eda). Il Consiglio dell'Unione europea affida alla neo-istituita agenzia un ruolo di supporto agli stati membri e al Consiglio nel miglioramento delle capacità di difesa europee e nel sostegno alla politica europea di sicurezza e di difesa.

maggio 2005, Azione comune del Cagre sulla missione Eusec Rd Congo nella Repubblica democratica del Congo. L'Unione europea lancia la sua prima missione civile-militare. L'obiettivo dei 46 esperti civili e militari dello staff è quello di svolgere attività di consulenza e di assistenza all'amministrazione congolese in merito alla riforma del settore della sicurezza.

dicembre 2007, Mercato europeo della difesa: "pacchetto difesa". La Commissione europea adotta un insieme di misure noto come "pacchetto difesa", volto ad incrementare la competitività del settore industriale della difesa limitando i casi di applicabilità dell'art. 296 del Trattato Ce - che permette l'esenzione dalle regole del mercato comune, per interessi essenziali alla sicurezza nazionale - fornendo un regime alternativo che tenga conto delle specificità del

comparto. L'iniziativa comprende due proposte di direttiva - sugli appalti pubblici della difesa (beni e servizi), e sulla semplificazione dei trasferimenti intra-comunitari di attrezzature e materiali militari - ed una comunicazione sul rafforzamento della competitività del mercato e l'industria della difesa.

dicembre 2008, Azione comune del Cagre sulla missione Eu Navfor Somalia. Il Consiglio approva la prima missione militare navale dell'Unione europea, l'operazione Eu Navfor Somalia (Operazione Atalanta), dispiegata al largo delle coste somale per scortare i convogli umanitari del Programma alimentare mondiale (Pam) proteggendoli da attacchi di pirateria e contribuire alle attività di deterrenza, prevenzione e repressione della pirateria somale nella regione.

dicembre 2008, Relazione sull'attuazione della Strategia di sicurezza europea del 2003. Stilato da Solana, allora Alto rappresentante per la PESC, il rapporto aggiorna la Ess sulle priorità per la politica di sicurezza dell'Unione. Vengono quindi incluse la sicurezza informatica, la sicurezza energetica e l'impatto dei cambiamenti climatici tra le nuove aree di intervento, come pure la, pirateria, la diffusione di armi leggere e di piccolo calibro quali rischi crescenti per la sicurezza internazionale e dell'Ue.

Quarta fase: si inaugura la figura dell'Alto Rappresentante per la Politica Estera e la Difesa Comune: Javier SOLANA (fino al 2009), Chaterine ASTHON (fino al 2014) e Federica MOGHERINI (fino al 2019).

1 dicembre 2009, entra in vigore il Trattato di Lisbona. All'insegna di una maggiore coerenza nell'azione esterna dell'Unione, il trattato introduce significativi cambiamenti anche in tema di sicurezza e difesa comune. Tra questi, il superamento formale della struttura a pilastri dell'Ue, con l'Alto rappresentante che riunisce in sé anche le funzioni di vicepresidente della Commissione e Commissario delle relazioni esterne; la scomparsa di qualsiasi limitazione di difesa alle cooperazioni rafforzate; l'introduzione della cooperazione strutturata permanente (che pone le basi per un'Europa a più velocità in materia di difesa); l'istituzionalizzazione dell'Agenzia europea per la difesa, etc.. Il Trattato dota inoltre l'Ue di una singola personalità giuridica.

febbraio 2010, Strategia per la sicurezza interna dell'Ue: Ess. Approvata dal Consiglio Giustizia e affari interni, e complementare alla Ess, la strategia individua

cinque “obiettivi strategici” che richiedono una maggiore cooperazione tra gli stati membri Ue per rafforzare la sicurezza del continente: smantellare le reti criminali internazionali; prevenire il terrorismo e contrastarne la radicalizzazione e il reclutamento; aumentare i livelli di sicurezza nel cyberspace; migliorare la gestione delle frontiere; aumentare la resilienza europea alle crisi e alle calamità naturali.

luglio 2010, Decisione del Consiglio istituisce il Servizio europeo di azione esterna, Seae. Il Consiglio Affari generali dell’Ue istituisce il SEAE quale struttura di supporto per l’operato del VP/AR per gli affari esteri e la politica di sicurezza. Risulta composto da funzionari del Consiglio, della Commissione e dei corpi diplomatici nazionali. Diventa operativo il 1 gennaio 2011.

novembre 2010, Accordi franco-britannici per la cooperazione in materia di difesa. Francia e Regno Unito firmano accordi per la cooperazione bilaterale nel settore della difesa che prevedono: la condivisione delle rispettive portaerei; la progressiva formazione di una forza militare “expeditionary” congiunta di circa 5.000 uomini; la collaborazione nella gestione dei rispettivi apparati di deterrenza nucleare e la cooperazione su diversi programmi di acquisizione e sviluppo capacità militari.

23 marzo 2012, Decisione del Consiglio dell’Unione europea per l’attivazione dell’EU Operations Centre nel Corno d’Africa. Per la prima volta dalla sua creazione (2007), l’Ops Centre ha il compito di coordinare tre missioni Psdc nella regione: Eu Navfor Atalanta a contrasto della pirateria nel Golfo di Aden; Eutm Somalia per l’addestramento delle forze di sicurezza somale, e la prossima missione civile Regional Maritime Capacity Building (Rmcb) per il rafforzamento delle capacità marittime delle forze di sicurezza degli stati della regione.

dicembre 2013, riconoscendo la necessità di fornire un impulso strategico ai capi di Stato e di governo, il Consiglio europeo ha fissato una serie di obiettivi iniziali per far progredire la PSDC, ovvero aumentare l’efficacia e l’impatto della PSDC, potenziare lo sviluppo delle capacità di difesa e rafforzare l’industria europea della difesa. Inoltre ha incaricato il VP/AR e la Commissione di valutare l’impatto dei cambiamenti nel contesto globale dell’UE.

giugno 2015, a conclusione del percorso di valutazione del 2013, nel giugno 2015, il VP/AR è stato incaricato di elaborare una «strategia globale per la politica estera

e di sicurezza dell'Unione europea» (EUGS) per il 2016, che il VP/AR, Federica Mogherini, ha presentato al Consiglio europeo nel giugno 2016. Tale strategia individua cinque priorità per la politica estera dell'UE: la sicurezza dell'Unione; la resilienza degli Stati e della società a est e a sud dell'UE; lo sviluppo di un approccio integrato ai conflitti; gli ordini regionali cooperativi; e la governance globale per il XXI secolo. Nel mese di luglio 2016 gli Stati membri hanno accolto con favore la strategia globale per la politica estera e di sicurezza dell'Unione europea e hanno deciso di passare alla fase di attuazione.

16 settembre 2016, a Bratislava, gli Stati membri dell'UE hanno ribadito il loro proposito di rafforzare la cooperazione dell'UE nell'ambito della sicurezza esterna e della difesa. Nel novembre 2016 è stato presentato al Consiglio il «Piano di attuazione in materia di sicurezza e difesa», volto a rendere operativa la visione definita nell'EUGS per quanto concerne le questioni in materia di difesa e sicurezza. Il piano stabilisce 13 proposte, tra cui una revisione annuale coordinata in materia di difesa (CARD), con particolare riferimento alla spesa; una migliore risposta rapida dell'UE anche mediante il ricorso ai gruppi tattici dell'UE; e una nuova disposizione unica per ciò che riguarda la cooperazione strutturata permanente (PESCO) per gli Stati membri che intendono assumere maggiori impegni in materia di sicurezza e difesa. Il 30 novembre 2016 il VP/AR Mogherini ha presentato agli Stati membri dell'UE il «Piano d'azione europeo in materia di difesa», unitamente a proposte chiave relative al Fondo europeo per la difesa, incentrando l'attenzione sulla ricerca e sullo sviluppo di capacità nel settore della difesa. Il Consiglio ha inoltre adottato conclusioni che approvano un piano per applicare le decisioni sulla cooperazione UE-NATO adottate a Varsavia (42 proposte).

2017 e 2018: anni cruciali per l'attuazione della PSDC Nel marzo 2017 il Consiglio europeo ha riesaminato i progressi e ha sottolineato l'istituzione della capacità militare di pianificazione e condotta (MPCC), una nuova struttura per migliorare la capacità dell'UE di reagire in maniera più rapida, efficace e omogenea ai fini della pianificazione e della condotta di missioni militari senza compiti esecutivi. Inoltre ha preso atto dei progressi compiuti in altri settori. Nel dicembre 2018 i leader dell'UE hanno inoltre riconosciuto i progressi realizzati nel settore della sicurezza e della difesa, sottolineando l'evoluzione della PESCO, della mobilità militare e del

patto sulla dimensione civile della PSDC. Il 7 giugno 2017 la Commissione ha presentato una comunicazione intitolata «Istituzione del Fondo europeo per la difesa», che delinea le proposte volte a stimolare e a strutturare gli investimenti nel settore della difesa nell'UE. Essa ha proposto un sostegno diretto a favore della ricerca, il cofinanziamento dello sviluppo di prodotti per la difesa e il sostegno per il loro acquisto da parte degli Stati membri dell'UE. Il sostegno al settore è inoltre evidenziato nel progetto di regolamento relativo a un programma europeo di sviluppo del settore industriale della difesa (EDIDP).

Fase più recente: Joseph Borrel e Fontelles, Alto rappresentante UE dal 1 dicembre 2019

giugno 2020, Incarico del Consiglio dell'Unione Europea. In questa data si è convenuto di avviare l'elaborazione della "bussola strategica" (Strategic Compass) per tradurre in orientamenti strategici più concreti il livello di ambizione in materia di sicurezza e di difesa concordato nel 2016.

novembre 2022, Prima analisi Europea delle Minacce. Il primo passo nell'elaborazione della "bussola strategica" è quello di fornire un'analisi completa e indipendente a 360°, basata sull'intelligence dell'intera gamma di minacce.

prima metà del 2021, Dialoghi strategici con i Paesi membri. Per l'adozione della bussola strategica l'UE ha dovuto superare i dialoghi strategici con i Paesi membri e le istituzioni, compreso il coinvolgimento di gruppi di studio e riflessione. Il dialogo è stato mirato a chiedere ai Paesi membri di valutare i loro principali bisogni, le principali implicazioni dell'analisi delle minacce e le linee guida politiche, pertinenti le rispettive priorità

seconda metà del 2021, Sviluppo della bussola strategica. Nell'impostazione iniziale e nella sua prima versione, affronta quattro aree diverse ma interconnesse: *"crisis management mission; capabilities; resilience; partnership"*.

21 marzo 2022, Adozione della bussola strategica. I quattro pilastri approvati sono: *action; investment; partner and security*. Fornisce all'UE uno strumento per poter rafforzare la Politica di Sicurezza e Difesa entro il 2030, rendendola garante della Sicurezza, più forte e capace.

Capitolo 1. La Politica di Sicurezza e Difesa dell'Unione Europea

1.1 Le origini

1.1.1 Le esigenze di sicurezza e il Trattato di Bruxelles

Alla fine della seconda guerra mondiale, l'espansionismo dell'Unione Sovietica progressivamente affermatosi in Europa Centrale e nel resto del mondo, cominciò a esercitare una notevole apprensione sia per gli Stati Uniti e sia per gli stessi Paesi europei. Il Vecchio Continente si presentava come un territorio distrutto e diviso, profondamente segnato da sei anni di conflitto: una parte di esso fu liberata dagli Stati Uniti e dai suoi alleati, la restante parte fu liberata dall'Unione Sovietica. Gli Stati Uniti comunque non volevano ripetere lo stesso errore commesso dalla Francia nei confronti della Germania successivamente alla Prima Guerra Mondiale e si attivarono sin dalle prime fasi affinché questo non avvenisse. Una prima risposta a questa situazione venne determinata da una serie di trattati e tra questi, merita di essere ricordato il Trattato di Bruxelles, firmato il 17 marzo 1948 da Belgio, Francia, Lussemburgo, Paesi Bassi e Regno Unito⁵. Si trattava di un trattato di collaborazione economica, sociale e culturale improntato sul principio dell'autodifesa, entrato in vigore il 25 agosto successivo, con lo scopo principale di voler riaffermare la fede nei diritti umani fondamentali, fortificare e preservare i principi della democrazia e di cooperare e coordinare gli sforzi per creare nell'Europa occidentale una solida base per la ripresa economica europea. L'articolo II prevedeva che le parti contraenti avrebbero fatto ogni sforzo per promuovere il raggiungimento di un tenore di vita più elevato da parte dei propri popoli e di sviluppo corrispondente alle linee sociali. In conformità alle disposizioni

⁵ Source: Western European Union – Union de l'Europe Occidentale. (en ligne). (Bruxelles): Unione de l'Europe occidentale (06.10.2000). Disponible sur <http://www.weu.int/index.html>. Archives nationales du Luxembourg, Luxembourg. <http://anlux.lu/>. Ministère des Affaires étrangères (1732-1998). Ministère des Affaires étrangères – Traités et Conventions. Traité entre la Belgique, la France, le Luxembourg, les Pays-bas et le Royaume Uni de Grande-Bretagne et d'Irlande du Nord – s. à Bruxelles, AE TC 365.

di cui all'art. 51 della Carta delle Nazioni Unite, se una qualsiasi delle parti contraenti fosse stata oggetto di attacco, tutte le altre parti contraenti l'avrebbero sostenuta con tutti i mezzi e il loro aiuto disponibile, a seguito di coordinamento tramite il Consiglio Consultivo. Nessuno di essi inoltre avrebbe potuto far parte di coalizioni o alleanza dirette contro uno solo delle parti contraenti.

Les Hautes Parties Contractantes associeront leurs efforts, par la voie de consultations directes et au sein des Institutions spécialisées, afin d'élever le niveau de vie de leurs peuples et de faire progresser, d'une manière harmonieuse, les activités nationales dans le domaine social. Les Hautes Parties Contractantes se concerteront en vue d'appliquer le plus tôt possible les recommandations d'ordre social, émanant d'Institutions spécialisées, auxquelles Elles ont donné leur approbation au sein de ces Institutions et qui présentent un intérêt pratique immédiat. Elles s'efforceront de conclure entre Elles, aussitôt que possible, des conventions de sécurité sociale.⁶

Per molti aspetti, il Trattato può essere definito quale precursore dell'Alleanza Atlantica ma anche di una organizzazione conosciuta come Unione dell'Europa Occidentale.

1.1.2 Il Trattato Nord Atlantico

La creazione dell'Organizzazione del Trattato del Nord Atlantico il 4 aprile del 1949 fu un ulteriore passo verso una più efficace cooperazione militare tra l'Europa e gli Stati Uniti. Oltre ai cinque Stati firmatari del Trattato di Bruxelles, aderirono anche Canada, Danimarca, Islanda, Italia, Portogallo, Norvegia e Stati Uniti. Il Trattato Nord Atlantico entrò in vigore il 23 agosto 1949 e aprì la strada per la difesa dell'Europa occidentale su base transatlantica; rappresenta tuttora un irrinunciabile strumento di difesa collettiva e di cooperazione militare tra i suoi Stati Membri, nonché un cruciale foro di dialogo politico. Caposaldo dell'Alleanza Atlantica è il principio di difesa collettiva, sancito dall'articolo 5 del Trattato di Washington, in virtù del quale:

⁶ Traité de Bruxelles, du 17 mars 1948, modifié et complété par les protocoles signés à Paris le 23 octobre 1954. https://www.cvce.eu/content/publication/2003/11/26/7d182408-0ff6-432e-b793-0d1065e695/publishable_fr.pdf

“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, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell’esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall’Art. 51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti attaccate, intraprendendo immediatamente, individualmente e di concerto con le altre parti, l’azione che giudicherà necessaria, compreso l’uso delle forze armate, per ristabilire e mantenere la sicurezza nella regione dell’Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali.”

Il 1949 può essere considerato un anno cruciale, non soltanto perché vede la nascita della NATO, ma anche perché vennero predisposte e attuate strategie a lungo termine di rilevante interesse per i futuri assetti geopolitici. In quegli anni, gli Stati Uniti avevano già chiara quale architettura dare a una Germania che doveva essere collocata necessariamente in un ambito europeo ma non eccessivamente autonoma e vincolata con un progetto di unificazione a lunga scadenza, allo scopo di garantire la sicurezza e la stabilità del vecchio Continente. Esemplificativo, in tal senso è un documento del Dipartimento di Stato USA – Ufficio per gli Affari di Germania e Austria, a firma di Henry A. Byroade⁷, Acting Deputy Director, elaborato per l’amministrazione Truman in previsione della Conferenza dei Ministri degli Esteri svoltasi a Parigi dal 23 maggio all’11 giugno

⁷ Henry A. Byroade, soldier and diplomat, was born in Indiana on July 24, 1913. He graduated from the U.S. Military Academy in 1937 and spent most of World War II in the China-Burma India Theater of Operations. After the war he served as attaché to General George Marshall during Marshall’s negotiations between the Communist and Nationalist Chinese forces. In 1949 he was assigned to the Department of State as a foreign policy expert. He resigned from the Army in 1952 when President Truman appointed him Assistant Secretary of State for Near Eastern, South Asian and African Affairs. In 1955 President Eisenhower appointed him Ambassador to Egypt, where he served during the Suez Canal crisis of 1956. He later served as ambassador to the Union of South Africa, Afghanistan, Burma, the Philippines and Pakistan. After retiring from the Department of State in 1977 he worked for two years for a private company in Saudi Arabia, after which he settled in the Washington, DC, area. He died on December 31, 1994. <https://www.eisenhowerlibrary.gov/sites/default/files/finding-aids/pdf/byroade-henry-papers.pdf>

1949 per discutere del futuro della Germania. Il documento, un *memorandum* originariamente “top secret” e successivamente declassificato come da codifica “Authority NND 812009”, riporta la data 25 aprile 1949⁸, evidenzia la preferenza di Washington per una prospettiva della Germania divisa, almeno nel primo periodo e comunque destinata ad una sfera di inclusione tale da poter essere agevolmente integrata con i restanti Paesi dell’Europa occidentale:

“...this does not imply that a reunification of Germany can at no time be tolerated, but it does mean that a united Germany must be held bound by integration in a wider European free community in the same degree that it is intended to absorb western Germany in western Europe.”

Tale integrazione avrebbe dato modo di assecondare dei passaggi di “rinascita” seppure in una veste di “contenimento”, a fronte di una eccessiva e rischiosa libertà di movimento che avrebbe consentito alla stessa di trarre beneficio sia dai sistemi politico-economici dei Paesi limitrofi (in gran parte impostati su direttrici volute dagli U.S.A.) e sia di quelli orientali, provocando uno sviluppo non gradito. Un aspetto di incredibile lungimiranza nella visione geopolitica di Byroade è costituito dalla previsione in base alla quale la Germania prematuramente unificata avrebbe probabilmente assunto una postura variabile o come forte Stato nazionalista o come partner eccessivamente disponibile della Russia sovietica e, in entrambi i casi, avrebbe creato una pressione intollerabile nell’ambito degli accordi di difesa occidentali:

*“...At the worst, Germany would be an uncertain factor either as a strong nationalist state or as a willing partner of Soviet Russia, in either eventuality placing an intolerable strain upon the western defense arrangements”.*⁹

1.1.3 La CECA

Il 18 aprile 1951, a Parigi, i rappresentanti di Belgio, Francia, Italia, Lussemburgo, Paesi Bassi e Germania occidentale/Repubblica Federale di Germania firmarono il trattato per l'istituzione della Comunità Europea del Carbone e dell'Acciaio (CECA).

⁸ Source: National Archives, Records of International Conferences, Record Group 43, Jessup-Malik Agreement, May 1943, box 304, Jessup-Malik Conversations, March, April, May 1949 <https://nsarchive.gwu.edu/document/17547-document-02-henry-byroade-acting-deputy-director>.

⁹ Ivi

La Comunità Europea del Carbone e dell'Acciaio era basata su un mercato comune, comune obiettivi e istituzioni comuni. La sua missione era legata all'espansione economica, lo sviluppo dell'occupazione e il miglioramento del tenore di vita dei paesi partecipanti attraverso l'istituzione, in armonia con l'economia generale degli Stati membri e di un mercato comune. È possibile affermare che per la prima volta, una sola istituzione sovranazionale divenisse responsabile della messa in comune delle risorse europee di carbone e acciaio per il mantenimento della pace in Europa e lo fece attraverso una complessa struttura composta da un'Alta Autorità (precursore dell'attuale Commissione Europea) assistita da un Comitato Consultivo (precursore dell'attuale Comitato economico e sociale europeo), nonché da un Comune Assemblea (precursore del Parlamento Europeo), un Consiglio speciale dei ministri nell'area dell'Europa (precursore del Consiglio Europeo) e infine una Corte di giustizia (precursore della Corte di Giustizia Europea). Il padre fondatore della CECA, Jean Monnet, è stato il primo presidente dell'Alta Autorità (1952-1954). Questa integrazione settoriale era parte di un disegno strategico assai più ampio il cui passo successivo avrebbe dovuto vedere la nascita di una Comunità Europea della Difesa (CED), quale pilastro europeo dell'Alleanza Atlantica, e quindi di una partecipazione della Repubblica Federale Tedesca, ancora non ammessa nella NATO, a capacità militari che la legassero indissolubilmente agli altri paesi europei occidentali di fronte all'URSS e ne impedissero ogni velleità revanscista. Questo disegno strategico fu subito colto dall'Italia come corrispondente al proprio interesse nazionale prioritario di rientrare pienamente e in condizioni di parità nella comunità internazionale dopo la sconfitta e di trarne tutti i vantaggi economici, politici e di sicurezza che ne sarebbero derivati.

1.1.4 La presenza militare nel continente, il Piano Marshall

Altra decisione fondamentale fu quella assunta dagli Stati Uniti circa il mantenimento di una consistente presenza militare nel vecchio continente. Nelle sue fasi iniziali, questa presenza si poneva come garanzia nei confronti della Germania e, in seguito, verso l'URSS, specie dopo l'annuncio della dottrina Truman nel 1947 in relazione alla pressione sovietica esercitata su Grecia e Turchia e stante

le modalità con cui i sovietici imponevano regimi satelliti nei paesi da essi occupati e infine, nel 1948, del colpo di Stato a Praga e del blocco degli accessi a Berlino. Va sottolineato comunque che gli abitanti dei paesi europei, alle prese con l'avvio della ricostruzione post-bellica molto difficilmente avrebbero potuto tollerare la presenza di militari stranieri e, soprattutto, di loro installazioni destinate ad agire anche su un orizzonte temporale esteso. La risposta a queste difficoltà venne individuata dal Gen. Charles Pearre Cabell, membro dell'aeronautica USA all'interno del JCS, il quale espresse la necessità per gli Stati Uniti di avere delle basi in Europa e lo fece all'interno del concetto di "Maintenance Covenant" che individuava la possibilità che i paesi ospitanti potessero essere risarciti dagli Stati Uniti attraverso interventi sul debito di guerra maturato, attraverso assistenza logistico/operativa, sulla fornitura di armamenti e nella ricostruzione dei loro eserciti. L'utilizzo di contropartite, finanziarie ed in dotazioni militari, alla presenza di installazioni militari, non rappresenta tuttavia un'esclusività di questo periodo. Gli accordi per il mantenimento di installazioni militari all'estero si inseriscono, nella maggior parte dei casi, in più ampi programmi di collaborazione che individuano proprio nell'assistenza tecnica e nella formazione i corrispettivi, almeno formalmente, principali.¹⁰ Completarono il quadro un forte impegno americano con il Piano Marshall (*European Recovery Program Act*) per la ricostruzione dell'Europa distrutta dalla guerra, l'avvio di un processo di liberalizzazione degli scambi in ambito monetario e finanziario definito dalle intese di Bretton Woods e l'incoraggiamento alla coesione e alla progressiva integrazione dei paesi dell'Europa occidentale e poi ad uno stretto rapporto tra Francia e Germania. Una particolare iniziativa fu rappresentata dalla citata costituzione della CECA, la Comunità Europea del Carbone e dell'Acciaio con la quale venivano messe in comune, le risorse per le quali e con le quali erano state combattute le guerre che avevano insanguinato l'Europa dall'inizio della rivoluzione industriale. Il piano fu fortemente voluto dal Primo Ministro francese Robert Schumann, dal Cancelliere Konrad Adenauer, e dal Presidente del Consiglio Alcide De Gasperi. Il piano predisposto da Marshall ha una sua complessità, perché racchiude una serie di riforme che avrebbero consentito, in tempi brevi di ristabilire un equilibrio

¹⁰ Paragano D.: Le basi militari degli Stati Uniti in Europa: posizionamento strategico, percorso localizzativo e impatto territoriale. Università degli Studi di Trieste – AA – 2007/2008.

politico favorevole, tanto da inserirsi in un concetto molto più ampio che è quello della Political Warfare ipotizzata da George Kennan e che contraddistinse la politica estera degli USA nel dopoguerra.¹¹

1.2 La CED: il progetto di un esercito europeo

1.2.1 Le origini e le perplessità dei francesi

Sin dall'inizio degli anni Cinquanta, l'Europa occidentale si è confrontata con la minaccia sovietica, in un contesto geopolitico internazionale sempre più problematico. Nel 1950, le truppe comuniste della Corea del Nord (appoggiate anche dall'Unione Sovietica oltre che dalla Cina) entrarono in guerra con il sud del Paese; a questo punto gli Stati Uniti unitamente ad altri 17 Paesi e sotto l'egida dell'ONU, si lanciarono con immediato slancio in questo conflitto inviando truppe e mezzi a sostegno del governo di Seoul. L'ascesa e il riarmo intrapreso da Cina e Russia in particolare, costituì la spinta per gli Stati Uniti ad elaborare strategie ormai inderogabili e dirette a contrastare l'espansione comunista e "combattere per la libertà e la democrazia".¹² L'alleanza Cina – Unione Sovietica, in particolare, cominciava a preoccupare gli Stati Uniti non solo sul versante asiatico ma anche per quanto riguarda lo scacchiere europeo. Ritenevano inoltre che un eventuale attacco sferrato dall'Unione Sovietica ad est del continente europeo, sarebbe stato impossibile da fronteggiare: la nascente Alleanza Atlantica (NATO) non era ancora operativa ma quello che più preoccupava era l'assenza dell'esercito tedesco ormai sconfitto e inesistente, la cui ricostruzione (e di conseguenza il suo riarmo) poneva un notevole problema esistenziale alla Francia che vi si opponeva categoricamente verosimilmente per un'atavica paura di vederla riemergere dalle proprie ceneri e recuperare il pieno potere nel continente. A questi sentimenti di apprensione, se non di paura nei confronti del vecchio nemico, va poi aggiunto il crescente orgoglio da parte di Parigi, di ritrovare al più presto la propria grandezza e le caratteristiche di una potenza mondiale. A questo punto per gli Stati Uniti non

¹¹ Lucania P.: L'attualità della Political Warfare" in Brainfactor – 2021 - <https://www.brainfactor.it/lattualita-della-political-warfare/>

¹² Breccia G.: "Corea, la guerra dimenticata" – Il Mulino – 2019 ISBN-13: 978-8815280145

restava altro che dare vita a una nuova strutturazione politico militare dell'Europa attraverso alcuni passaggi fondamentali. Il primo dei quali fu quello di rendere pienamente operativa la NATO, poi senza tergiversare oltre si pensò a ricostituire (e quindi a riarmare) l'esercito tedesco che avrebbe avuto il compito di portare 12 divisioni all'interno del Patto Atlantico. La proposta U.S.A. fu accolta dalla maggioranza dei 12 ministri degli esteri della NATO e il Cancelliere Konrad Adenauer intraprese con convinzione la strada del riarmo del suo Paese, chiedendo contestualmente a Stati Uniti, Regno Unito e Francia di incrementare i rispettivi contingenti presenti, auspicando la creazione di un esercito europeo con la partecipazione attiva della Germania. La prospettiva francese non poteva che divergere da tale assunto; i francesi si dichiararono disponibili ad un riarmo della Repubblica Federale Tedesca ma non all'interno di un assetto nazionale, bensì in un più ampio contesto europeo sovranazionale, che ne avrebbe consentito e garantito la supervisione e il controllo. Ciò avrebbe rappresentato un passo decisivo verso l'unità europea, sigillando una riconciliazione definitiva tra tedeschi e francesi. Questi ultimi prospettavano un'architettura futura nella quale era concepibile un sovranismo europeo per controllare e prevenire eventuali derive dei tedeschi, mentre erano intenzionati, da soli, a ripristinare una grandezza e realizzare una maggiore indipendenza nazionale anche rispetto ad un potere assicurato da Regno Unito e Stati Uniti. Si trattava di un ideale di difesa europea funzionale ad attuare una precisa strategia francese.

1.2.2 La visione europea, gli interessi USA e la posizione italiana

Il progetto della Comunità Europea di Difesa poteva essere considerato, in un certo senso una trasposizione in campo militare del piano Schuman che venne elaborato per il carbone e l'acciaio. È infatti l'idea di un'Europa federale che presiede effettivamente all'elaborazione della politica di Difesa. L'esercito europeo così formato avrebbe di fatto sostituito gli eserciti nazionali la cui operatività sarebbe stata condizionata dal comando di un ministro della Difesa europeo. Pertanto, il riarmo della Germania poteva anche essere visto come una consistente fornitura di armi ed equipaggiamento da usare per uno scopo comune e comunque sotto una precisa supervisione. Concettualmente si tratta di un

progetto notevole per la sua portata federalista e decisamente sovranazionale, almeno in apparenza. Si parla per la prima volta della creazione di un esercito europeo annesso alle istituzioni politiche dell'Europa unita, posto sotto la responsabilità di un ministro della Difesa europeo, sotto il controllo di un'assemblea europea, con un bilancio militare comune. I contingenti forniti dai paesi partecipanti nell'idea originaria sarebbero stati incorporati nell'esercito europeo, a livello della più piccola unità possibile, il che avrebbe impedito alla Germania di ricreare un esercito e uno Stato Maggiore. In effetti, questo esercito sarebbe stato strutturato su divisioni europee, all'interno delle quali le unità nazionali sarebbero state integrate a livello di battaglione da 800 a 1.000 uomini, il che alla fine avrebbe reso possibile disperdere i contingenti tedeschi il più possibile. Ma se questo esercito è stato davvero pensato per essere federale ed europeo nella sua formazione e nelle sue unità, non lo era certamente al suo più alto comando, ovvero l'integrazione nell'apparato militare della NATO e quindi con una netta preminenza degli Stati Uniti. Per Washington, quindi, non si trattava di fornire all'Europa occidentale uno strumento di difesa indipendente. Al contrario, il nascente esercito europeo a fronte di una prima dipendenza dal Comando Atlantico, era suscettibile di una ulteriore dipendenza diretta cioè dagli Stati Uniti. I tedeschi, da parte loro, temevano questa integrazione militare della Germania Ovest, vista come una potenziale dissoluzione, che avrebbe sicuramente messo a repentaglio le prospettive della loro riunificazione con la Germania dell'Est quando questa sarebbe arrivata (dal momento che si tratta di una strategia a lungo termine predisposta già all'indomani della conclusione della seconda guerra mondiale). Inoltre, ritennero discriminatorie le disposizioni previste in merito al loro status militare. La partecipazione della Germania alla CED poteva avvenire solo a condizione di avere gli stessi doveri ma soprattutto gli stessi diritti degli altri paesi. Il progetto iniziale sarà poi emendato dai diplomatici americani, che lo trasformeranno radicalmente cambiandone anche la struttura che, nella sua fase finale prevedeva:

- la fine dello status di occupazione della Germania e la parità di diritti con degli Stati membri, circostanza quest'ultima che implicava la piena riabilitazione dei suoi territori e la sua piena sovranità. Inoltre, ciò supponeva che la Francia avrebbe dovuto rinunciare al suo programma

nucleare, altrimenti anche la Germania avrebbe potuto recriminare questo diritto che, invece, le era stato rifiutato dagli Alleati durante la capitolazione del Terzo Reich;

- la creazione di divisioni tedesche, limitate a 12, in questo nascente esercito che sarebbero state incluse in tutte le 40 divisioni nazionali di 13.000 uomini caratterizzati da un'uniforme comune. Si trattava di formare un esercito integrato sotto un comando comune, senza discriminazioni tra i paesi membri;
- l'abbandono della prevista carica di ministro della Difesa europeo quale luogo di decisione del CED che invece sarebbe passato nelle mani del Consiglio dei ministri, sede ove ogni paese membro è rappresentato dal proprio ministro della Difesa, compresa la Germania che in tal modo avrebbe ottenuto pari diritti all'interno della stessa Comunità nascente.

Le nuove istituzioni proposte per la CED sono meno sovranazionali di quanto inizialmente previsto in quanto il vero organo decisionale della CED, il Consiglio dei Ministri, era un luogo di coordinamento e decisione tra Stati, ma assolutamente non un organo federale, indipendente da essi, come l'Alta Autorità della CECA. Inoltre, il Consiglio dei ministri doveva pronunciarsi all'unanimità su tutte le questioni importanti, inerenti la sovranità di ciascuno Stato. Un aspetto che più degli altri destò perplessità perché in totale contraddizione con i principi precedenti, riguardava la possibilità che un accordo di uno solo dei ministri europei, anche contro il parere di tutti gli altri, venisse reputato sufficiente per autorizzare il comandante in capo della NATO, a ridistribuire le forze di difesa, o di cambiare il loro uso, senza dover chiedere il parere di altri stati europei. La nuova struttura, negli aspetti pratici, non avrebbe potuto nemmeno sviluppare una politica di difesa comune, ma accontentarsi di organizzare l'amministrazione militare, subordinata alla NATO, e quindi a Washington. Il comandante in capo della NATO avrebbe avuto la piena discrezionalità di scelta degli armamenti necessari secondo la strategia di volta in volta adottata dall'Alleanza Atlantica. Inoltre, fu previsto il divieto di tutte le esportazioni di equipaggiamenti militari, tranne che con l'autorizzazione del comandante della NATO, che portò a porre sotto la supervisione di Washington l'industria francese degli armamenti, all'epoca l'unica grande in Europa. La Comunità europea di difesa era diventata puramente

americana e apertamente antifrancese. La posizione ufficiale italiana¹³ era sintetizzata dalla volontà del Presidente del Consiglio Alcide De Gasperi di portare avanti un progetto che secondo le sue parole, avrebbe incarnato una dialettica positiva tra nazione ed Europa, e di una nazione che si proponeva all'Europa senza per questo annullarsi. Storiograficamente accomunato spesso a Konrad Adenauer e a Robert Schuman definiti quali "padri dell'Europa", in realtà De Gasperi presentava un profilo diverso dai due personaggi citati poiché la sua visione progettuale andava oltre le premesse già dettate da Jean Monnet ricercando una visione politica incisiva che poteva portare a una Europa federata ma con precisi vincoli in una sfera atlantica.¹⁴ Entusiasta del progetto, esaltava lo spirito di solidarietà che si sarebbe creato in diversi settori ma soprattutto nella difesa della pace attraverso uno sforzo unitario che, nel comprendere anche la Germania, avrebbe eliminato il pericolo di altre guerre e rappresaglie. Capì comunque che lo sforzo più grande non doveva essere unicamente quello di gettare le basi per strutture e comparti settoriali ma era preminente l'idea di far accettare alle masse un progetto di ampio respiro che oltre a rispondere alle esigenze del momento, racchiudesse il presupposto per coltivare speranze e attrattività per tutte le giovani generazioni europee.¹⁵ In un discorso¹⁶ pronunciato a Strasburgo il 10 dicembre 1951, all'Assemblea del consiglio d'Europa, De Gasperi espose con enfasi l'importanza del progetto della CED:.

"...Se noi chiamiamo le forze armate dei diversi paesi a fondersi insieme in un organismo permanente e costituzionale e, se occorre, a difendere una Patria più vasta, bisogna che questa Patria sia visibile, solida e viva, anche se non tutta la costruzione è perfetta occorre che sin da ora se ne vedano le mura maestre e che una volontà politica comune sia sempre vigilante perché riassuma gli ideali più puri delle nazioni associate e li faccia brillare alla luce di un focolare comune". "...Quando questo esercito, così organizzato ed amministrato, sarà inserito nella NATO secondo

¹³ Varsori A. (a cura di), Nazione, interdipendenza, integrazione. Le relazioni internazionali dell'Italia (1917-1989), Carocci, Roma 2006.

¹⁴ Di Nolfo E., Rainero R., L'Italia e la politica di potenza in Europa, Marzorati, Milano, 1992.

¹⁵ Fanfani A., Autunno 1956: la Democrazia Cristiana e i problemi internazionali, Cinque Lune, Roma, 1956

¹⁶ De Gasperi A.: Scritti e discorsi di politica internazionale, Alcide De Gasperi e la politica internazionale: un'antologia degli scritti su "L'illustrazione Vaticana" (1933-1938) e di discorsi all'estero (1945-1954). Allara, G. Volume 3. Roma: Cinque Lune, 1990. 445 p. "x", URL:http://www.cvce.eu/obj/discorso_di_alcide_de_gasperi_strasburgo_10_dicembre_1951-it-7dbeb557-c313-4703-a237-d909f35a2c25.html

le risoluzioni della Conferenza di Roma, noi avremo raggiunto l'unione di tutte le forze difensive e nel medesimo tempo avremo creato all'interno un nucleo federale europeo che sarà la garanzia della nostra solidarietà democratica. È assolutamente necessario che il nostro compito non fallisca, e che trovi nei paesi la collaborazione di tutte le forze democratiche e di rinnovamento sociale, e ridia nello stesso tempo in tutti i nostri amici, particolarmente in America, la fede nei destini dell'Europa".

1.2.3 Il rifiuto francese, l'assetto NATO e il Piano Fouchet

La supremazia e le continue manifestazioni di controllo da parte degli USA non piacquero al generale de Gaulle che si schierò apertamente per una indipendenza della Francia. Dal 1953 si impegnò contro la ratifica del trattato che, secondo lui, avrebbe conferito al comandante in capo della NATO diritti quasi discrezionali "*che nessun governo di nessun paese, in qualsiasi momento, ha mai concesso a nessuno dei suoi generali*". De Gaulle non poteva accettare l'idea di cedere il comando del suo esercito nazionale agli americani, né di imbavagliare la sua industria delle armi, e ancor meno di abbandonare il suo programma nucleare. In quell'anno, nuovi accadimenti contribuirono a mutare il quadro geopolitico: il 1953 segna la morte di Stalin e l'avvento di Nikita Khrushchev che pur nella consapevolezza del suo ruolo decise comunque di strutturare una convivenza più pacifica con gli USA; anche la fine della guerra di Corea produsse i suoi effetti e il "pericolo comunista" perse, in parte, la sua forza in un contesto internazionale interessato da nuove spinte. De Gaulle ebbe modo di ridurre il ruolo (o per meglio dire la dipendenza) della Francia nel quadro atlantico: mentre 4 dei 6 paesi, tra cui la Repubblica Federale di Germania, ratificarono la CED nel 1953 e nel 1954, in Francia il dibattito tra i fautori e i critici assunse toni molto aspri a vantaggio di questi ultimi. L'Italia cominciò ad avere dubbi sull'iniziativa e sospese la ratifica in attesa di un pronunciamento francese che non si fece attendere molto; il 30 agosto 1954 dopo un acceso e appassionato dibattito, l'Assemblea nazionale, con 319 voti contro 263, ottenne addirittura di non discutere neppure su una eventuale ratifica del Trattato. Il rifiuto francese assunse non valore ancora più pronunciato perché incarnò il fallimento di un intero progetto politico: quello stesso progetto politico

europeo a cui era associato.¹⁷ Jean Monnet si dimise dalla carica di Presidente dell'Alta Autorità della CECA ritenendo inaccettabile la battuta d'arresto inflitta alla costruzione di una idea che aveva personalmente portato avanti sin dal 1950. Robert Marjolin, uno dei principali collaboratori di Monnet nelle sue memorie espresse un suo convincimento, in parte sorretto da constatazioni direttamente vissute: "L'incapacità dell'Europa di unire, deriva da una decisione implicitamente presa dagli europei dopo la fine della seconda guerra mondiale, quella di affidarsi agli americani per la loro difesa"¹⁸. Dopo il fallimento della CED, i partner NATO intrapresero un dialogo deciso per trovare una soluzione al riarmo e all'attuazione della sovranità tedesca. Messi da parte i francesi, le iniziative inglesi, sostenute dagli americani, si imposero rapidamente. Un punto di svolta fu segnato dalla conferenza di Londra svoltasi nell'ottobre del 1954, la Germania venne autorizzata ad un programma di riarmo e a creare un esercito nazionale, le venne consentito inoltre di far parte della NATO alla stregua degli altri alleati. Alla Francia vennero date alcune garanzie: minore dipendenza organizzativa nel settore delle Forze Armate e la rassicurazione che il riarmo tedesco sarebbe avvenuto nell'ambito dell'UEO (Unione dell'Europa Occidentale) al cui interno sedevano i sei paesi aderenti alla CECA oltre al Regno Unito. All'interno della UEO venne creata anche una Agenzia per il Controllo degli Armamenti con il potere di controllare tutti gli armamenti dei paesi membri; soltanto alla Repubblica Federale di Germania fu fatto divieto di fabbricare armi di tipo nucleare, batteriologico e chimico. Oltrecortina, i sovietici si mostrarono chiaramente insoddisfatti: dieci giorni dopo l'entrata ufficiale della RFT nella NATO nel 1954, annunciarono la creazione del Patto di Varsavia e vi incorporarono la nuova Repubblica Democratica Tedesca. Tra i numerosi documenti dell'epoca che confermano l'evoluzione storica esaminata, merita un particolare approfondimento il memorandum predisposto nel 1954 da Livingston Tallmadge Merchant¹⁹, all'epoca Assistant Secretary of

¹⁷ De Lorenzi C.: "Jean Monnet - il Padre fondatore o l'ispiratore dell'Europa?", Università Ca' Foscari, Venezia, 2012.

¹⁸ Marjolin R.: "Le travail d'une vie", memoires 1911-1986, avec un preface de Raymond Barre, Laffont edit., 1986

¹⁹ Livingston Tallmadge Merchant (1903–1976) was a United States official and diplomat. He twice served as Assistant Secretary of State for European and Eurasian Affairs (1953–1956); Assistant Secretary of State for European and Eurasian Affairs (1953–1959); Ambassador Extraordinary and Plenipotentiary, Canada (1956–1958); Deputy Under Secretary of State for Political Affairs (1959); Under Secretary of State for Political Affairs (1959–1961); Career Ambassador (1960); Ambassador

State for European and Eurasian Affairs e diretto al Segretario di Stato John Foster Dulles che credeva fortemente nell'idea della CED e si mostrava riluttante rispetto alle proposte riduttive, elaborate da Gran Bretagna e Francia e al rifiuto finale di quest'ultima. Su tali basi, Livingston Merchant predispose il memorandum (consapevole della sua importanza in vista di un parere favorevole da parte del Presidente USA). Il documento, un *memorandum* "top secret" in seguito declassificato come da codifica "Authority NND 934569", riporta la data 10 settembre 1954²⁰, palesa la volontà di Washington di andare oltre e portare comunque le forze armate della Germania in una cornice occidentale e di sicurezza europea, limitandone comunque l'indipendenza militare. Tratti salienti del documento dimostrano come tali volontà siano espressione anche degli alleati in una sorta di comune desiderio di andare oltre la diatriba Germania-Francia:

"...many of the provisions in our program which will limit German control over their military establishment are multilateral".

Peraltro, tali accordi multilaterali erano tutti finalizzati a produrre "quali effetti collaterali" quello più importante di limitare l'autonomia di tutte le forze tedesche impegnate nella NATO, in tal modo, il Comandante Supremo delle Forze Alleate in Europa (ovvero il SACEUR), in qualità di massimo leader militare, avrebbe il controllo totale sul dispiegamento delle forze a lui affidate in modo coerente ai piani NATO; accordi, secondo Merchant da non considerarsi quali discriminatori nei confronti di una Germania che, consapevole della sua posizione al termine del conflitto, li avrebbe certamente accettati. Come prezzo della sua ammissione nell'UEO e nella NATO, la Germania Ovest non avrebbe prodotto armi atomiche e termonucleari, bombardieri e sottomarini, a causa della sua posizione strategica esposta tranne che per gli ambiti concessi e concordati con la NATO:

"...Germany should be invited to access to the North Atlantic Treaty by agreement among all the signatories in accordance with Article 10. In accepting this invitation, Germany would submit a formal reply emphasizing the defensive character of the forces she expects to contribute and undertaking to follow in her initial contribution the size and composition of force specified in the EDC Special Military Agreement

Extraordinary and Plenipotentiary, Canada (1961–1962); Secretary of State ad interim (1961). <https://history.state.gov/departmenthistory/people/by-name>

²⁰ Source: RG 59, Conference Files, box 56, CF 359 Secretary's Trip to Bonn-London Sept. 15-18, 1954 (Also published in *Foreign Relations of the United States 1952-1954 Volume 5 Part II Western European* Washington, D.C., 1983)

(this excludes submarines and strategic bombers)". "...She would state, however, that she would not produce atomic and thermonuclear weapons, military aircraft, etc (other items in Annex II of Article 107 of EDC Treaty) because of her exposed strategic position except as agreed by NATO".

Quanto gli Stati Uniti tenessero a questo programma, è dimostrato dallo spasmodico interesse a monitorare anche i singoli incontri europei in materia. L'11 settembre 1954 a Bruxelles, poche settimane prima della Conferenza delle nove potenze che si sarebbe poi svolta a Londra, il Ministro degli Esteri britannico Anthony Eden presentò ai ministri degli esteri dei paesi del Benelux (Belgio, Paesi Bassi e Lussemburgo) il suo piano per portare la Germania occidentale nella NATO. In questa circostanza il primo Ministro lussemburghese Joseph Bech fornì un resoconto segreto dell'incontro a Wiley Buchanan (all'epoca incaricato d'affari presso l'ambasciata degli Stati Uniti, in seguito divenuto ambasciatore. Tale evidenza si rileva dal documento "top secret" poi declassificato, riportante la data "20 settembre 1954".²¹ Nel corso della riunione i partecipanti si mostrarono concordi circa "il pericolo" rappresentato non solo dall'eventuale riarmo tedesco tramite una progettazione di autonome divisioni tedesche ma anche da una sorta di indipendenza costituita da una "Germania che viva al di fuori della comunità europea" potenzialmente punto di attrazione di orbite geopolitiche diverse da quelle occidentali. Per impedire ciò era dunque necessario procedere con specifiche garanzie attraverso controlli, ivi comprese le limitazioni al contributo militare in ambito NATO; sostanzialmente, anche in questo caso, si è cercato di operare delle restrizioni che non apparissero discriminatorie ma anzi che potessero essere accettate con favore dai tedeschi anche contando sullo spirito fortemente europeo di Adenauer:

"...While admitting Germany into the Bruxelles pact and NATO one must seek guarantees against the dangers of German militarism, These guarantees can be found in a limitation of the German contribution, in a control of the use of German force, in a control of production of arms, etc. etc. But one must seek for limitations which, while being fully efficient, would not appear discriminatory towards Germany and would be accepted by it. It does not seem impossible to arrive at a

²¹ Source: RG 59, Conference Files, box 56, CF 359 Secretary's Trip to Bonn-London Sept. 15-18, 1954 <https://nsarchive.gwu.edu/document/17552-document-07-nine-power-meeting-september-28-29>

solution in this regard, with the assistance of technicians, counting on the european spirit of Adenauer”.

Per tutti gli europeisti, diventò di primaria importanza il superamento del fallimento della CED per proseguire nella strada di una costruzione europea e per fare ciò occorreva non fermarsi alla CECA; il tema dell'unificazione militare venne abbandonato a favore dell'unificazione economica, sull'esempio di quest'ultima istituzione. Dall'autunno del 1954 nacquero svariati progetti molti dei quali riproponenti una rivisitazione dei vecchi. I poteri della CECA furono estesi ai trasporti e alle fonti energetiche. Si passò alla creazione di un'organizzazione per l'energia atomica EURATOM. Finalmente venne lanciato il grande progetto di mercato comune generalizzato, per riunire tutti i settori dell'economia: il suo scopo era quello di procedere verso uno sviluppo di istituzioni comuni, della progressiva fusione delle economie nazionali, della creazione di un mercato comune e della progressiva armonizzazione della loro politica sociale. La Comunità Europea continuerà il processo di costruzione istituzionale dell'Europa attraverso i Trattati di Roma del 1957, che istituiranno la Comunità Economica Europea (CEE) e la Comunità Europea dell'Energia Atomica (EAEC). Queste due comunità, limitate al coordinamento economico, non affrontarono la questione della difesa, di cui la NATO si è appropriata, né la questione dell'Europa politica, o qualsiasi forma di messa in comune della sovranità, o istituzioni comunitarie. Nel 1961 fu lanciato un ultimo tentativo sotto forma di un nuovo piano "Fouchet". L'attuazione di questo piano avvenne in un contesto travagliato per la Comunità Europa. Fu davvero un periodo in cui la Guerra Fredda si intensificò e in cui De Gaulle, tornato al potere in Francia, riprese la sua linea di strenuo oppositore del federalismo europeo, sostenendo "indipendenza nazionale" in rottura con il federalismo europeo e la divisione di Yalta: propugnò una "Europa delle nazioni" che coinvolgesse la riconciliazione franco-tedesca in uno spazio esteso "dall'Atlantico agli Urali". Fu con questo in mente che creò la forza di deterrenza nucleare francese, ritirò la Francia dal comando militare della NATO nel 1966, e poi nel 1967 pose il veto all'ingresso del Regno Unito nel Mec. Nel 1961 la questione della difesa era quindi ancora oggetto di disaccordo tra, da una parte, la Francia, favorevole ad una semplice cooperazione intergovernativa, e dall'altra gli altri 5 paesi membri della CEE, favorevoli quanto loro alla attribuzione di competenze di tipo politico alla

Comunità Europea. Il progetto di questi paesi era quello di dare forma alla volontà di unione politica, già implicita nei trattati che istituiscono le Comunità europee. Il piano Fouchet prevedeva l'istituzione della cooperazione tra gli Stati membri in materia di politica estera e di difesa, scienza, cultura e tutela dei diritti umani. La centralizzazione all'interno dell'Unione veniva accantonata a favore della cooperazione tra le istituzioni delle comunità europee. Inoltre, il generale de Gaulle vi aggiunse competenze e obiettivi di politica economica, che interessavano quindi i campi di azione delle comunità europee appena create. Le stesse cause che avevano impedito la realizzazione della CED producevano così gli stessi effetti su questo nuovo progetto: il piano francese Fouchet rimarrà lettera morta.

1.2.4 Il Trattato dell'Eliseo

Il Trattato dell'Eliseo rappresenterà il tamponamento di questo piano intergovernativo, riprendendo le principali disposizioni ma limitandole a due paesi, Germania e Francia. Nel 1963, 18 anni dopo la capitolazione della Germania nazista, il cancelliere tedesco Konrad Adenauer firmò con il presidente francese Charles de Gaulle il Trattato dell'Eliseo, che voleva stabilire una stretta alleanza tra i due paesi, nel campo delle relazioni internazionali, della difesa e dell'istruzione, stabilendo una concertazione attraverso un programma di vertici militari o intergovernativi. Nel campo della difesa, si trattava, ripetutamente, di allontanare la Germania occidentale dal suo protettore americano, per promuovere un'Europa indipendente dagli Stati Uniti e dall'Unione Sovietica. La Francia aveva una propria forza deterrente nucleare che avrebbe potuto sostituire la deterrenza americana sul suolo europeo. Da questo punto di vista, il progetto era destinato a fallire: gli Stati Uniti non erano pronti a rinunciare alla loro posizione nell'Europa occidentale di fronte all'Unione Sovietica, con la quale si era aperta la guerra fredda, e che stavano cercando di arginare in tutto il mondo. Qualsiasi progetto di unione franco-tedesca nel campo della difesa rischiava di essere vanificato dalla cooperazione militare che legava la Germania Ovest al protettore americano, l'Alleanza Atlantica della NATO. Gli Stati Uniti erano i garanti dell'esistenza della Germania Ovest di fronte al minaccioso comunismo dell'Unione Sovietica e alle truppe pesantemente armate del Patto di Varsavia. Non avendo né i mezzi né il

diritto di garantire la propria difesa, la Germania rimase sotto il controllo degli Stati Uniti, il che avrebbe impedito, ancora per molto tempo, qualsiasi progetto di unione con la Francia. Al di là di tutto, questo trattato ratificherà il rapporto di fiducia e amicizia che si è instaurato tra gli ex "nemici ereditari" e si basava, tra l'altro, su un punto molto importante: l'incontro dei popoli dei due paesi. Per i due firmatari era importante che non si trattasse di un trattato deciso solamente dai rispettivi capi di Stato, ma era necessario che ai cittadini fosse dato un segnale concreto di avvicinamento e di cooperazione. Per molto tempo i giovani tedeschi e francesi furono oggetto di campagne pubblicitarie circa l'apertura a programmi reciproci sull'apprendimento delle lingue e sull'equivalenza dei diplomi. Lo dimostrano gli scambi internazionali tra i due Paesi e i numerosi programmi studio instaurati con le scuole superiori proprio a seguito del Trattato. Era tuttavia evidente che la Germania non avrebbe potuto scegliere liberamente di recidere i legami mantenuti con gli Stati Uniti: il 15 giugno 1963, il Bundestag della Repubblica Federale di Germania ratificava il Trattato dell'Eliseo dopo aver votato un preambolo che introduceva espressamente ed esplicitamente le medesime parole e concetti che de Gaulle aveva ostinatamente respinto. Il preambolo menzionava "la stretta associazione tra Europa e Stati Uniti d'America", "l'ammissione della Gran Bretagna", "la difesa comune nel quadro dell'Alleanza del Nord Atlantico", "l'abbassamento delle barriere doganali con Gran Bretagna e Stati Uniti Stati d'America, così come altri Stati, nell'ambito del GATT". A De Gaulle non restava altro che accettare con estrema delusione il nuovo preambolo imposto dal Bundestag e la nuova cooperazione franco-tedesca, nonostante ciò, il legame personale tra i due capi di Stato giocò un ruolo decisivo nella concretizzazione dell'amicizia franco-tedesca. Le loro buone relazioni sono state all'origine di una cooperazione bilaterale che proseguirà con i presidenti che seguiranno e che avrà effetti di ricaduta per la costruzione europea. Questo fu l'inizio del "motore franco-tedesco". Da allora, tutti i presidenti francese e tedesco formarono così coppie politiche destinate ad arrivare a un'intesa su molti aspetti strategici per il vecchio continente. Le relazioni franco-tedesche comunque sono sempre state tollerate e valutate nei loro equilibri dalla politica statunitense che sin dalle loro prime fasi storiche ha saputo inserirsi con abilità. Significativo, in tale

quadro, appare il documento redatto da Thomas L. Huges²² per conto dello U.S. Department Of State – Director of Intelligence and Research nel 1965, in un periodo in cui la crisi sul ruolo della Francia all'interno della NATO cominciava ad avere aspetti consistenti. Il memorandum "secret" declassificato con ratifica "Authority NND 70949" riporta la data del 5 febbraio 1965²³ e nonostante presenti come oggetto: "Can We Do Business With De Gaulle ?", nella realtà non serviva a "rispondere" a tale richiesta, bensì si proponeva di suggerire come un probabile ritiro francese dalla NATO poteva essere impedito, se non del tutto, almeno come parte di un "pacchetto" più globale tra gli U.S.A. e la Francia partendo da elementi di comune interesse quali, ad esempio la resistenza alla minaccia sovietica e l'opposizione al riarmo e alla creazione di armamento nucleare della Germania. In realtà questo documento era il terzo di una serie che affrontava le possibili prospettive dettate da una "uscita" francese dall'Alleanza Atlantica e ancor più circa una eventuale forza nucleare alleata che in qualche modo potesse vedere coinvolta (seppure in parte) la Germania. Era quindi di vitale importanza "contenere" la Germania e trattare con la Francia non perdendo mai di vista il bilanciamento delle forze in Europa, suscettibili di accordi che avrebbero potuto alterare gli equilibri creati da Washington:

"...French withdrawal from NATO can be prevented if at all only as part of an overall "package deal" between the United States and France. The key element of this would be that the two parties agree 1) that they still had common interests on which they could collaborate (e.g., resistance to a continuing Soviet threat, opposition to German national nuclear armament); and 2) that, therefore, they would agree to disagree on other subjects (e.g., the future "organization" of Europe)".

Preso atto della nota suscettibilità di De Gaulle che difficilmente avrebbe limitato la sua libertà di azione nel perseguire le sue mire politiche in cambio di qualche concessione, diventava preminente realizzare più tentativi di approccio, su accordi diversificati e limitati ma nell'intento di migliorare i rapporti diplomatici con Parigi

²² Thomas Lowe Hughes (born December 11, 1925) was Assistant Secretary of State for Intelligence and Research during the Kennedy and Johnson administrations. From 1971 he was President of the Carnegie Endowment for International Peace. He was also counsel to Minnesota Senator Hubert Humphrey (1955-1958). Born in Mankato, Minnesota, Hughes was educated at Carleton College, Minnesota, Oxford University, as a Rhodes Scholar, and Yale Law School, graduating in 1952. <https://www.academyofdiplomacy.org/member/thomas-l-hughe>

²³ Source: RG 59, INR, Reports Coordination and Review Staff. Intelligence Reports, 1965-1966, box 155, REU-4-RM

e operare i tanto desiderato contenimento tedesco. Si sarebbe trattato di una scelta politica importante ma, proprio per le implicazioni future, assolutamente da non sottovalutare.

“...This sketch of the possible terms of a limited agreement with de Gaulle is not presented as an argument for such an agreement or even for a change in the present US approach to the "French problem." It only suggests the kinds of things that de Gaulle might possibly agree to and the kinds of things that would, at a minimum, be necessary to cause him to carry out the major reversal of his policy which French tolerance of the ANF would involve. It may be objected that it is hard to think that de Gaulle, would thus limit his freedom of action in pursuit of his policies even in return for the concessions that the United' States might make to him. Reality may turn out to be too interconnected to permit profitable or safe exploration of this kind of pragmatic, limited approach”.

1.3 La nuova Politica di Sicurezza e Difesa

1.3.1 Il concetto di Foreign and Security Policy

Il concetto di *Common Foreign and Security Policy* venne introdotto per la prima volta in seno al Trattato sull'Unione Europea (TUE) firmato a Maastricht nel 1992 ed entrato in vigore nel 1993; si trattava di una prospettiva a medio-lungo termine per la costituzione di una difesa del territorio europeo fattivamente organizzata e partecipata dagli stessi Paesi membri. Una nuova dimensione europea nasceva sulla base delle idee in precedenza espresse nel contesto di quella Cooperazione di Politica Europea che si andava sviluppando già a partire dal 1970.²⁴ Successivamente, il trattato firmato a Maastricht contribuì a dare all'Unione nuove direttrici; tra queste, un proprio rafforzamento “con ogni misura possibile”; il mantenimento della pace ed il rafforzamento della sicurezza internazionale; lo sviluppo ed il consolidamento della democrazia e dello Stato di diritto; il rispetto dei diritti umani e delle libertà fondamentali. La PESC costituiva così il “secondo pilastro” dell'Unione Europea, caratterizzato dal ricorso al “metodo

²⁴ La cooperazione politica europea (CPE) - lanciata in via informale nel 1970, (in seguito al rapporto Davignon) e successivamente istituzionalizzata dall'Atto unico europeo del 1987 - prevedeva la consultazione tra gli Stati membri in ordine ai settori attinenti alla politica estera.

intergovernativo”, basato su una logica di cooperazione tra i governi²⁵. L’avvento della PESC apportava inoltre significativi progressi in tre direzioni:

- riuniva le questioni politiche e quelle di sicurezza, inclusa “l’eventuale formulazione di una politica di difesa comune”;
- rafforzava il significato della concertazione e dell’elaborazione di posizioni comuni sui temi di politica internazionale, obbligando gli Stati membri a “vegliare sulla conformità delle loro politiche nazionali alle posizioni comuni”;
- creava un nuovo strumento giuridico, l’Azione Comune, in grado di impiegare risorse finanziarie dell’UE per azioni collettive nel settore della politica estera e di sicurezza.

Si trattava pur sempre di settori, nell’ambito dei quali ognuno dei Paesi membri aveva sempre affermato di dover esercitare la propria prerogativa di sovranità e che invece, con tale formulazione e con l’accordo delle parti si decise (seppure con qualche distinguo) di affrontarli congiuntamente, nella consapevolezza che si trattasse di un nuovo approccio alla difesa con innegabili vantaggi per tutti. Il momento storico inoltre contribuì a dare una ulteriore valenza di tipo geopolitico a questa iniziativa: si era alla fine della Guerra Fredda²⁶ e quindi non esisteva più la preoccupazione per una minaccia monolitica e ben individuata quale era stata la vecchia Unione Sovietica mentre cominciavano ad emergere preoccupazioni su più fronti in un panorama globalizzato con sfide nuove e complesse da affrontare. Interessante a tal proposito risulta essere il dibattito accademico legato a questo periodo dal quale emerge, a fattore comune, l’inadeguatezza degli strumenti a disposizione dell’UE di fronte all’insorgere di crisi internazionali. Due gli elementi sui quali si caratterizza l’attenzione: la forma che avrebbe dovuto assumere la cooperazione europea in politica estera e la questione relativa al rapporto tra

²⁵ Il metodo comunitario che regolava il funzionamento istituzionale del primo pilastro, si differenziava dal metodo intergovernativo (valido per il secondo e terzo pilastro) fondato appunto su una logica di cooperazione intergovernativa caratterizzata dal diritto di iniziativa della Commissione limitato ad aspetti specifici, anche se condiviso con gli altri paesi e dal ricorso generalizzato all’unanimità in sede di Consiglio con un ruolo meramente consultivo del Parlamento Europeo ed un ruolo limitato della Corte di giustizia.

²⁶ L’espressione Guerra Fredda sintetizza la divisione del mondo nei due blocchi occidentale e sovietico, venutasi a creare dopo la fine della Seconda guerra mondiale, tra gli Stati Uniti e l’Unione Sovietica. La Guerra Fredda ha permeato la seconda metà del 900, in un periodo compreso tra il blocco di Berlino del 1948 e la caduta del sistema sovietico del 1991.

Europa e Alleanza Atlantica ²⁷ Un tentativo di superare tale stallo, arrivò dalla Commissione Europea con il parere espresso il 21 ottobre 1990 con il quale si proponeva di incorporare la politica estera e di difesa all'interno della sfera comunitaria²⁸ . La proposta rimase vana dal momento che non venne sostenuta né dagli atlantisti e né dagli europeisti per motivi determinati da una diversa prospettiva. Gli atlantisti temevano che così facendo si sarebbe registrato un deciso indebolimento del legame con la NATO, mentre gli europeisti ritenevano estremamente macchinoso l'ampliamento delle competenze che, a loro dire, avrebbe comportato un rallentamento del funzionamento del complesso comunitario. ²⁹ Non passò molto tempo però prima che emergessero le evidenti lacune circa la possibilità con la quale l'Unione potesse davvero esprimere una concreta azione di difesa comune. L'occasione si presentò, con la violenta crisi provocata dalle guerre interetniche balcaniche iniziate nel 1992 e protrattesi fino al 1996 che ebbero il loro culmine col massacro di Srebrenica tra l'11 e il 17 luglio del 1995. In quel caso l'Unione europea dimostrò una chiara impreparazione a gestire la crisi: l'auspicata nascente PESC non consentì di operare nell'immediatezza una obiettiva interpretazione degli eventi e di mettere in campo un adeguato apparato politico militare. Solamente alla fine del 1995 si pervenne all'accordo di Dayton realizzato grazie ad un consistente contributo degli Stati Uniti.

1.3.2 Nascita ed evoluzione della PESD

Con il trattato di Amsterdam, firmato il 2 ottobre 1997 dagli allora 15 Paesi dell'Unione Europea ed entrato in vigore il 1º maggio 1999 vennero introdotte altre innovazioni, attribuendo al Segretario Generale del Consiglio anche il ruolo di Alto Rappresentante per la Politica Estera e di Sicurezza Comune e conferendo al Consiglio Europeo una specifica competenza di "orientamento" in tema di PESC e di Politica europea di sicurezza e difesa (PESD). Ma il vero acceleratore del

²⁷ Graziani F., *Lo spazio di sicurezza europeo. L'Unione europea e i suoi rapporti con la NATO e con l'OSCE*, Napoli, Editoriale Scientifica, 2006, pp.79-87.

²⁸ Parere della Commissione europea del 21 ottobre 1990 sul progetto di revisione del Trattato che istituisce la Comunità economica europea, in *Boll. Suppl.* 2/91.

²⁹ Comelli M., *Gli interventi dell'Unione europea e la cooperazione con la NATO*, in Natalino Ronzitti (a cura di), *Le forze di pace dell'Unione Europea*, Roma, Rubbettino, 2005, p. 138.

processo può essere considerato con il vertice franco-britannico di Saint Malo³⁰, del dicembre 1998, durante il quale la Francia, desiderosa di realizzare una politica di difesa tradizionalmente europea e la Gran Bretagna, convinta della necessità di non poter prescindere dall'assistenza USA, approdarono a delle significative decisioni comuni tra cui la volontà di porre a carico dell'Unione la gestione delle crisi internazionali, dotandosi anche di adeguate capacità militari. Attività fino a quel momento in parte svolta dall'UEO sul cui ruolo i due Paesi erano da tempo divergenti, dal momento che la Francia era favorevole all'integrazione di tale struttura nell'Unione mentre la Gran Bretagna proponeva la sua estinzione. Il punto di convergenza invece fu proprio quello di incardinare la PESD sotto la guida dell'UE che avrebbe dovuto disporre di una capacità d'azione autonoma fondata su forze armate credibili e strutture politiche e militari adeguate, ma non indipendenti dalla NATO e avrebbe dovuto limitarsi alla realizzazione delle missioni di Petersberg³¹. Il metodo privilegiato per lo sviluppo della PESD era ancora quello intergovernativo ed un ruolo centrale, nell'elaborazione della nuova politica, era assegnato soprattutto al Consiglio Europeo. L'iniziativa di St. Malo fu accolta con favore anche dal Consiglio Atlantico del 1999,³² con l'invito tuttavia a evitare duplicazioni di forze con conseguenti inutili sovrapposizioni di ordine politico ed economico. In ragione di ciò, al Consiglio europeo svoltosi ad Helsinki nello stesso anno venne ribadito il concetto "*determination to develop an autonomous capacity to take decisions and, where NATO as a whole is not engaged, to launch and conduct eu-led military operations in response to international crisis*"³³, tanto che venne considerato come un punto di svolta nella storia della difesa europea. Sostanzialmente, il *Consiglio Europeo di Helsinki* (1999) sancì la "determinazione Europea di sviluppare capacità decisionali autonome e di

³⁰ Il 3 e 4 dicembre 1998, a Saint-Malo, in Bretagna si è tenuto un importante vertice franco-britannico. L'incontro fra Tony Blair e Jacques Chirac ha creato i presupposti per una nuova area politica dell'Unione europea, che sarebbe stata denominata Politica Europea di Sicurezza e di Difesa (PESD).

³¹ Il Trattato sull'Unione europea (Amsterdam 1997) fissava come obiettivi da realizzare in questo ambito: le missioni umanitarie e di evacuazione, le missioni per il mantenimento della pace, la disponibilità di forze per la gestione degli stati di crisi, compreso il ristabilimento della pace. Definite in seno ad una riunione dei Ministri dell'Unione dell'Europa Occidentale (UEO) nella città tedesca di Petersberg, queste vengono, da allora, chiamate missioni di Petersberg.

³² AA.VV. La cooperazione tra l'Unione Europea e la NATO, Contributi di Istituti di ricerca specializzati, XV Legislatura, servizio studi Senato della Repubblica n. 69, maggio 2007.

³³ Consiglio Europeo di Helsinki, Conclusioni della Presidenza 10-11 dicembre 1999 - Extract from the Declaration of the Helsinki European Council <https://publications.parliament.uk/pa/cm199900/cmselect/cmdfence/264/26425.htm>

avviare e condurre operazioni militari sotto egida europea in risposta a crisi internazionali, qualora la NATO opti per non intervenire come organizzazione”. Si trattava di un impegno da parte degli Stati membri, tendente a sviluppare, tutte le capacità atte a condurre le cosiddette missioni di Petersberg, missioni che prevedono lo svolgimento dei compiti stabiliti dagli accordi di Petersberg, definiti dall’UEO nel 1992 e poi incorporati nel Trattato di Amsterdam del 1997. L’articolo 17 del trattato circoscrive l’ambito delle missioni Pesd all’esecuzione di tre compiti fondamentali:

- missioni umanitarie e di soccorso, come per esempio l’evacuazione di cittadini di stati membri dell’UE da aree di crisi;
- missioni di mantenimento della pace (peace-keeping) per prevenire l’erompere di un conflitto tra due stati;
- missioni di unità di combattimento nella gestione delle crisi, comprese le missioni tese al ristabilimento della pace (peace-making), come per esempio l’imposizione di una zona demilitarizzata per separare due fazioni in guerra.

Nello stesso Consiglio di Helsinki venne stabilito quale “*headline goal*”,³⁴ di attuare un decisivo sviluppo capacità militari dell’Unione attraverso la costituzione entro il successivo 2003 di una forza capace di affrontare tutte le missioni di tipo Petersberg, forte di 15 brigate o comunque dotata di un dispositivo di 60.000 uomini.³⁵ Le caratteristiche della stessa erano ben individuate con riguardo al *self sustaining* con capacità di comando, controllo, *intelligence*, di *combat support* e logistiche e in aggiunta, quando ritenuto opportuno, con supporto navale e aereo. Completavano il quadro la necessità di disporre la stessa con tempi di proiezione contenuti (proiezione e dispiegamento entro 60 giorni) e capacità di permanere in teatro per almeno un anno. Con il Consiglio europeo di Nizza (2000) furono poi istituite, con atto del Consiglio dell’Unione, “un’architettura definitiva e nuove strutture politiche e militari permanenti” tese ad assicurare il controllo politico e la direzione strategica delle crisi, e la condotta delle operazioni. Era nata la PESD ovvero la Politica Europea di Sicurezza e Difesa (così definita per la prima volta nel precedente vertice di Colonia del 1999) quale parte integrante e strumento

³⁴ Civilian Headline Goal 2010, Council of the European Union, novembre 2007.

³⁵http://www.consilium.europa.eu/uedocs/cmsUpload/MilitaryCapabilitiesFC06backgroundNov06_en.pdf

indispensabile della PESC. Nel gennaio 2001 a seguito di accordi tra il Segretario Generale della NATO e la Presidenza dell'Unione Europea vennero create le basi per dei *meetings* congiunti a livello ministeriale e di Ambasciatori. Tale accordo prevedeva almeno tre riunioni a livello di Ambasciatori ed una a livello ministeriale ogni 6 mesi durante ciascuna Presidenza europea. Nello stesso ambito venne deciso che dei gruppi di lavoro congiunti si riunissero a partire dalla metà del 2000 allo scopo di affrontare tematiche come le procedure per lo scambio di informazioni classificate e di *intelligence*, le modalità per l'accesso dell'Unione Europea agli assetti ed alle capacità dell'Alleanza, gli obiettivi relativi alle capacità (incluse le questioni concernenti il sistema di pianificazione della difesa dell'Alleanza), gli accordi per la consultazione. Tali *meetings* si svolgono regolarmente dal febbraio 2001, presso il Comitato politico e di sicurezza (COPS) e il Consiglio del Nord Atlantico (NAC). Le strutture destinate ad assicurare il controllo politico, la direzione strategica delle crisi, e la condotta delle operazioni sono:

- il Comitato politico di sicurezza (COPS) composto da rappresentanti permanenti con il rango di Ambasciatori;
- il Comitato militare (EUMC) composto dai Capi di Stato Maggiore della Difesa, rappresentati dai loro delegati permanenti;
- lo Stato Maggiore (EUMS) responsabile dell'allertamento rapido, dell'analisi delle situazioni, e della pianificazione strategica per le missioni cosiddette di Petesberg.

La PESD fu dichiarata operativa nel 2001, al Consiglio Europeo di Laeken. Nel 2002, il Consiglio Europeo di Siviglia definì il principio del possibile impiego di risorse PESD anche a sostegno della lotta al terrorismo nei Paesi terzi e, soprattutto, l'UE e la NATO raggiunsero un'intesa (nota come *Berlin plus*) che fra l'altro consente all'Unione Europea di ricorrere, se del caso, ai mezzi e alle capacità collettive dell'Alleanza Atlantica. Al termine di questa fase di preparazione, il 1° gennaio 2003, l'Unione Europea avviò la sua prima operazione di gestione internazionale di crisi: la missione di polizia in Bosnia Erzegovina (EUPM). L'ampliarsi del raggio d'azione della PESC e l'avvio dell'operatività della PESD su nuovi fronti indussero l'UE a predisporre un quadro concettuale che permettesse di meglio definirne i

principi e le linee-guida, anche a fini di comunicazione esterna.³⁶ Nacque la “Strategia europea di sicurezza”, elaborata per la prima volta dal Segretario Generale/Alto Rappresentante Javier Solana ed adottata dal Consiglio Europeo il 12 dicembre 2003, sotto la Presidenza italiana. Si tratta di un compendio delle principali sfide globali e delle minacce più insidiose per la sicurezza dell’UE (terrorismo, proliferazione delle armi di distruzione di massa, conflitti regionali, Stati inefficienti o a rischio di “fallimento”, criminalità organizzata), e dei principali obiettivi da raggiungere per difendere la sicurezza dell’Unione e promuovere i valori europei, tra i quali quelli finalizzati a:

- affrontare le minacce con una politica di prevenzione e gestione dei conflitti, utilizzando mezzi civili e militari;³⁷
- irradiare all’esterno i caratteri fondamentali della sicurezza europea, partendo dalle aree più vicine (Medio Oriente, Balcani, Caucaso);
- promuovere un multilateralismo efficace, fondato sul diritto internazionale, in linea con la Carta delle Nazioni Unite, cooperando con la NATO e con le organizzazioni regionali.

In essa appare evidente l’esigenza di prevenire ed affrontare le situazioni di crisi sia attraverso le risorse PESC/PESD (da sviluppare adeguatamente, soprattutto in termini di capacità) e sia attraverso l’utilizzo coordinato di altri strumenti dell’Unione (come ad esempio, la cooperazione allo sviluppo gestita dalla Commissione)³⁸, in modo da incrementare l’efficacia dell’azione esterna UE nel suo complesso. I continui aggiornamenti della strategia dimostrano l’ineluttabilità di un adeguamento alle nuove sfide della sicurezza. Nel 2004 venivano fissati nuovi obiettivi sotto il profilo delle capacità militari (*si tratta dell’headline goal 2010*), tendente a coprire l’intero spettro delle possibili missioni di gestione di crisi UE, nell’ottica “ampliata” dalla Strategia Europea di Sicurezza del 2003. Tra le varie tappe del progetto, la creazione dell’Agenzia Europea per la Difesa, l’avvenuta

³⁶ Terzi di Sant’Agata G., *La Cooperazione Internazionale nel campo della sicurezza: l’Italia nelle principali organizzazioni multilaterali*, in *La Comunità Internazionale*, Fasc 1/2008, Editoriale Scientifica, Napoli.

³⁷ Quille G./, Gasparini G./, Menotti R./Pirozzi N., *Developing EU Civil Military Co-ordination: the role of the new Civilian Military Cell*, Joint Report by ISIS Europe and Ce.Mi.SS, giugno 2006, Bruxelles.

³⁸ European Parliament Report On The Role Of Nato In The Security Architecture Of The Eu (2008/2197(INI)), 28 January 2009.

realizzazione dei Battlegroups³⁹, la progressiva integrazione degli assetti di trasporto aereo strategico, lo sviluppo di nuove capacità di trasporto marittimo, lo sviluppo di un sistema di comunicazioni integrato, l'incremento quantitativo e qualitativo delle forze armate nazionali e lo sviluppo di adeguate sinergie tra le forze armate nazionali.

1.3.3 Rapporti UE-NATO

Per comprendere meglio i rapporti tra l'UE e la NATO occorre osservare che le due organizzazioni, da circa venti anni, procedono su una direttrice comune per quanto attiene ai membri comuni, e alla condivisione di alcuni obiettivi strategici. Entrambe svolgono un ruolo complementare e di reciproco sostegno per la tutela della pace e della sicurezza internazionale, in aderenza ai principi della Carta delle Nazioni Unite. Per quanto riguarda la partnership operativa, questa è stata confermata in una dichiarazione congiunta NATO-UE sulla PESD nel dicembre 2002 e poi formalizzata nel marzo 2003 con gli Accordi *Berlin Plus*. Gli Accordi *Berlin Plus* consentono all'UE di accedere alle capacità di pianificazione e di comando della NATO e di utilizzarne i mezzi per realizzare missioni di gestione delle crisi. Come è facilmente intuibile i vantaggi per l'UE sono enormi dal momento che si tratta di dispositivi e asset militari complessi e costosi. Finora, gli accordi *Berlin Plus* sono stati attivati due volte: in Macedonia, nel 2003 (Operazione Concordia), e in Bosnia, nel 2004 (operazione *Eufor Althea*), dove l'UE ha assunto la guida di missioni prima dirette dalla NATO, ma continuando a utilizzare la struttura di comando dell'Alleanza. Sotto il profilo istituzionale, la *partnership* si concretizza, seguendo una struttura definita "leggera" in:

- due incontri annuali a livello di Ministri degli Esteri e tre incontri tra i rappresentanti del Consiglio Atlantico e quelli del Comitato Politico di Sicurezza UE;
- riunioni congiunte per ogni turno semestrale di Presidenza dell'Unione Europea degli Ambasciatori accreditati rispettivamente presso il Consiglio Atlantico e il Comitato Politico e di Sicurezza dell'Unione Europea.

³⁹ Gruppi tattici dell'UE: si tratta di unità militari che aderiscono alla politica di sicurezza e di difesa comune dell'Unione europea.

- eventuali incontri dei Comitati militari delle due organizzazioni e riunioni periodiche di alcuni organi sussidiari
- infine da regolari incontri a livello di Ministri degli Esteri, Ambasciatori, Rappresentanti militari e consulenti di difesa.

Sotto il profilo organizzativo delle operazioni, viene data per acquisita la disponibilità (*presumption of availability*) a favore dell'Unione Europea di capacità e di assetti comuni e già individuati dalla NATO ai fini dell'impiego in operazioni a guida UE, in cui la NATO non sia direttamente impegnata. La supervisione su tali operazioni è attribuita al *Deputy Supreme Allied Commander Europe*,⁴⁰ parte integrante dello Staff militare dell'Alleanza atlantica. Sono altresì stabilite cellule di collegamento tra le due strutture militari a ulteriore garanzia del coordinamento tra le due organizzazioni. Futuri impegni per un reciproco sostegno. Sulla base del successo della cooperazione nei Balcani occidentali, gli ultimi vertici della NATO hanno espresso la necessità di migliorare gli strumenti di raccordo, evitando inutili duplicazioni e nel rispetto dell'autonomia delle due organizzazioni. Il nuovo Concetto strategico della NATO approvato nel Vertice di Lisbona ha fatto del rilancio dei rapporti tra la NATO e l'Unione europea un pilastro dell'azione dell'Alleanza per il prossimo decennio. Una più stretta cooperazione NATO-UE si pone come un ulteriore tassello per lo sviluppo di un "*Comprehensive approach*"⁴¹, un approccio globale internazionale alla gestione delle crisi (principio ribadito dal Vertice di Chicago del 2012) che richiede l'applicazione effettiva sia di strumenti militari che civili -come ad esempio succede in Afghanistan, dove il contributo dell'UE alla missione ISAF è finalizzato soprattutto al rafforzamento della statualità. Di conseguenza, sono state prese in considerazione nuove aree in cui le

⁴⁰ At the top of the ACO structure are the posts of Supreme Allied Commander Europe (SACEUR) supported by the Deputy Supreme Allied Commander Europe (DSACEUR) and the Chief of Staff (COS); all are 4 Star Generals. SACEUR's position is always assigned to the United States of America, while DSACEUR and COS posts are now permanently assigned to the United Kingdom and the Federal Republic of Germany respectively. SACEUR is also the commander of the US European Command (USEUCOM) with its Headquarters located in Stuttgart, Germany. <https://shape.nato.int/about/leadership-staff/command-group>

⁴¹ Il *Comprehensive Approach* sottolinea l'importanza dell'integrazione degli aspetti politici, economici, sociali, della sicurezza, dello sviluppo economico, dello stato di diritto, e umanitari, oltre a quelli propriamente militari, nella gestione delle moderne missioni, caratterizzate da una sempre crescente complessità, proprio per i numerosi fattori, tra loro connessi e interdipendenti. <https://www.analisedifesa.it/2021/02/il-comprehensive-approach-della-nato/#:~:text=Il%20Comprehensive%20Approach%20sottolinea%20,da%20una%20sempre%20crescente%20complessit%C3%A0%2C>

due organizzazioni possano incrementare la cooperazione, in particolare le questioni inerenti la sicurezza energetica e la difesa da attacchi informatici.

1.3.4 Il Trattato di Lisbona e la PSDC

Il 13 dicembre 2007 i Capi di Stato e di Governo dei 27 Stati membri siglarono a Lisbona un Trattato che modificò in parte sia quello dell'Unione Europea e sia quello della Comunità Europea. Il Trattato di Lisbona agevolò il funzionamento della PESC e della PSDC attraverso il miglioramento degli strumenti cosiddetti di flessibilità come emerge da una visione di alcuni suoi articoli. Tra questi merita di essere citato l'art. 28⁴² che estende la possibilità di interventi PSDC alle "operazioni congiunte di disarmo", ai "compiti di assistenza e consulenza militare", alla "stabilizzazione post-conflitto" ed alla "lotta contro il terrorismo"; ad essi vanno aggiunte le cd Azioni Congiunte e, in materia di disarmo, le missioni di Assistenza e di Ausilio in materia militare, le missioni di prevenzione dei conflitti e quelle di Stabilizzazione alla fine dei conflitti. Nel testo è evidenziato che tali operazioni sono potenzialmente in grado di contribuire alla lotta contro il terrorismo, comprese quelle per il sostegno a Paesi terzi per combattere il terrorismo sul loro territorio. Parimenti significativa può essere considerata l'introduzione della clausola di difesa reciproca, prevista dall'art. 42 paragrafo 7 del TUE;⁴³ una innovazione che consente agli Stati membri di portare il loro aiuto e la loro assistenza, con tutti i mezzi in loro potere, a qualsiasi Paese dell'Unione fosse oggetto di un'aggressione armata sul suo territorio. Lo stesso articolo 42 TUE

⁴² Art. 28: para 1. The Union shall comprise a customs union which shall cover all trade in goods and which shall involve the prohibition between Member States of customs duties on imports and exports and of all charges having equivalent effect, and the adoption of a common customs tariff in their relations with third countries. Para 2. The provisions of Article 30 and of Chapter 2 of this Title shall apply to products originating in Member States and to products coming from third countries which are in free circulation in Member States. http://www.lisbon-treaty.org/files/170-article-28_pfi2jcpbngqfksmc053m37.htm

⁴³ Art. 42: para 7. If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M042>

richiama e amplifica le competenze dell’Agenzia europea per la difesa, nata nel 2004, con le finalità di migliorare le capacità di difesa dell’UE nel settore della gestione delle crisi; di promuovere la cooperazione europea in materia di armamenti; di rafforzare la base industriale e tecnologica della difesa europea e creare un mercato europeo dei materiali di difesa che fosse competitivo, nonché di promuovere le attività di ricerca al fine di rafforzare il potenziale industriale e tecnologico dell’Europa in questo settore. Negli anni, La PSDC – si è andata via via rafforzando, pur restando parte della Politica Estera e di Sicurezza Comune. Lo dimostra la possibilità di disporre l’invio di forze militari e di polizia europee in aree di guerra per svolgere operazioni nella gestione delle crisi, nelle situazioni d’emergenza umanitaria e per il mantenimento e ristabilimento della pace. L’Unione si è dotata di una capacità di reazione militare rapida, basata sul concetto del “gruppo tattico”: il dispositivo si basa su due gruppi tattici in grado di consentire una pronta risposta militare per far fronte ad un’eventuale situazione di crisi. Composti da circa 1.500 uomini provenienti dai diversi Stati membri ed operativi per periodi di sei mesi, con un sistema a rotazione, le citate formazioni non stravolgono i principi di sovranità derivanti da un impiego delle forze armate su base sovranazionale proprio perché non si tratta di un esercito europeo, bensì di formazioni multinazionali organizzate e coordinate sulla base di un Trattato condiviso e approvato, secondo una formula che finora ha dato molte risposte nel solco di una politica condivisa. Certamente la Politica di Sicurezza e Difesa oggi è una realtà più concreta rispetto al passato, tuttavia spesso è evidente una mancanza di visione globale e, cosa ancor più incidente, risente dell’esistenza di una Alleanza Atlantica che troppo spesso si colloca in una posizione di leader assoluto vista la maggiore potenza degli apparati politici e militari a disposizione di quest’ultima. Il rapporto tra l’UE e la NATO nella risoluzione dei conflitti, nella gestione delle fasi successive agli stessi e negli interventi di ricostruzione e stabilizzazione è dunque uno degli aspetti che dovrà essere migliorato. Un complesso dibattito è tutt’ora in corso, avviato successivamente al Trattato di Lisbona nell’ambito del quale occorre trovare nuovi obiettivi che consentano di proiettare la PSDC verso il futuro.

1.4 Dal Trattato di Lisbona alla PESCO

1.4.1 Il Trattato di Lisbona e le sue implicazioni

L'articolazione del Trattato di Lisbona, entrato in vigore nel 2009, prevedeva sin dalle prime fasi, la graduale definizione di una *politica di difesa comune dell'Unione*; la possibilità di una *cooperazione strutturata permanente* nel settore della difesa; il rafforzamento della figura dell'*Alto Rappresentante* con funzioni di guida della politica estera e di sicurezza comune dell'Unione, di presidenza del Consiglio "*Affari esteri*" e con diritto di iniziativa per le decisioni relative alla politica di sicurezza e di difesa comune adottate dal Consiglio dell'UE. In particolare, la discussione sul rafforzamento della cooperazione nel settore della difesa subì una accelerazione tra il 2014 e il 2016 anche per il mutato contesto globale nei paesi del vicinato europeo dovuto a molteplici fattori quali l'esplosione di crisi e di conflitti in prossimità dei confini esterni orientali e meridionali dell'Europa (la crisi russo-ucraina), il persistere del conflitto in Siria (che ha avuto diverse implicazioni sui paesi limitrofi), nonché la perdurante instabilità in Libia. A ciò va aggiunto, il progressivo disimpegno da parte degli Stati Uniti nei confronti del continente europeo, a vantaggio di un ricollocamento delle loro priorità strategiche nel Pacifico. Numerose le missioni militari approvate dall'Unione Europea a partire dal 2003 (data dell'operazione "Concordia" in Macedonia che ha rappresentato la prima missione militare in attuazione agli accordi Berlin Plus. Tra queste, la missione EUTM in Somalia, intrapresa a seguito alla decisione del Consiglio UE n. 2010/197/PESC del 31 marzo 2010 relativa all'avvio della missione militare dell'Unione europea volta a contribuire alla formazione delle forze di sicurezza somale (EUTM Somalia)⁴⁴. Scopo principale della missione "*European*

⁴⁴ Council Decision 2010/197/CFSP of 31 March 2010, on the launch of a European Union military mission to contribute to the training of Somali security forces (EUTM Somalia): The Council Of The European Union, Having regard to the Treaty on European Union, and in particular Articles 28 and 43(2) thereof, Having regard to Council Decision 2010/96/CFSP of 15 February 2010 on a European Union military mission to contribute to the training of Somali security forces⁽¹⁾, and in particular Article 4 thereof, Having regard to the proposal by the High Representative of the Union for Foreign Affairs and Security Policy, Whereas: In its Resolution 1872 (2009) on the situation in Somalia, adopted on 26 May 2009, the United Nations Security Council (UNSC) stressed the importance of the re-establishment, training, equipping and retention of Somali security forces, and urged Member States and regional and international organizations to offer technical assistance for the training and equipping of the Somali security forces. In its Resolution 1897 (2009), adopted

Union Training Mission to contribute to the training of Somali security forces” è quello di contribuire all’addestramento delle Forze di sicurezza della Somalia in un periodo caratterizzato da una forte instabilità di quei territorio e nel contesto della Strategia Europea per il Corno d’Africa. Risultati apprezzabili sono stati raggiunti nel corso di questi anni come confermato dal Generale di Divisione Massimo Mingiardi, nel periodo 2014-2015 all’epoca Mission Commander della missione⁴⁵, nel corso di una intervista in annesso 1. Dalla fase iniziale caratterizzata da qualche criticità logistica (in quella fase la missione era dislocata in Uganda stante l’assenza di condizioni di sicurezza in Somalia dove solo successivamente sarebbe stata dislocata) si è quindi passati a un coordinamento di alto livello anche sotto il profilo operativo, nonostante la co-presenza di personale provenienti da Paesi non NATO. Quest’ultimo aspetto è stato curato personalmente dal Comandante che è riuscito ad amalgamare le varie componenti nazionali della missione, uniformandone le procedure e sviluppando mirate attività con le quali alcuni contingenti si trovavano ad operare per la prima volta. L’addestramento di 2500 militari somali, già nel primo anno di missione rende l’idea del raggiungimento di obiettivi di tutto rispetto. L’esperienza sul campo, anche in questo caso ha portato ad una valutazione complessiva del contesto “missioni UE” in virtù della quale è possibile affermare che nonostante le intenzioni, ci sono oggettive difficoltà nel portare avanti operazioni di questo genere. L’aspetto dell’autonomia, in particolare, rappresenta un punto cruciale sul quale lavorare perché nella pratica è pressoché costante rilevare come a volte in assenza di una unità decisionale e di una mancata unanimità in scelte prioritarie, lo stesso processo decisionale possa subire ritardi o bruschi arresti. A conclusione dell’intervista, il Gen. Mingiardi ha sottolineato come uno strumento militare, va certamente adeguato alle nuove sfide senza

on 30 November 2009, the UNSC recalled its previous resolutions and reaffirmed its respect for the sovereignty, territorial integrity, political independence and unity of Somalia. By letter dated 5 January 2010, the Minister of Defence of Uganda welcomed the Union's envisaged mission in support of the Somali security sector and invited the Union to participate in the training of Somali security forces in Uganda for a period of at least one year. Decisione n. 2010/197/PESC del 31 marzo 2010 <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32010D0197&from=EN>

⁴⁵ The EU's military training mission for Somalia (EUTM Somalia) has started its first “Train the Trainers” course at the Jazeera Training Camp in Mogadishu. The previous day, EUTM Somalia's new Mission Commander, Brigadier General Massimo Mingiardi, was appointed by the Political Security Committee.

tralasciare gli aspetti fondamentali, costituiti da addestramenti altamente professionali, equipaggiamenti all'avanguardia e grandi capacità motivazionali.⁴⁶

1.4.2 La nuova Strategia Globale

Da questo mutamento cominciò a delinearsi la nuova *Strategia globale*, presentata al Consiglio europeo del 28 e 29 giugno 2016 dall'Alto Rappresentante, Federica Mogherini, che pur riconoscendo il ruolo della NATO per la difesa collettiva, affermò che l'UE avrebbe dovuto dotarsi di una capacità ed autonomia strategica sia per contribuire all'Alleanza atlantica sia per agire autonomamente se e quando necessario. I meccanismi di tale strategia furono riassunti in tre direttrici che vennero così sintetizzate:

- Il piano di attuazione per la sicurezza e difesa, presentato il 14 novembre 2016, focalizzato sui profili politico e militari della cooperazione europea;
- Il piano di azione per la difesa europea (European Defence Action Plan – EDAP) presentato dalla Commissione europea il 30 novembre 2016, incentrato sul rilancio di una industria della difesa europea;
- La dichiarazione congiunta UE-NATO sul rafforzamento della cooperazione in materia di sicurezza e difesa, adottata a margine del Vertice NATO di Varsavia del luglio 2016.

Il piano di attuazione della Strategia globale per la sicurezza e difesa

Si tratta di un programma comprendente una serie di azioni sinergiche e tra queste:

- rivedere le priorità e gli ambiti delle missioni civili e rafforzare la capacità di gestione delle crisi civili in ambito di PSDC;
- riconfigurare una procedura di revisione coordinata annuale sulla difesa (CARD) coordinata dall'Agenzia Europea per la Difesa (EDA) da parte degli Stati membri, funzionale ad aiutare questi ultimi a sincronizzare i loro bilanci per la difesa, a pianificare insieme i loro investimenti futuri e a evitare duplicazioni;

⁴⁶ 06.01.2022: annesso 1 - intervista al Generale di Divisione Massimo Mingiardi

- potenziare le strutture di analisi, pianificazione e controllo delle missioni dell'UE condotte in ambito PSDC, in particolare rafforzando le sinergie tra le missioni civili e quelle militari;
- migliorare il coordinamento delle capacità europee di intelligence, attraverso il centro situazionale e valutazione di intelligence (INTCEN);
- fare un migliore utilizzo delle esistenti strutture di comando e forze multinazionali già presenti in Europa (come ad esempio le forze *Eurocorps* di Belgio, Francia, Germania, Lussemburgo e Spagna), rafforzando le capacità di comando e controllo;
- migliorare le potenzialità della forza europea di reazione rapida e dei gruppi tattici dell'UE (*EU-Battlegroups*);
- rivedere le forme di finanziamento comune delle azioni condotte nell'ambito della PESC, in particolare con una revisione del meccanismo *Athena* che gestisce il finanziamento dei costi comuni delle operazioni militari;
- favorire il ricorso alla cooperazione strutturata tra gli Stati membri desiderosi di contribuire alla PSDC;
- definire un approccio più strategico nella cooperazione PSDC con paesi partner che condividono gli stessi valori dell'UE desiderosi di partecipare alle missioni.

Il Piano d'azione per la difesa europea

Si incentra sui profili industriali della difesa europea, si articola su tre assi principali:

- l'istituzione di un Fondo europeo per la difesa; presentato il 13 giugno 2018 dalla Commissione europea quale proposta di regolamento volto a migliorare la competitività, l'innovazione, l'efficienza e l'autonomia dell'industria della difesa dell'Unione, mediante il sostegno alla cooperazione transfrontaliera tra gli Stati membri e tra imprese, centri di ricerca, amministrazioni nazionali, organizzazioni internazionali e università nella fase di ricerca sui prodotti e sulle tecnologie della difesa;
- la promozione di investimenti nelle catene di approvvigionamento della difesa attraverso l'accrescimento delle sinergie e della sincronizzazione della spesa di bilancio; la previsione di una equa ripartizione dei costi e dei rischi;

l'esclusione dei vincoli di finanziamento nell'ambito della catena di approvvigionamento;

- il rafforzamento del mercato unico della difesa, con misure volte a sostenere l'accesso al mercato transfrontaliero delle PMI e dei subcontraenti, nonché ad agevolare la loro integrazione nelle catene di approvvigionamento, da attuare attraverso una riduzione della frammentazione e il miglioramento delle funzionalità del mercato; l'offerta di un sostegno nell'ambito dei Fondi strutturali e di investimento europei o di programmi UE gestiti in modo centralizzato; l'agevolazione dell'accesso ai finanziamenti della Banca europea per gli investimenti (BEI), del Fondo europeo per gli investimenti e di altri attori.

La dichiarazione congiunta UE-NATO

l'UE e la NATO, al termine del vertice NATO dell'8 e 9 luglio 2016 in Polonia, hanno sottoscritto una dichiarazione congiunta sull'intensificazione dei rapporti attraverso iniziative di cooperazione nei seguenti settori:

- contrasto alle minacce ibride, anche mediante l'elaborazione di procedure coordinate;
- cooperazione operativa in mare e in materia di migrazione;
- coordinamento nella cybersicurezza e nella difesa;
- sviluppo di capacità di difesa coerenti, complementari e interoperabili;
- agevolazione di un'industria della difesa più forte e di una maggiore ricerca nel settore;
- potenziamento del coordinamento relativo alle esercitazioni;
- supporto alle capacità di difesa e sicurezza dei partner a est e a sud.

Successivamente, il 5 dicembre 2017, Il Consiglio dell'UE ha adottato delle conclusioni nelle quali ha approvato nuove iniziative di cooperazione con la NATO, comprendenti aspetti quali l'antiterrorismo, la cooperazione donne, pace e sicurezza e la mobilità militare. Il 10 luglio 2018, l'UE e la NATO hanno firmato una nuova dichiarazione congiunta, che integra le precedenti, e nella quale si indica che l'UE e la NATO concentreranno la propria cooperazione in settori quali: mobilità militare; cybersicurezza; minacce ibride; lotta al terrorismo; donne, pace e sicurezza.

1.4.3 La Cooperazione Strutturata Permanente PESCO

Il Consiglio dell'Unione europea, con la decisione dell'11 dicembre 2017, ha istituito una cooperazione strutturata permanente (PESCO) in materia di difesa, cui partecipano 25 tra gli Stati membri. La decisione era stata preceduta, da una notifica degli Stati partecipanti al Consiglio e all'Alto rappresentante, proposta da Francia, Germania, Italia e Spagna e firmata da 23 paesi a margine del Consiglio Affari esteri del 13 novembre dello stesso anno. Il Portogallo, inizialmente escluso ancorché membro NATO, ha notificato la sua intenzione di aderire, il successivo 7 dicembre a seguito del voto favorevole del Parlamento, e così l'Irlanda. È una forma di cooperazione rafforzata specifica per l'ambito della difesa introdotta dal trattato di Lisbona, entrato in vigore nel 2009, che a sua volta ha ripreso integralmente le norme introdotte nel trattato costituzionale del 2004, mai ratificato. Non si trattò quindi di un istituto di nuova concezione, ma strettamente legato all'epoca in cui stava nascendo una dimensione europea della difesa, sotto il profilo dello svolgimento di missioni e operazioni militari da parte dell'Unione (al riguardo si rimanda alla Dichiarazione di Saint-Malo del 1998). La PESCO si differenzia dall'istituto generale della cooperazione rafforzata di cui agli articoli 326 e seguenti del trattato sul funzionamento UE, oltre che per l'oggetto specifico (Difesa), soprattutto per il fatto che per la sua istituzione non è richiesta l'unanimità dei voti nel Consiglio ma solo la maggioranza qualificata così come non è richiesto un numero minimo di partecipanti. Prima che se ne prospettasse una configurazione modulare e inclusiva, era interpretata come un oggetto diverso da quello attuale. Anche in considerazione del contesto nel quale le norme erano state concepite, veniva vista come uno strumento tale da consentire ad un'avanguardia di Stati decisi a farlo (*willing*), ma anche dotati delle necessarie capacità (*capable*), di avviare un cammino di integrazione nell'ambito della difesa nell'ottica dello svolgimento in comune di missioni e operazioni militari. Tuttavia, al momento della stesura definitiva è stata abbandonata la visione legata a un gruppo ristretto di paesi proiettati verso un nucleo di difesa comune, preferendo una strutturazione molto più istituzionale, tendenzialmente aperta a tutti i membri, per realizzare in comune progetti in materia di difesa. Non è stato quindi posto nessun requisito di accesso, se non la sottoscrizione di memorandum

comprensivo di 20 impegni, come richiesto dall'articolo 42 del Trattato UE. Ogni paese è stato lasciato libero di decidere a quali progetti aderire, posto l'obbligo di prenderne parte ad almeno uno di essi, adattando la propria partecipazione al livello ritenuto più opportuno. Fino all'ultimo, le posizioni degli Stati membri sono state differenziate. Francia e Germania puntavano a una PESCO particolarmente ristretta e aderente alla sua concezione iniziale, mentre molti Stati piccoli temevano una cooperazione troppo incentrata sull'asse franco-tedesco. L'Italia e la Spagna, prediligevano un nucleo forte dei quattro grandi cui potessero aggiungersi altri partner minori purché riunissero le capacità *willing and capable*. L'ampio consenso ha però fatto sì che, per non rimanerne esclusi, aderissero anche ulteriori paesi, come la Polonia o l'Irlanda, che non avevano mostrato particolare interesse. Tra la notifica del 13 novembre e la decisione dell'11 dicembre 2017 ogni Stato membro partecipante ha potuto presentare un Piano nazionale di attuazione (*National implementation plan*), con il quale ha esposto la propria capacità di soddisfare i singoli impegni, indicandone il contributo nazionale previsto per la fase 2019-2021 e, se ritenuto opportuno, anche per la fase 2022-2025. In quella sede sono anche stati proposti 17 progetti rispetto ai quali gli Stati membri si sono offerti come capofila, che spaziano dalla costituzione di nuovi Comandi settoriali unificati, alla creazione di hub logistici e operativi, nonché a Centri di Eccellenza su tematiche strategiche, Centri per la Formazione per le missioni e le operazioni internazionali e Scuole di intelligence. L'Italia ha deciso di inserirsi quale capofila di quattro progetti ma si è riservata di valutare la partecipazione a molti altri. La procedura di approvazione di un singolo progetto (o dei progetti) prevede una iniziale proposta da parte di un gruppo di Stati membri e una conseguente approvazione unanime del Consiglio. Tale decisione può essere preceduta da una raccomandazione dell'Alto rappresentante, che deve a sua volta acquisire il parere del Comitato militare UE (EUMC) e basarsi sulla valutazione che del progetto faranno, il Servizio europeo di azione esterna (SEAE) e l'Agenzia europea per la difesa (EDA), a seconda che il progetto riguardi aspetti operativi ovvero di sviluppo delle capacità.

1.4.4 La Revisione Strategica della PESCO

Gli avvenimenti che hanno caratterizzato gli ultimi anni hanno certamente rimodulato le esigenze e le priorità in gran parte dei settori strategici. Tuttavia, il Consiglio europeo riunitosi il 20 novembre 2020 ha segnato un punto di svolta nella Difesa europea: in quella sede è stato approvato il documento relativo alla Revisione Strategica della PESCO allo scopo di favorirne l'ingresso in una fase denominata "fase2" per il periodo 2021-2025. Avviato anche il processo di elaborazione dello *Strategic compass* (per una visione condivisa delle principali minacce e della capacità di farvi fronte), nonché l'implementazione dello Strumento europeo per la pace che ha lo scopo di facilitare il finanziamento delle missioni militari. Discussa anche la revisione della struttura di Comando e controllo delle missioni militari, significativo passo verso la formazione di un vero e proprio Consiglio di Difesa UE. Resta sostanzialmente comune la posizione del gruppo PESCO 4 (Germania, Francia, Italia e Spagna) seppure vi siano divergenze di non poco conto tra la Germania che ha ribadito in più sedi, l'indispensabilità di legarsi agli Stati Uniti e quindi alla NATO, a differenza della Francia che continua a sostenere un approccio che renda "sovrana" la politica di difesa UE, svincolata quindi da altri contesti atlantici. Per la seconda fase, il Consiglio prova dunque a tener conto dell'esperienza maturata in questi anni ponendosi quale obiettivo quello di superare i limiti mostrati nella sua prima fase attuativa. È certamente necessaria una razionalizzazione dei progetti esistenti; rivista anche la scansione temporale del ciclo di programmazione per i progetti futuri, nell'ottica di ridurre il numero a fronte di un aumento della qualità. A tal scopo sono stati selezionati alcuni dei progetti già approvati, che sono considerati suscettibili di produrre risultati concreti entro il 2025. Siamo di fronte a un quadro in evoluzione e la Politica di Difesa europea si mostra ancora una volta come una figura poliedrica che non ha ancora raggiunto una sua definizione in termini di aspetto e di sostanza. Determinante, per il suo futuro, una "consapevole" scelta dei paesi che prima ancora di discutere di difesa comune devono "consapevolmente" coordinarsi per una visione di politica globale che, al momento non sembra essere del tutto compiuta.

1.5 La PSDC nell'Europa dei 27

1.5.1 La Brexit

Trascorsi ventitré anni dal vertice di Saint-Malo del 1998, sono riemerse le perplessità di quel periodo circa la possibilità di una difesa europea irreversibile e sulla sua autonomia. Quel che è certo è che dal 31 gennaio 2020 il Regno Unito, uscito dall'Unione Europea, ha posto una serie di quesiti su come la PSDC saprà adattarsi facendo a meno di un partner che, da solo, costituiva il 20% delle capacità globali della Difesa. É un dato di fatto che Londra non ha mai illuso circa l'offerta di queste capacità ai partner del vecchio continente e ciò per vari motivi, primo fra tutti il fatto che, per certi aspetti le sue forze armate sono perfettamente integrate con quelle statunitensi; ma andando oltre, il concetto più ampio di "sicurezza" del Regno Unito è intimamente legato ai rapporti con gli Stati Uniti. Lo dimostrano le cooperazioni privilegiate nel settore nucleare, nelle tecnologie emergenti, nella produzione degli armamenti e in quella dell'intelligence e delle hybrid warfare. Certamente la fiducia viene riposta al mantenimento in costanza di valore, di stabili e positivi rapporti economici auspicati da chi resta nel circuito, tassello cruciale per la predisposizione di cooperazione in materia di politica estera e di difesa, ma molti degli oneri dovranno essere assunti dalla Francia, l'unica in grado di sopperire al momento, ma solo in parte, al ruolo del Regno Unito per l'ampio spettro di capacità tecnico-tattiche sia in ambito convenzionale e sia in ambito nucleare. Proseguirà nel solco della collaborazione tra Londra e Bruxelles la partecipazione britannica ai bandi dell'EDF (European Defence Found) e ai progetti PESCO già intrapresi. Sostanzialmente, il rispetto della Letter of Intent del 2000, i contatti con l'Agenzia di Difesa Europea e i principi siglati con l'Organizzazione congiunta in materia di armamenti, dimostrano come sia possibile proseguire con una collaborazione meno scontata ma più razionale.⁴⁷

⁴⁷ <https://www.consilium.europa.eu/it/press/press-releases/2022/11/15/pesco-the-uk-will-be-invited-to-participate-in-military-mobility-project/>

1.5.2 Il Trattato di Aquisgrana/Aachen (Francia-Germania)

Il 22 gennaio 2019 Germania e Francia hanno siglato il nuovo trattato franco-tedesco, rinnovando e completando in tal modo il Trattato dell'Eliseo firmato da Adenauer e De Gaulle nel 1963. Questa volta ad Aquisgrana (la tedesca Aachen) erano presenti la cancelliera tedesca Angela Merkel e il presidente della Repubblica francese Emmanuel Macron che suggellano una linea comune intrapresa da più di cinquant'anni.

“Acknowledging the historic achievement of the reconciliation of the German and French peoples to which the Treaty between the Federal Republic of Germany and the French Republic of 22 January 1963 on Franco-German cooperation has made an exceptional contribution and which has been the foundation for an unprecedented network of bilateral relations between their civil societies and public bodies at all levels, Convinced that the time has come to take their bilateral relations to the next level and prepare for the challenges that the two countries and Europe face in the 21st century and aiming to further the convergence of their economies and social models, promote cultural diversity and bring their societies and citizens closer together, Convinced that the close friendship between Germany and France has been decisive for a united, efficient, sovereign and strong European Union and continues to be an indispensable element”

Il trattato, strutturato su 28 articoli è finalizzato a incrementare le relazioni tra i due Paesi così come meglio si intravede dalla sintesi del documento visionabile sul sito del Ministero degli Esteri Tedesco:

- La messa in comune delle regole e degli apparati di sicurezza. Entrambi i paesi svilupperanno le loro capacità militari e le forze di impiego collaboreranno in modo più stretto. I due paesi si accordano su regole comuni in materia di esportazione di armi. Un consiglio bilaterale per la difesa e la sicurezza fungerà da orientamento. L'obiettivo è di sviluppare una presenza in Africa attraverso l'aiuto al settore privato.

The two countries shall endeavour to build an ever closer partnership between Europe and Africa by strengthening their cooperation in private sector development, regional integration, education and vocational training, gender equality and women's empowerment, with the aim of improving social and economic prospects, sustainability and good governance, as well as crisis prevention and conflict

management, including through peacekeeping, and managing post-conflict situations. The two countries shall establish an annual dialogue at the political level on international development policy to intensify the coordination of policy planning and implementation.

- Germania e Francia vogliono sviluppare una posizione comune nel contesto delle Nazioni Unite e si impegnano per una riforma del Consiglio di Sicurezza dell’Onu. In tale contesto la dichiarazione comune stabilisce che l’assegnazione di un seggio permanente alla Germania rappresenta una priorità per Parigi.

- Un programma di cooperazione sarà inteso a sviluppare l’interscambio tra i giovani dei due paesi. Uno speciale comitato, il “Laboratorio per il futuro”, composto da sociologi, scienziati e intellettuali, viene istituito per considerare le necessità di cambiamento delle due società.

The two countries acknowledge the decisive role played by culture and the media in strengthening the Franco-German friendship. They are therefore determined to create a common space of freedom and opportunity for their peoples, as well as a common cultural and media space. They shall expand mobility and exchange programmes between their countries, especially for young people within the framework of the Franco-German Youth Office, and set quantifiable targets in these areas. In order to promote ever closer relations in all fields of cultural expression, including through integrated cultural institutes, they shall set up specific programmes and a digital platform, geared to young people in particular.

- Un’attenzione particolare viene dedicata alle zone di confine, teatro in passato di continui combattimenti. Verrà introdotto un regime di bilinguismo e di sviluppo delle vie di comunicazione, a cominciare da ferrovie e autostrade. Inoltre uno speciale regime di facilitazione dell’attività di impresa dovrebbe ridurre gli ostacoli burocratici all’integrazione delle regioni confinanti. Anche in questo caso viene istituito uno speciale comitato che dovrebbe produrre le soluzioni più convenienti l’integrazione transfrontaliera.

The two countries acknowledge the importance of cross-border cooperation between the Federal Republic of Germany and the French Republic in order to foster closer ties between citizens as well as businesses on both sides of the border, including the essential role of local authorities and other local actors in this respect. They intend to facilitate the removal of obstacles in border regions with a view to

implementing cross-border projects and to simplify the daily lives of people living in border regions.

1.5.3 L'era COVID-19

Germania e Francia sono due paesi molto diversi per forma di governo, gestione strategica del proprio futuro, apparati militari e assetti economici, tuttavia hanno finora dimostrato che possono entrambi beneficiare di un asse preferenziale che si perpetua da decenni. Entrambi consapevoli delle difficoltà intrinseche di quell'Europa che finora ha dato prova di non essere un attore internazionale e di non parlare con un'unica voce e allo stesso livello con le altre potenze, hanno finora proceduto molto pragmaticamente su percorsi condivisi, non disdegnando di ostacolare gli altri partner nei settori da loro ritenuti più strategici. Che lo si chiami "motore dell'Europa" o "nocciolo duro" o "asse Franco-Tedesco" poco importa poiché sono tanti ormai gli esempi riguardanti politiche economiche, bancarie e obiettivi strategici internazionali che vedono privilegiare i loro interessi su binari di opzioni/concessioni difformi a quelli cui sono tenuti gli altri partner europei. L'impatto del Covid-19 ha fatto emergere delle vulnerabilità da parte di una Unione Europea che non ha saputo dare una risposta univoca nell'immediato ed ha tentato di rimediare elaborandone una successiva, caratterizzata dalle consuete diversità di ambito ma soprattutto gravata da una ambiguità di fondo che da sola basta a delineare la debolezza principale: il ricorso a istituti di credito macchinosi, vincolanti e diversificati tra partner che non sembrano godere del medesimo trattamento (a distanza di due anni restano comunque dei proclami). Vi è sostanzialmente una incertezza globale che al momento non appare superabile. L'Unione Europea dovrà rinsaldare il legame con la NATO, riproporsi quale attore affidabile a livello internazionale, portare a compimento la ristrutturazione dell'industria Difesa e recuperare i gap derivanti dalla Brexit. Parlare di autonomia strategica è certamente un modo per promuovere i propri valori e, contestualmente portare avanti una governance globale caratterizzata dal multilateralismo e dalla cooperazione: la Politica di Sicurezza e Difesa è destinata ad una trasformazione complessa e durevole. Si assiste oggi a una ridefinizione geopolitica internazionale all'interno della quale l'Unione Europea ha necessità di ritrovare una propria affermazione. Ovviamente l'integrazione della Difesa è un

passaggio obbligatorio senza il quale non è possibile neppure ipotizzare una “*autonomia strategica europea*” concetto che spesso crea confusione proprio perché non riguarda solo ed esclusivamente l’approccio difensivo ma tutta una serie di correlazioni con i settori economici, industriali, i rapporti con gli altri Paesi, in un’ottica cioè molto più complessa e per ciò stesso, problematica. L’opzione di puntare sulla *sovranità tecnologica e digitale*. potrebbe essere un aspetto qualificante dal momento che si tratta di problematiche da molto tempo al centro dei principali cambiamenti geopolitici internazionali. Una crescita tecnologico-digitale deve tuttavia essere accompagnata da una adeguata regolamentazione che sappia contemperare investimenti tecnologici e regolamentazione in settori sempre più di interesse quali gli algoritmi e l’intelligenza artificiale.⁴⁸ Analogamente si dovrebbe affrontare il nodo di ciò che si vuole ottenere quando si parla di autonomia strategica dal momento che la gestione dei rapporti internazionali con Stati terzi, ad esempio, è un passaggio molto delicato nei rapporti U.S.A./Russia/Cina per le innumerevoli implicazioni che riveste.⁴⁹ Sostanzialmente, potrebbe essere interessante perseguire una scelta contraddistinta da due direttrici che si completano: una “autonomia strategica europea per la difesa e l’azione esterna” che riprenda la *PSDC/PESC*, adeguandola alle esigenze contingenti e una “autonomia strategica tecnologica e industriale europea” che permetta di sviluppare l’agenda della sovranità tecnologica, obiettivo di comune interesse.⁵⁰

1.5.4 Il Trattato del Quirinale (Francia-Italia)

Il 26 novembre 2021, a Roma, il Presidente del Consiglio Mario Draghi e il Presidente francese Emmanuel Macron, alla presenza del Presidente della Repubblica Italiana Sergio Mattarella e del Ministro degli Esteri Luigi Di Maio hanno firmato il trattato "per una cooperazione bilaterale rafforzata" tra i due Paesi.

⁴⁸ Picchiarelli A., “Per un’intelligenza artificiale a misura d’uomo: una possibile regolamentazione valoriale?”, in *IAI Papers*, n. 20|47 (dicembre 2020), <https://www.iai.it/it/node/12578>.

⁴⁹ Lamberth M., Rasser M., “A Solid Plan to Compete with China in Artificial Intelligence”, in *Defense One*, 1 marzo 2021, <https://www.defenseone.com/ideas/2021/03/solid-plan-compete-china-artificial-intelligence/172360>.

⁵⁰ Darnis J.P.: *The European Union between strategic autonomy and technological sovereignty: impasses and opportunities in Recherches & Documents - Fondation pour la recherche stratégique - N°10/2021 - April 2021*

Noto anche con il nome di "Trattato del Quirinale", l'accordo appare sia come la concretizzazione di un rapporto di grande intensità sotto il profilo economico, sia come punto di partenza per una più proficua partnership politico istituzionale. Storicamente il Trattato ha origini da una idea enunciata nel 2017, in occasione del vertice di Lione, per poter disporre di meccanismi di consultazione bilaterale, in una fase storica molto particolare in cui, subito dopo gli inizi della presidenza Macron, si erano registrati alcuni episodi di tensione tra Parigi e Roma su varie tematiche, tra le quali il caso Libia, la gestione dei flussi migratori e le rivalità economiche su asset strategici. I lavori così intrapresi, subirono delle fasi di rallentamento nel 2018 e 2019 (in conseguenza a episodi e prese di posizioni politiche reciproche molto forti), fino a registrare una improvvisa accelerazione con l'arrivo del Presidente del Consiglio Mario Draghi, nel mese di febbraio 2021. Gli iniziali parallelismi con il Trattato tra Francia e Germania non hanno trovato conferma con il passare del tempo, né nella fase iniziale, caratterizzata da una concreta segretezza degli ambiti e dei punti focali inseriti, e né in quella successiva al passare del tempo e con l'emergere di qualche particolare sul contenuto seppur molto nebuloso, trattandosi di un Trattato rimasto segreto per i primi anni e svelato nella sua parte testuale (ma non del tutto). Se si valuta il profilo delle convenienze reciproche occorre sottolineare che esso nasce in un momento storico in cui nell'Unione Europea è pressante la richiesta di maggiore assunzione di responsabilità almeno da parte dei Paesi di maggior peso che vada al di là del consueto asse franco-tedesco, formalizzato nel Trattato del 1963 e aggiornato con il successivo di Aquisgrana del 2019. Interessi e sensibilità diverse sono la costante nei rapporti tra la Germania e la Francia e in tal senso il Trattato tra i due si pone in un'ottica compensativa che, sostanzialmente sia in grado di temperare le divergenze e le esigenze di supremazia reciproche. È del tutto evidente però che nel caso citato ci sia una prevalenza di Berlino nei confronti dei francesi che invece, nel caso del confronto con l'Italia assumono il ruolo opposto ovvero esercitano una supremazia già sperimentata e consolidata in ambito geopolitico nei suoi risvolti strategici militari ed economici anche recenti. In astratto quindi potrebbe rivelarsi utile tutta quella serie di meccanismi "ipotizzati" dal Trattato del Quirinale che prevede un dialogo funzionale in diversi settori di collaborazione e su più livelli, fino a prevedere partecipazioni incrociate nei rispettivi Consigli dei

Ministri.⁵¹ Tuttavia, una visione accurata non può prescindere dall'osservare che si fonda tra due Paesi profondamente diversi anche in termini di modelli. Da una parte ci troviamo la Francia, caratterizzata da un accentramento della struttura istituzionale e con un modello di pubblica amministrazione efficiente e per certi versi all'avanguardia. Nel caso dell'Italia si predilige il decentramento e l'amministrazione pubblica è in costante trasformazione nell'ottica di un rinnovamento che stenta a concretizzarsi. I rischi circa un'eventuale prevalenza di una delle due parti potrebbero sorgere anche da questi aspetti. L'esistenza di un Trattato Germania-Francia e di uno tra Italia e Francia ha generato varie ipotesi circa un futuro Trattato tra Germania e Italia che al momento non è neppure in una fase embrionale e che idealmente sarebbe servito a chiudere in una sorta di triangolazione, le due segmentazioni pattizie citate, ma da più parti viene ricordato che sono profondamente diversi i rapporti di forza tra i due e che la Germania non sembra avere molti interessi a strutturare accordi in tal senso. Una rapida analisi ad alcuni articoli dello stesso, mettono in evidenza molti dubbi circa le motivazioni sottese e soprattutto ritorna il rapporto di forza tra il nostro Paese e la Francia che non ha mai nascosto una tangibile supremazia in molti settori.

Articolo 1, paragrafo 3: *“Riconoscendo che il Mediterraneo è il loro ambiente comune, le Parti sviluppano sinergie e rafforzano il coordinamento su tutte le questioni che influiscono sulla sicurezza, sullo sviluppo socio-economico...esse s'impegnano altresì a favorire un approccio comune europeo nelle politiche con il Vicinato Meridionale e Orientale”*. Circa l'espressione *approccio comune europeo* ci si interroga affinché essa non si intenda unicamente quale imposizione degli obiettivi geopolitici francesi rispetto all'Italia; il riferimento ovviamente è rivolto all'ambito della politica estera mediterranea, dove spesso gli interessi dei due Paesi si sono trovati in collisione, con inevitabile supremazia di quella francese.

Articolo 2, paragrafo 7: *“Le Parti si impegnano a facilitare il transito e lo stanziamento delle forze armate dell'altra Parte sul proprio territorio”*. Di elevata delicatezza, questa disposizione non è stata del tutto esplicitata a livello istituzionale e pertanto lascia inevitabilmente spazio a più interpretazioni e a molti

⁵¹ Massolo G. Italia-Francia: un messaggio per Bruxelles, ISPI online, novembre 2021
<https://www.ispionline.it/it/pubblicazione/italia-francia-un-messaggio-bruxelles-32470>

dubbi. Sorgono lecite perplessità circa la necessità che le rispettive forze armate possano “transitare” o addirittura “stanzarsi” in uno dei due territori in un contesto militare che indubbiamente vede la supremazia di una delle due parti rispetto all’altra. Con uno sforzo di creatività è stato proposto in tale contesto un parallelismo con una parte del Trattato dell’Eliseo e più precisamente al Titolo II, sezione B “*Défense*”, art. 2) che tuttavia parla di: “...*détachements temporaires d’unités entières*”. È fin troppo chiaro come il riferimento sia a formazioni militari congiunte, un concetto completamente diverso rispetto a quello prima enunciato. Formazioni comuni che non vengono più neanche menzionate nel rinnovato Trattato del 2019 dove agli artt. 4.1 e 4.3 si parla di principio di sicurezza collettiva e reciproca assistenza in caso di aggressione armata nei confronti di uno dei due partner, nonché di cooperazione fra le due forze armate per operazioni congiunte. Articolo 10, circa la “*Cooperazione transfrontaliera*”.

- paragrafo 1: “*La frontiera italo-francese costituisce un bacino di vita interconnesso, in cui le popolazioni italiana e francese condividono un destino comune*”.
- paragrafo 2: “*Le Parti...sostengono i progetti che favoriscono l’integrazione di questo spazio*”.
- paragrafo 3: “*Le Parti approfondiscono la loro cooperazione in materia di sicurezza, in particolare attraverso scambi di personale e favorendo la realizzazione di operazioni comuni o coordinate*”.
- paragrafo 5: “*Le Parti favoriscono la formazione dei parlanti bilingue in italiano e in francese nelle regioni frontaliere, valorizzando in tal modo l’uso delle due lingue nella vita quotidiana*”.

Una integrazione così genericamente prospettata è certamente suscettibile di avere un peso e un bilanciamento a favore di una delle due parti e non è chiaro chi dei due può trarne il maggiore vantaggio. Lo stesso può dirsi per quanto concerne la cooperazione in materia di sicurezza, un punto fondamentale di dottrine europee e NATO che in questo caso troverebbe un “frazionamento” anomalo e soprattutto in contrasto con il rinnovato impegno ad agire secondo schemi e standardizzazioni ai più alti livelli.

Articolo 12, paragrafo 3: “*Il trattato ha durata indeterminata, fatta salva la facoltà di ciascuna Parte di denunciarlo con un preavviso di almeno dodici mesi per via*

diplomatica...Tale denuncia non mette in causa i diritti e gli obblighi delle Parti derivanti dai progetti avviati nel quadro del presente Trattato". Si deduce il principio per cui gli effetti pratici della stipula di questo accordo potrebbero non finire mai. Per analogia, è possibile immaginare che alcuni accordi di natura economica potrebbero impegnare l'Italia, anche di fronte a un netto vantaggio competitivo per la Francia, persino ad anni di distanza da un'eventuale denuncia del trattato. Ci si potrebbe poi chiedere quali siano, oltre a quelli di natura economica, gli eventuali altri «progetti avviati nel quadro del» trattato. Nel Policy Brief 39/2021 dal titolo "Il trattato del Quirinale, può rilanciare l'Italia in Europa" edito dalla LUISS School of Government, Jean-Pierre Darnis è convinto che nonostante i dubbi e le perplessità interpretative di alcuni passaggi, vi sono margini concreti affinché il nostro Paese possa trarre i massimi vantaggi dal Trattato in esame. Secondo Darnis infatti la posta in gioco è la seguente: "...sancire un nuovo corso politico di convergenza fra i due Paesi nell'ambito dell'Unione europea e favorire ulteriori forme di cooperazione, meccanismi in grado di sfruttare e governare assieme una fase di straordinaria crescita comune, ovvero un gioco a somma crescente nel quale le sinergie sono premiate e incentivate". La prospettiva per il nostro Paese è quella di guadagnarne in agilità e peso specifico negoziali rispetto ad altri partner.⁵² È ancora presto per valutare la portata e le sfaccettature di questo Trattato sul quale insistono alcune perplessità, alcune delle quali generate dall'altissimo livello di segretezza che ha accompagnato le fasi preparatorie da parte del "gruppo dei saggi" italiano, alcuni dei quali molto a contatto con Parigi in ragione di incarichi professionali anche istituzionali nel governo francese. Molti dubbi derivano dalla prevista presenza militare reciproca nei rispettivi territori, dalla compartecipazione nei rispettivi Consigli dei Ministri, ma più in generale vi sono posizioni mai del tutto chiarite relativamente agli interessi francesi nei confronti di asset strategici italiani e dei diversi ruoli in politica estera spesso caratterizzati da una "competizione esasperata".

⁵² Darnis Jean-Pierre: Il Trattato del Quirinale può rilanciare l'Italia in Europa" – LUISS School of Government – Policy Brief 39/2021.

Capitolo 2. L'intelligence nell'Unione Europea

2.1 L'idea di intelligence europea

2.1.1 La situazione nel dopoguerra

Ancor prima della resa della Germania del 1945, una moltitudine di agenzie di intelligence degli Stati Uniti mise piede in Europa, intenzionata a portare a termine un paziente e complesso lavoro che, per certi versi prosegue a tutt'oggi. La comunità di intelligence USA era molto interessata al territorio europeo e per una serie diversa di motivi iniziò a dedicare tempo e denaro alla costruzione di una imponente architettura di intelligence complessa e ramificata. Nel 1948, venne creato l'Office of Policy Coordination (OPC)⁵³, ovvero la branca dell'intelligence, destinata a organizzare e portare a termine le principali *covert operations*, necessarie per impedire a qualsiasi Paese dell'Europa occidentale di passare sotto il controllo dell'Unione Sovietica, di essere "attratti" dalla governance di quell'area e quindi di finire a far parte di quella coalizione. Altra esigenza parallela era quella di disporre di una piattaforma ideale (e l'Europa incarnava appieno tale funzione), che consentisse agli USA di avere l'accesso ai suoi primari obiettivi di intelligence ovvero l'Unione Sovietica e suoi Paesi alleati. Nel 1946 erano stati stanziati in Germania circa 900 unità dell'Army Security Agency (ASA)⁵⁴; si trattava per la maggior parte di Ufficiali e personale di supporto destinato in via prioritaria alle intercettazioni radio e operante nel settore signal intelligence, mentre la restante parte apparteneva al Counter Intelligence Corps (CIC)⁵⁵. Circa 300 unità della

⁵³ On 18 June 1948, National Security Council Directive NSCD 10/2 created the semiautonomous Office of Policy Coordination within the Central Intelligence Agency to conduct U.S. covert action. Historical Dictionary of United States Intelligence, M.A. Turner, Rowman & Littlefield, 9780810878891, 2014

⁵⁴ Prior to the Army Security Agency (ASA), the Signals Intelligence Service (SIS) was established in July 1929. In 1943, the Signals Intelligence Service (SIS) was re-designated as the Signal Security Service (SSS). Later, in 1943, the Signal Security Service (SSS) was re-designated as the Signal Security Agency (SSA). The Army Security Agency (ASA) was established on September 15, 1945 and existed through the end of 1976. In January 1977, the Intelligence & Security Command was established to integrate and consolidate Army intelligence assets. <https://www.thearmysecurityagency.com/history.html>

⁵⁵ In 1942, the CIP became the famed Counter Intelligence Corps (CIC) of World War II. American troops were once against fighting on foreign soil and operating in an environment exploited by

Strategic Services Unit (SSU)⁵⁶ erano invece dislocate in diverse aree tra le quali Heidelberg (170 uomini), un distaccamento di Francoforte (5 uomini) e uno a Berlino Ovest (25 uomini che costituirono l'avanguardia di quella che sarebbe poi diventata la Base Operativa di Berlino). Funzionari dell'intelligence militare erano presenti stabilmente anche in Austria e in Italia e nelle ambasciate USA presenti a Stoccolma, Oslo, Copenaghen, Bruxelles, Londra, Parigi, Madrid, Lisbona, Berna, Praga, Bucarest, Atene. Tuttavia, la scarsità di risorse e di capacità in questa prima fase, causò non poche limitazioni ad una incisiva attività di intelligence, tanto che inizialmente si dovette far ricorso a informazioni ottenute per il tramite dei servizi di intelligence dei paesi alleati, per quel poco che potevano sapere circa le capacità militari e le intenzioni dell'Unione Sovietica. Lo dimostra l'importanza che nel 1946 ebbe il nascente servizio di intelligence della Germania ovest il *Gehlen Organisation*⁵⁷, successivamente 1955 denominato *Bundesnachrichtendienst*, che

saboteurs and collaborators. CI units deployed worldwide to protect US and Allied Forces. One of the CIC units was the 902d CIC Detachment. Activated on 23 November 1944, the 902d CIC Detachment was formed in Hollandia, New Guinea; General Douglas MacArthur's Southwest Pacific Area. It provided security to combat forces on New Guinea, and later, on Luzon in the Philippines. For its service in the Philippines from October 1944 to July 1945, the detachment received the Philippine Presidential Unit Citation. Following the war, the 902d CIC Detachment was initially assigned to the Organized Reserve Corps. By the early 1950s, however, Cold War tensions had increased and the Army needed a greater counterintelligence and security capability. Consequently, the 902d CIC Detachment was reactivated in January 1952 with the mission of handling sensitive personnel assignments from the CIC School at Fort Holabird, Maryland. Moreover, the unit was responsible for counterintelligence operations being handled directly by the Assistant Chief of Staff for Intelligence (ACSI), G2 at the Pentagon. For the first time, all CI functions in direct support of Headquarters, Department of the Army (HQDA) were consolidated into a single organization. In December 1957, the unit was redesignated as the 902d Counter Intelligence Corps Group. Throughout the rest of that decade, the 902d provided technical, linguist, and security support to Army elements worldwide. The 902d represented the apex of Army counterintelligence. <https://www.nec.belvoir.army.mil/902dNCRFO/history.asp>

⁵⁶ The Strategic Services Unit (SSU) therefore was a holding operation intended to preserve, as far as possible, the clandestine intelligence capabilities developed in wartime until a decision could be reached on national intelligence policy in peacetime. Assistant Secretary of War John J. McCloy's initial instructions to the SSU director, Brigadier General John Magruder (who had been Donovan's deputy director of intelligence), directed him "to insure that the facilities and assets of OSS are preserved for any possible future use." (Document 95). Magruder said essentially the same to Assistant Secretary of War Lovett in a report on the future of U.S. intelligence activities. (Document 34) The Lovett Board in turn pressed the case for SSU as a trimmed-down nucleus for a future U.S. clandestine intelligence organization. https://1997-2001.state.gov/about_state/history/intel/intro3.html

⁵⁷ Die Organisation Gehlen (auch Organisation, Org., Operation Rusty, Operation Zipper oder O.G. genannt) war ein Nachrichtendienst, der Anfang 1946 entstand und aus dem am 1. April 1956 der Bundesnachrichtendienst (BND) hervorging. Langjähriger Leiter war Generalmajor a. D. Reinhard Gehlen, ehemaliger Chef der Abteilung Fremde Heere Ost (FHO) und erster Präsident des BND. Die USA, die die Organisation finanzierten und beaufsichtigten sowie die Aufklärungsergebnisse erhielten, verfolgten das Ziel, die deutsche nachrichtendienstliche Expertise über die Sowjetunion im sich abzeichnenden Kalten Krieg zu nutzen. Thomas Wolf: *Die Entstehung des BND. Aufbau, Finanzierung, Kontrolle*(= Jost Dülffer,

costituiva la principale fonte di informazioni di intelligence su questioni politiche e sviluppi militari della Germania dell'est. Si dimostrò utile anche l'uso di fonti interne al Vaticano, nel solco di un anticomunismo presente, che consentì di raccogliere informazioni su ciò che accadeva dietro la cortina di ferro, in particolare in Polonia, Ungheria e Ucraina, nonché per informazioni che potevano riguardare la situazione interna dell'Italia. Questa appena descritta rappresenta la genesi di una presenza dell'intelligence USA in Europa che dagli inizi degli anni 50 andò progressivamente a consolidarsi parallelamente allo sviluppo della Guerra Fredda e allo scoppio della guerra di Corea, fino ad aver un suo apice probabilmente negli anni 60 periodo in cui secondo alcune stime, erano presenti nel vecchio continente circa 25.000/30.000 uomini tra funzionari militari e civili oltre che un nucleo di circa 4.000 unità della CIA presenti nelle ambasciate e 15.000 addetti al signal intelligence appartenenti alla National Security Agency (NSA)⁵⁸. Storicamente è possibile sintetizzare due ondate di crescita dell'intelligence statunitense in Europa. La prima coincide con l'inizio della crisi di Berlino del 1948, momento in cui gli Stati Uniti si resero conto che l'Unione Sovietica poteva prendere iniziative che avrebbero messo in serio pericolo la stabilità non soltanto della Germania. Al di là del blocco di tutti gli accessi stradali e ferroviari di Berlino ovest, con le conseguenti difficoltà per le aree sotto il controllo di USA, Francia e Gran Bretagna, cominciava a preoccupare il numero di truppe e di armamenti tali che l'Unione Sovietica continuava ad accantonare. La seconda ondata coincide con lo scoppio della guerra in Corea. Secondo stime degli ambienti militari si temeva infatti che quella guerra fosse il preludio per un attacco da parte dell'Unione Sovietica in Europa. Nei mesi successivi all'inizio della guerra di Corea, le dimensioni della stazione tedesca della CIA esplosero e continuarono a crescere a un ritmo vertiginoso per il resto del decennio. Nel 1959, la Stazione

Klaus-Dietmar Henke, Wolfgang Krieger, Rolf-Dieter Müller [Hrsg.]: *Veröffentlichungen der Unabhängigen Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945–1968*. Band 9). 1. Auflage. Ch. Links Verlag, Berlin 2018, ISBN 978-3-96289-022-3

⁵⁸ The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both signals intelligence (SIGINT) insights and cybersecurity products and services, and enables computer network operations to gain a decisive advantage for the nation and our allies. Throughout the site, NSA/CSS will be referred to collectively as NSA. <https://www.nsa.gov/About/Mission-Combat-Support/>

più importante a Berlino, il Detachment-A⁵⁹ comprendeva più di un migliaio di unità. Parallelamente l'intelligence britannica e francese cominciò a inviare proprio personale nell'intento di spiare i sovietici. Col passare del tempo e le rinnovate capacità signal il maggior numero di unità venne destinato a stazioni di ascolto (posti di ascolto, stazioni di frontiera, centri di elaborazione SIGINT) che negli anni 60 arrivarono a contare circa diecimila unità. L'incremento di personale dell'intelligence (specie nel settore comunicazioni) non sfuggì ai sovietici che protestarono in più occasioni con i vertici USA. La priorità per la signal intelligence in Germania e le rimostranze sovietiche a tali presenze, emerge da molti documenti e tra questi il telegramma classificato "Eyes Only" del 2 aprile 1948, redatto da Robert Daniel Murphy (US Political Adviser for Germany) e diretto al Segretario di Stato USA:

Few additional developments affecting our Berlin situation have occurred since our last message. Soviet authorities have requested we close down effective May 1 US aid station which is midway on only highway available Berlin–Helmstedt traffic. Soviet representative also called on Chief of Staff OMGUS yesterday with request that US Signal Corps personnel stationed Weimar for purpose maintenance three repeater stations required for our official telephone service from Berlin to be removed from Weimar. British received similar request to remove their signal corps from Magdeburg. These repeater stations are necessary for maintenance of telephone cable lines.⁶⁰

2.1.2 I presupposti storici per una intelligence comune

Il sistema westfaliano, regolante le relazioni internazionali è stato nel tempo oggetto di critiche anche aspre e per ciò stesso indicato come un fallimento documentato da numerose crisi di portata internazionale come nel caso della

⁵⁹ Formed in 1956, Detachment A originally consisted of four A-teams that were each assigned an area of responsibility in Berlin — on the north, south, east, or west sides of the city. Later, two more teams were added. "The big mission was the stay-behind mission for World War Three," Colonel Farr said. Teams consisted of 11 men, with a B-team above them making the entire unit no larger than 80 or 90 people at any given time. <https://sofrep.com/news/special-forces-detachment-a-an-elite-cold-war-unit/>

⁶⁰ - Control (Germany)/4-248: Telegram 770, Personal for Saltzman and Hickerson, Berlin, April 2, 1948, 8 p. m. redatto da Robert Daniel Murphy, U.S. Political Adviser for Germany e diretto al Segretario di Stato. <https://history.state.gov/historicaldocuments/frus1948v02/d529>.

seconda guerra mondiale. Il politologo Leo Gross⁶¹, in un articolo del 1948 non a caso aveva parlato di un “maestoso portale che conduce dall’antico al nuovo mondo”. A distanza di 56 anni, Henry Kissinger dava la sua visione e ne tratteggiava le linee in un passaggio del suo libro *World Order*:

*The Peace of Westphalia became a turning point in the history of nations because the elements it set in place were as uncomplicated as they were sweeping. The state, not the empire, dynasty, or religious confession was affirmed as the building block of European order. The concept of state sovereignty was established. The right of each signatory to choose its own domestic structure and religious orientation free from intervention was affirmed, while novel clauses ensured that minority sects could practice their faith in peace and be free. Beyond the immediate demands of the moment, the principles of a system of “international relations” were taking shape, motivated by the common desire to avoid a recurrence of total war on the Continent.*⁶²

Proprio il Segretario Generale della NATO Javier Solana nel corso di un discorso a margine di un simposio sulla Pace di Westfalia, svoltosi a *Münster* il 12 novembre 1998, puntualizzò una sua visione critica non generica ma circostanziata e vertente su determinati aspetti. Secondo Solana finora vi era stata una costante rivalità che inevitabilmente finiva col degenerare in conflitti su vasta scala con una quantità di danni incalcolabile e un altissimo numero di vittime:

Yet the Westphalian system had its limits. For one, the principle of sovereignty it relied on also produced the basis for rivalry, not community of states; exclusion, not integration. Further, the idea of a strong, sovereign state was later draped with nationalistic fervour that degenerated into a destructive political force. The stability of this system could only be maintained by constantly shifting alliances, cordial and not-so-cordial ententes, and secret agreements. In the end, it was a system that could not guarantee peace. Nor did it prevent war, as the history of the last three centuries has so tragically demonstrated. It was only out of the ashes of the Second World War that the possibility of a new order for European security emerged. In the decade following the end of the war, its foundations were laid.

⁶¹ Leo Gross was born into a petit-bourgeois secular Jewish family in 1903, in the small Austro-Hungarian township of Krosno located in the Empire’s eastern most province of Galicia, modern day Poland.⁵⁰ He studied politics, law, and economics in Vienna in the 1920s and finished a doctoral dissertation titled *Pacifism and Imperialism* in 1927 under the supervision of Hans Kelsen (1881-1973), Austria’s leading legal scholar.

⁶² Vejas G.L., “The World Before the Treaty of Westphalia, The Great Courses Daily”, University of Tennessee, Knoxville:, July, 12, 2020, <https://www.thegreatcoursesdaily.com/the-world-before-the-treaty-of-westphalia/>

Occorreva invece pensare ad una integrazione regionale, quella stessa integrazione regionale che ha consentito all'Europa di fondersi nell'Unione Europea che dal 1945 in poi non ha più visto quei conflitti su vasta scala e che invece ha determinato la costituzione di un fronte comune: la NATO, sorta per fronteggiare la minaccia costituita dal Patto di Varsavia, creando altresì una integrazione che si mise in moto come più volte detto, con la Comunità Europea del Carbone e dell'Acciaio nel 1952:

*NATO has demonstrated that it is ready and able to play its full part in this emerging system of mutually reinforcing institutions. In Kosovo, its cooperation with the OSCE offers new hope for a peaceful resolution of the crisis. In Bosnia, it has proven essential in creating a safe environment and thus the basic conditions for long term reconstruction.... NATO must also seek new approaches to deal with the "hard" security challenges that lie ahead - such as proliferation and regional conflicts. And it must help foster a more mature transatlantic relationship, where burdens and responsibilities are equitably shared between North America and Europe.*⁶³

2.1.3 La visione NATO

Il quadro appena delineato fa emergere una pressante e improrogabile richiesta di sicurezza che vedeva le politiche di Difesa al centro di molti dibattiti come dimostrato dal Trattato di Dunkerque nel 1947, dal Trattato di Bruxelles del 1948 e dalla successiva creazione dell'Unione Europea Occidentale del 1954 con la quale Italia, Belgio, Francia, Lussemburgo, Paesi Bassi, Regno Unito e Germania diedero vita all'Unione Europea Occidentale. L'intelligence sul territorio europeo era prevalentemente statunitense o comunque creata e diretta da Washington ma i Paesi della nascente Alleanza Atlantica, poterono fin da subito fare riferimento anche a una struttura interna esistente. Si tratta della Divisione Intelligence dell'International Military Staff, quest'ultimo organo esecutivo del Military Committee⁶⁴.

⁶³ Speech by the Secretary General at the Symposium on the Political Relevance of the 1648 Peace of Westphalia, Münster, Thursday, 12th November 1998
<https://www.nato.int/docu/speech/1998/s981112a.htm>

⁶⁴ L'IMS è composto da uno staff di circa 500 persone, composto esclusivamente da personale militare e civile dei paesi membri della NATO, che lavora dal quartier generale della NATO a Bruxelles. Fornisce consulenza strategica e militare e supporto di personale al Comitato militare, che fornisce consulenza al Consiglio Nord Atlantico sugli aspetti militari della politica, delle

*NATO intelligence, in the way it exists today, is the result of the early years of NATO, when it was assumed that all NATO forces would remain under national command, and strategic intelligence would be mainly national intelligence. Each nation would separately and "statistically" collect data on Warsaw Pact nations and their forces. This deficiency was partially repaired, when it became necessary to maintain a closer observation of the Warsaw Pact forces in the 1980s, but NATO's intelligence branch always obtained the mass of data from U.S. agencies (mainly the DIA and military G-2/A-2 branches), and from some other governments like Great Britain, Norway, Turkey or Germany.*⁶⁵

Per quanto la letteratura scientifica non abbia prodotto finora molti lavori sulla strutturazione dell'intelligence NATO, è evidente che, specie alle sue origini vi era una forte connotazione nazionale, provenendo la maggior parte dei dati, dai singoli apparati di intelligence dei Paesi aderenti e in maniera più corposa da quella degli Stati Uniti. Col passare del tempo e l'evoluzione concettuale strategica, le nuove prospettive di Difesa evidenziarono l'esigenza di una intelligence funzionale al processo decisionale europeo che sin dalle prime fasi marcò spedito proponendo una prospettiva nuova: cittadinanza europea, abbattimento delle frontiere, libera circolazione all'interno dell'area Schengen, creazioni di programmi universitari per gli scambi studi tra giovani di diversi Paesi (programmi Erasmus) sono solo alcuni esempi di modalità attraverso le quali è stato possibile rafforzare il convincimento di far parte di una entità o di una identità europea. Tuttavia gli sforzi per fronteggiare specifiche esigenze, diedero origine a singole risposte, non coordinate tra loro e su tali basi, in tempi diversi, nacquero strutture diverse. Il riferimento è ai Centri che verranno trattati nei paragrafi a seguito: Centro di Intelligence e Situazione (SitCen/IntCen) - Divisione Intelligence Stato Maggiore Militare dell'Unione Europea (IntDiv EUMS) - Europol - Centro Satellitare dell'Unione Europea (SatCen), alcuni dei quali, solo recentemente si stanno evolvendo, assumendo una connotazione più integrata e rispondente alle esigenze contingenti.

operazioni e della trasformazione all'interno dell'Alleanza. L'IMS garantisce inoltre che le decisioni e le politiche della NATO in materia militare siano attuate dagli organi militari della NATO appropriati. È diretto da un direttore generale ed è composto da cinque divisioni. https://www.nato.int/cps/fr/natohq/topics_64557.htm?selectedLocale=pl

⁶⁵ Korkisch F. W.: *NATO Gets better Intelligence New Challenges Require New Answers to Satisfy Intelligence Needs for Headquarters and Deployed/Employed Forces* - Institut für Außen- und Sicherheitspolitik - Center for Foreign and Defense Policy – Vienna, April 2010.

2.2 Il SitCen (EU Situation Center)

2.2.1 Le origini del Centro

La creazione del Centro di situazione dell'UE (EU SITCEN) è intimamente legata ai processi evolutivi della politica europea di sicurezza e di difesa (PESD) e alla creazione della carica di Alto rappresentante nel 1999: lo sviluppo delle capacità di gestione delle crisi gestite in ambito PESD, e il conseguente dispiegamento di missioni sia civili che militari rendevano necessaria una struttura di analisi dell'intelligence adeguata al contesto. Sulla data di creazione ci sono discordanze dal momento che nonostante alcuni documenti ufficiali parlino del 2002, in realtà già dal 2000 si registra una decisione unilaterale dell'allora Alto Rappresentante Xavier Solana il quale decise per l'istituzione del Centro, pur in mancanza di un mandato giuridico ad hoc. Nella fase iniziale era composto unicamente da sette funzionari provenienti da Francia, Germania, Italia, Paesi Bassi, Spagna, Svezia e Regno Unito, che avevano il compito di monitorare fonti di intelligence aperte per informare l'alto rappresentante sulle situazioni più a rischio sicurezza nelle aree di interesse del SEAE. Primo direttore, nel 2001, fu nominato un diplomatico britannico, William Shapcott, che ebbe modo di svolgere un ruolo importante nel plasmare il futuro dell'organizzazione; già dall'anno successivo al suo insediamento, SITCEN divenne un circuito di sharing di informazioni sensibili non soltanto tra gli appartenenti dei sette Paesi da cui provenivano i funzionari ma con tutti gli altri membri. Nelle prime fasi organizzative venne suddiviso in tre unità: Operazioni, Analisi, Affari Consolari. Tra i principali destinatari delle analisi l'Alto Rappresentante UE, il Coordinatore anti-terrorismo, il Coreper II⁶⁶, il Comitato

⁶⁶ Il Coreper II ("parte seconda") sta per "comitato dei rappresentanti permanenti dei governi degli Stati membri dell'Unione europea". Il suo ruolo e le sue diverse formazioni sono illustrati all'articolo 240, paragrafo 1, del trattato sul funzionamento dell'Unione europea. Principale organo preparatorio del Consiglio, non è un organo decisionale dell'UE e gli accordi raggiunti al suo interno possono essere rimessi in discussione dal Consiglio, che è l'unico ad avere potere decisionale. E composto dai rappresentanti permanenti degli Stati membri ed è presieduto dal rappresentante permanente del paese che esercita la presidenza del Consiglio "Affari generali". prepara i lavori di quattro formazioni del Consiglio: economia e finanza, affari esteri, affari generali e giustizia e affari interni. <https://www.consilium.europa.eu/it/council-eu/preparatory-bodies/coreper-ii/>

Politico e di Sicurezza, comitati vari nei settori della cooperazione di polizia e della giustizia. Sin dalle prime fasi, opera 24 ore al giorno, sette giorni la settimana per garantire la produzione di analisi e aggiornamenti continui.

2.2.2 Evoluzione e nuove collaborazioni

Come riportato nei fact-sheet, predisposti dal SEAE in merito al centro di intelligence, dal 2002 in poi vi è stata un'evoluzione anche strutturale del centro che può essere così riassunta. Nel 2005, il Centro è stato rinforzato dall'arrivo di un team di esperti del settore antiterrorismo, provenienti dai servizi degli Stati membri; tale innovazione ha consentito al Centro di elaborare e fornire una serie di valutazioni strategiche anche nel delicato ambito, diventato di importanza prioritaria già all'indomani dell'11 settembre 2001. Nel 2007, il SITCEN ha rafforzato la sua collaborazione con la Direzione dell'Intelligence dello Stato Maggiore Militare (EUMS) stabilendo in tal modo l'elaborazione di un ulteriore prodotto, ovvero le valutazioni basate sulla cosiddetta Single Intelligence Analysis Capacity (SIAC). Con l'entrata in vigore del Trattato di Lisbona il 1° dicembre 2009, EU SITCEN è passato sotto l'autorità dell'Alto Rappresentante di l'Unione europea per gli affari esteri e la politica di sicurezza/Vicepresidente della Commissione e il 1° gennaio 2011, il Centro è stato definitivamente posto alle dipendenze del Servizio europeo per l'azione esterna (SEAE).⁶⁷ Da un esame di documentazione della House of Lords Select Committee on the European Union è possibile rilevare molti particolari sulla prima fase del SitCen, sul suo ruolo e su come veniva individuato specialmente da Londra. Il documento datato 6 dicembre 2010 è il resoconto di una *Oral and associated written Evidence* a seguito di una *Inquiry into The EU Internal Security Strategy*, nell'ambito della *Sub-Committee F*. Si tratta di un comitato ristretto (facente parte della Camera dei Lord, quindi all'interno del Parlamento del Regno Unito) che ha il compito di esaminare i documenti UE e di rappresentare l'Assemblea nella cooperazione interparlamentare interna all'Unione. L'analisi dei documenti è portata avanti da i sottocomitati ciascuno dei quali si occupa di un settore politico specifico.

⁶⁷ <https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf>

Nell'esaminare l'Oral and associated written evidence del 06 dicembre 2010 è possibile riscontrare una preliminare richiesta da parte di Lord Richard⁶⁸

Q11 Lord Richard: Can I ask a more specific question about SitCen, which at the moment has a particular mandate? There were some occasions in the past – particularly in January 2005 – when SitCen's mandate was extended to include the domestic or internal threat gleaned from information provided by the member states' intelligence agencies. So there was a slight widening there. Do you see that widening continuing? Do you think it ought to continue and that SitCen should have responsibility for both external and internal affairs?

Alla quale fa seguito una precisazione da parte della rappresentante della Commissione affari interni Cecilia Malmström⁶⁹

know that Lady Ashton is now looking at this aspect very closely and we discussed it the other day. SitCen is excellent but we need to have it more co-ordinated with the other agencies and with what the rest of the European Union is doing. There is a lot of information at Frontex and Europol, for instance, and we need to co-ordinate the work much better. I am discussing this with Lady Ashton and she shares my view. I have also visited SitCen to discuss how we can increase our co-operation.

Ma una parte consistente della riunione è stata l'esame di Sir William Shapcott⁷⁰ già direttore di SitCen, la cui trattazione nel documento va dalla question 40 alla 66 (e relative risposte). Molti i passaggi nei quali, fatta una debita premessa circa la distanza temporale che lo separava dal suo incarico, entra in merito all'organizzazione del Centro, alla sua utilità e soprattutto alle potenzialità.

Q41 - William Shapcott: SitCen, of course, has had no operational role so it has been limited essentially to sharing assessed intelligence with a view to producing evaluations to support policy-makers in Brussels. It has touched on the issue that you raise but that has not been a central issue. My personal view is that the member states are still a bit too coy about sharing in these sorts of frameworks. It is perfectly

⁶⁸ Lord Ivor Seward Richard (Cardiff 30.05.1932-18.03.2018) was educated at Cheltenham College, at Pembroke College, as well as in Oxford where he obtained a BA in jurisprudence. From 1981 to 1984, Lord Richard was European Commissioner responsible for Social Affairs, Employment, Education and Vocational Training. <https://members.parliament.uk/member/1688/career>

⁶⁹ Cecilia Malmström (Stockholm 15 may 1968) has devoted the better part of her career to global affairs and international relations and has extensive experience from multilateral leadership and cooperation. She has served as European Trade Commissioner and European Home Affairs Commissioner, as well as Minister for EU Affairs in the Swedish Government. Ms Malmström is currently Visiting Professor at the School of Business, Economics and Law at the University of Gothenburg. <https://www.oecd.org/about/secretary-general/selection-process/Cecilia-Malmstrom-Sweden-Bio.pdf>

⁷⁰ The first head of SitCen/IntCen was former *British Diplomat William Shapcott* who played a crucial role in shaping its development.

understandable that sensitive operational information should be shared on very limited circuits. It is not a question of nationality and limiting the number of nationalities in each area; it is simply a question of limiting the number of people that you share it with. The UK does share sensitive things with a range of nationalities, so the hang-up is not the notion of sharing with foreigners—the hang-up is the notion of sharing with lots of foreigners, sometimes in frameworks where you cannot control what every single one of them does with the information.

Nella lunga e articolata risposta alla question 41 ritroviamo inoltre un passaggio sulla necessità di garantire una più efficace condivisione delle informazioni e dell'intelligence finalizzate a garantire la sicurezza del personale spesso inviato in aree calde (quali Afghanistan e Iraq) e sul fatto che costituisce una chiara lacuna il fatto che alcune di queste informazioni vengono condivise solo in ambito NATO e non anche in ambito UE.

But we realized that the EU is now doing operational things, and you can't limit this discussion just to assessed information to support policy. The Union has people in dangerous places now, such as Afghanistan and Iraq, and we began to realize that the block on the sharing of more punctual operational information meant that these operations were not properly supported. Thank goodness, we have not so far had a terrorist attack on one of our ESDP missions, but a couple of years ago I tried to interest the member states in going a little further with regard to these vulnerable operations. They are what I call "operational diplomacy". In the case of Afghanistan, for example, people would say, "Ah, but this information's all shared with NATO and your mission is in Kabul, it's next to a NATO mission, it's all perfectly safe". Unfortunately, that's not how it really happens. Information may be shared with NATO but I think you know that the state of EUNATO relations is not good. NATO accorded the EU mission in Kabul the same status as it accorded the United Nations mission—it would be protected within means and capabilities. NATO was not able to reach agreement with us on an intelligence-sharing agreement, so our people had no solid intelligence feed from NATO and no protection beyond that which was offered through normal means and capabilities. So, in my view, it's a gap.⁷¹

⁷¹https://www.asktheeu.org/en/request/history_and_co_operation_of_intc?utm_campaign=alaveteli-experiments-87&utm_content=sidebar_similar_requests&utm_medium=link&utm_source=asktheeu.org

2.3 L'IntCen (EU Intelligence and Situation Center)

2.3.1 Struttura e compiti

Nel 2012, il SEAE decise di adottare una nuova denominazione per il centro di analisi che diventò INTCEN (acronimo di *EU Intelligence Analysis Centre*), parallelamente si attuò una rimodulazione dell'organico e della struttura, allo scopo di consentire lo svolgimento di quel "ciclo delle informazioni" più adeguato ai tempi e alle emergenze contingenti (il *cybercrime* e la minaccia terroristica), che danno a questa struttura Europea l'opportunità di costituire un reale valore aggiunto, al di là di quello che i singoli Stati Membri siano in grado di produrre da soli. La *mission* del centro così riformato, fu quella di fornire analisi di *intelligence* (*early warning* e *situational awareness*) in particolar modo in materia di potenziali minacce terroristiche, problematiche inerenti la proliferazione delle armi di distruzione di massa e criticità emergenti nelle aree interessate ai conflitti; a ciò si aggiunsero analisi afferenti alla politica estera e di sicurezza comune, politica di difesa e valutazioni strategiche su particolari tematiche. Oltre a fornire gli aggiornamenti in tempo reale su crisi internazionali e situazioni di instabilità politica è in grado di elaborare rapporti di *intelligence* e valutazioni strategiche in prospettiva di medio e lungo periodo. Strutturalmente è diviso in due divisioni: la *Divisione Analisi*, il cui compito è quello di fornire analisi strategiche sulla base di *input* dei servizi di *intelligence* Europei (a sua volta composta da varie sezioni che trattano argomenti tematici o specializzati in aree geografiche di interesse) e la *Divisione Affari Generali e Relazioni Esterne* che si occupa di questioni amministrative, degli aspetti legali e delle analisi *open source* (composta da tre sezioni dedicate all'*Information Technology*, alle attività di comunicazione interna ed esterna, e all'analisi *open source*). Riceve informazioni da tutti gli Stati Membri oltre che dalla Svizzera e dalla Norvegia; sempre nell'ambito del SEAE, il centro ha la possibilità di integrare le proprie informazioni con quelle del Direttorato di *Intelligence* del EUMS (*European Union Military Staff*) in ambito SIAC (*Single Intelligence Analysis Capacity*) che consente quindi di ottenere una migliore offerta del prodotto finale, attraverso una efficace condivisione delle informazioni delle varie strutture esistenti, anche per il raggiungimento dei requisiti richiesti

dalla Politica di Sicurezza e di Difesa Comune. Usufruisce inoltre delle potenzialità informative dell'*European Union Satellite Centre* per quanto attiene alle attività legate all'*intelligence* geospaziale, nonché dell'agenzia per la cooperazione delle frontiere *Frontex* e dell'*Europol*. Anche per l'IntCen, periodicamente, vengono sollevate interrogazioni parlamentari comunitarie circa maggiore trasparenza specie sul mandato. È questo il caso dell'interrogazione parlamentare datata 03 marzo 2021 alla quale è stata fornita risposta "*4 June 2021 Answer given by High Representative/Vice-President Borrellon behalf of the European Commission Question reference: E-001243/2021*".

Council Decision 2010/427 is the legal basis for the existence of the EU Intelligence and Situation Centre (EU INTCEN) within the European External Action Service. All Members of the European Parliament who intend to get EU INTCEN briefings must have a valid Personal Security Clearance (issued by the national authorities) to receive any classified intelligence in a restricted briefing room. The Director of EU INTCEN provides briefings, in compliance with the EU classified information (EUCI) rules, typically in Committee on Foreign Affairs (AFET) and Subcommittee on Security and Defence (SEDE) meetings according to the 'third party rule'. EU INTCEN is not an Intelligence Service; it has no intelligence collection powers. It is an intelligence fusion centre, functioning based on finished intelligence, shared voluntarily by EU Member States' Intelligence and Security Services. EU INTCEN fuses these inputs to provide classified assessments to EU decision-makers, according to a strict need-to-know principle, in respect of the 'third party rule' and the EUCI rules (and Member States' rules). Member States' Intelligence and Security Services also provide expert staff (Seconded National Experts and Temporary Agents) to EU INTCEN to support its work and to facilitate contacts with national services.

2.3.2 Le sfide attuali

L'evoluzione più recente rappresentata dalle nomine a Direttori del Centro da parte di ex Dirigenti dei Servizi di Intelligence dell'Unione ha evidenziato la volontà di rafforzare il ruolo di *INTCEN* e uno dei compiti principali del nuovo direttore è sicuramente quello di elaborare strategie di cooperazione tra i servizi di *intelligence* Europei che siano più idonee alle sfide attuali. Per far fronte alle

attività specifiche del SEAE e comunque per attuare tutti gli indirizzi in materia di PSDC, è indispensabile che l'UE si doti di uno strumento che possa costituire il punto di riferimento per l'aspetto "sicurezza", sia che si parli di attività militari all'estero e sia che ci riferisca a specifiche necessità interne; questo strumento può identificarsi in una fonte comune di analisi e di *intelligence* attraverso la quale perseguire i citati obiettivi. Fino a che punto però i singoli Paesi siano disponibili a condividere le proprie informazioni, specialmente quelle classificate, resta comunque un problema di non facile soluzione: lo scambio di informazioni classificate nell'*intelligence* spesso può contrastare con l'esigenza di proteggere i propri interessi strategici. Alla base di tale diffidenza si possono intravedere diversi fattori tra i quali il timore che le informazioni possano essere utilizzate per fini diversi da quelli condivisi: la perdita di influenza su altri *partner*, o perfino la possibilità di svelare dinamiche e indirizzi politici che non sempre rispondono alle posizioni ufficialmente adottate. Altro elemento da non sottovalutare è rappresentato dalle differenze esistenti tra i Paesi Membri, non soltanto in termini di *budget* annuali ma soprattutto per quel che riguarda l'eterogeneità dei sistemi giuridici, la diversità nei rapporti internazionali, la diversa concezione della sicurezza e della cultura e legittimazione dell'*intelligence*. Solo a titolo di esempio, ognuno dei Paesi UE è dotato di una propria legislazione in materia di scambio di dati personali e trattazione di informazioni classificate e solo recentemente sono state introdotte nuove normative per lo più dettate da emergenze legate alla lotta al terrorismo e al crimine organizzato; inoltre, ognuno di essi dispone di strutture di *intelligence* che operano secondo *standard* e sistemi normativi di riferimento nazionali, per cui ogni confronto e ogni scambio di notizie risente, inevitabilmente, di numerose variabili con evidenti ripercussioni in situazioni di emergenza nelle quali è indispensabile procedere con rapidità ed efficacia. Molto si è discusso circa il mandato legale di IntCen e tra i documenti ufficiali va menzionata la risposta a una interrogazione scritta, fornita dall'Alto rappresentante C. Ashton in data 03 settembre 2013 con nota protocollata al n. E-008808/2013. Si tratta sostanzialmente di un chiarimento che l'AR/VP Ashton fornisce circa la natura riservata del Centro, il controllo diretto effettuato dall'Alto Rappresentante e il richiamo alla decisione del Consiglio Europeo del 26 luglio 2010 che istituì il SEAE.

E-008808/2013 - Answer given by High-Representative/Vice-President Ashton on behalf of the Commission . The EU INTCEN (EU Intelligence and Analysis Centre) is the successor of the EU Situation Centre (EU SITCEN), which is mentioned in Article 4, paragraph 3, sub (a), third indent of the Council Decision of 26 July 2010 (Decision establishing the organization and functioning of the European External Action Service). The aforementioned reference to the EU SITCEN serves as legal basis for EU INTCEN, which has taken over the intelligence and analytical tasks of EU SITCEN. It should furthermore be recalled that in answers to previous questions the HR/VP has provided the EP a full overview of the structure and activities of EU INTCEN. Providing detailed information regarding the subject-matter of its reports would however undermine the confidentiality of the reports drawn up by EU INTCEN. Analytical reports of EU INTCEN classified, restricted, confidential or secret can in this respect not be compared with Council documents that are not classified but only marked LIMITE (thus not to be disclosed to the public). The powers and competencies of EU INTCEN (as well as of its predecessor EU SITCEN) have been spelled out in detail in various answers to the EP, both by the Council (to which EU SITCEN belonged until 1.1.2011) as well as by the HR/VP. A sample of the answers is listed above. Finally, it should be stressed that, as indicated in the previous answers to the European Parliament, EU INTCEN is under full operational control of the HR/VP and that all EU rules regarding data protection, access to documents and security of information apply in full to EU INTCEN. Bearing in mind that EU INTCEN is not handling personal data and only producing strategic analysis, further parliamentary supervision is not foreseen.

2.3.3 Evoluzione e nuove direttrici

L'INTCEN è una struttura di raccolta dati ed elaborazione analisi con una configurazione distante da un tipico servizio di *intelligence* (e difficilmente, almeno nel medio termine, riuscirà ad assumere tale connotazione), tuttavia la sua funzione può essere implementata attraverso l'adozione di soluzioni più idonee. Attualmente il principio che viene applicato alla distribuzione delle analisi è quello che tradizionalmente viene denominato "need-to-know" così come la security clearance. In tale contesto, quando i documenti che il Centro produce ricevono la classifica "SECRET" o "CONFIDENTIAL" rientrano sotto la protezione dell'Art. 9 del Regolamento 1049/2001 ovvero ("*sensitive documents shall be recorded in the*

register or released only with the consent of the originator”). Quello che, molto più pragmaticamente può essere fatto, in un’ottica di adattamento ai tempi, è una rimodulazione dei suoi assetti, la dotazione di personale altamente specializzato, l’adozione di protocolli di collaborazione tra diverse agenzie col fine ultimo di apportare dei vantaggi, in termini di sicurezza, per tutti i Paesi *partner*. Le minacce alla sicurezza che si profilano ogni giorno, impongono un’accelerazione dei processi di adeguamento e in tal senso si sta già lavorando, come dimostra la recente costituzione, sempre in ambito INTCEN, della “*cellula per l’analisi delle minacce ibride*” in grado di ricevere ed esaminare informazioni riservate e pubbliche sulle minacce ibride. Si tratta di una unità ritenuta indispensabile a garantire un adeguato coordinamento con l’esistente *East StratCom task force*, creata nel 2015 allo scopo di affrontare delle campagne di disinformazione provenienti dall’area orientale e produrre un piano d’azione incentrato sulla comunicazione strategica e le analoghe strutture di analisi delle minacce ibride istituite in ambito NATO. In ambito SEAE, oltre all’INTCEN, esistono altre strutture e dipartimenti che presentano caratteristiche specifiche per le quali non si può parlare di sovrapponibilità in termini assoluti. Tra queste si ricordano:

Military Staff

Struttura che opera sotto il coordinamento dell’EU *Military Committee*, il *Military Staff* fornisce consulenza e sostegno nel settore della Politica di Sicurezza e Difesa Comune, compresa l’esecuzione delle operazioni di gestione delle crisi nelle missioni a guida UE. Assicura il tempestivo allarme, la valutazione della situazione e la pianificazione strategica nell’ambito dei compiti di *Petersberg*, comprendente l’individuazione delle forze nazionali e multinazionali da impiegare in missione. Composto dagli esperti militari designati dai Paesi membri, opera anche quale centro di condivisione dell’*intelligence* a sostegno della sicurezza dell’Unione.

In ambito UE, nel corso degli anni, si sono sviluppati molti dibattiti circa l’opportunità di inglobare il Military Staff all’interno del SEAE; lo dimostra la *Question for written answer E-006027/2012 to the Commission (Vice-President/High Representative) Rule 117 Martin Ehrenhauser (NI)* che in realtà racchiude una molteplicità di domande:

1. *What are the consequences of incorporating the EU Military Staff (EUMS) in the European External Action Service regarding the terms of reference, operations, staffing and budget of the Intelligence Division (INT)?*

2. *What are the INT's current responsibilities?*
3. *What is the current INT staffing level and what have been its staff numbers by year since its inception?*
4. *What are the INT's current staff categories and what have been its staff categories by year since its inception?*
5. *What is the present INT budget? What were its previous annual budgets?*
6. *Can the High Representative provide an updated establishment plan showing the internal structure of the INT?*
7. *Who exactly has the final say regarding the appointment of the INT chief within the EU Military Staff and what selection procedures are followed?*
8. *What exact procedures are followed for cooperation between the INT, the EU Military Staff and INTCEN (Intelligence Analysis Centre)?⁷²*

La risposta, in questo caso fornita dall'Alto rappresentante Chaterin Ashton, è incentrata sull'utilità di uno strumento i cui prodotti, già di alto livello, acquisiscono ulteriore valore poiché inseriti in un contesto di analisi integrata.

E-006027/2012 - Answer given by High Representative/Vice President Ashton on behalf of the Commission - (7.8.2012)

With the establishment of the European External Action Service (EEAS) the terms of reference for the EU Military Staff Intelligence Division (EUMS INT) Directorate remained unchanged but the requirements for Intelligence products in quality and quantity have increased considerably. The budget of EUMS INT is part of the EUMS budget which has experienced the same constraints like all other EEAS departments. The responsibilities of EUMS INT are to provide, together with the EU Intelligence Analysis Centre (INTCEN) within the format of the Single Intelligence Analysis Capacity (SIAC), the Intelligence support for the EU, thus contributing to policy development, early warning, advance and crisis response planning and to planning and conduct of CSDP missions/operations and exercises. This cooperation between EUMS INT and EU INTCEN allows both, while maintaining their independent identity and capabilities, to operate jointly and to combine their analysis tools, generating a wide range of intelligence products from different sources. In 2001, when established, EUMS INT comprised 30 posts. It currently has 41 posts and it is organised in three units (Policy, Support and Production). The staff of EUMS INT mainly consist of seconded national experts with the exception of two Assistants as EU officials. Following the standard procedures for all posts at Director level within

⁷²https://www.europarl.europa.eu/doceo/document/E-7-2012-006027_EN.html?redirect

*the EUMS, the EU Military Committee at MilRep level selects and endorses the future Director out of the candidates nominated by Member States, and offers the endorsed candidate for HR/VP's approval. The final decision lies therefore with the HR/VP.*⁷³

SatCen

A partire dagli anni 90, l'UEO decise di dotarsi di uno strumento in grado di sviluppare un prodotto di intelligence strategica specializzato in rilevazioni satellitari; nacque così il SatCen con sede a Torrejòn de Ardoz nei pressi di Madrid, inizialmente creato quale organismo sussidiario dell'UEO nel 1991, divenuto sperimentale nel 1993 e, quindi permanente nel 1995. Per certi versi considerato tra gli organismi fondamentali per l'architettura dell'intelligence europea. Funzionalmente dipendente dal SEAE, si tratta di un centro operativo di *intelligence* geospaziale in grado di fornire analisi qualificate sia a beneficio dell'Unione e sia ai Paesi membri. L'analisi strategica geospaziale è un elemento fondamentale nel processo di *intelligence*, che da sempre ha indotto molte agenzie a costituire settori dedicati esclusivamente a questo e a far nascere collaborazioni anche trasversali tra Paesi di diversa area geografica. Sin dalle prime fasi gran parte delle immagini sono state fornite dai satelliti SPOT 1, 2 e 4 (Francia), Landsat (U.S.A.), Radarsat (Canada), ERS 1C e D (India), Helios 1Ae B (Francia/Italia/Spagna). Come evidente, non tutte le informazioni raccolte sono provenienti da satelliti militari, essendo compresi, in questa attività di raccolta, anche le reti satellitari commerciali e governative, da tempo il Centro è coinvolto nello sviluppo delle potenzialità del programma Copernicus finalizzato allo sviluppo di servizi europei di informazione basati su dati satellitari; in prospettiva SatCen potrebbe svolgere un ruolo più concreto nel tentativo di promuovere e sviluppare una autonoma capacità nei settori Geoint e Imint.⁷⁴ Nel 2017 il Centro

⁷³ https://www.europarl.europa.eu/doceo/document/E-7-2012-006027-ASW_EN.html

⁷⁴ Copernicus (formerly known as GMES) is the European Union's Earth Observation Programme. It consists of a complex set of systems which collect data from multiple sources: Earth Observation satellites and in-situ sensors. Copernicus gathers these data in order to provide users with reliable and up-to-date information through a set of services related to environmental and Security issues. The Copernicus services address six thematic areas: Land, Marine, Atmosphere, Climate Change, Emergency Management and Security. They support a wide range of applications, including environment protection, management of urban areas, regional and local planning, agriculture, forestry, fisheries, health, transport, climate change, sustainable development, civil protection, and tourism. <https://www.satcen.europa.eu/page/copernicus>.

intelligence a tale livello. Il collegamento tra Paesi *partner* non sempre si rivela facile e per questo sono molteplici gli sforzi per superare i tradizionali accordi bilaterali, la cui validità e utilità è pur sempre riconosciuta. Per ovviare a tale situazione, da tempo l'Unione Europea ha cercato di potenziare i Dipartimenti già esistenti creando anche due nuove strutture: *l'Intelligence College in Europe* e la *Joint Eu Intelligence School* definite due piattaforme per la condivisione dell'*intelligence* a livello europeo, in grado di contribuire positivamente alla formazione di una visione strategica. Si tratta certamente di una novità nel panorama di riferimento e, probabilmente, di un buon inizio verso la creazione di una struttura unitaria.

L'Intelligence College in Europe

Il 26 febbraio 2020 a Zagabria in Croazia, 23 paesi europei (20 dell'UE più la Gran Bretagna, Norvegia e la Svizzera) hanno firmato una dichiarazione di intenti per la creazione dell'*Intelligence College in Europe (ICE)*, una piattaforma ad uso comune destinata alla formazione e alla condivisione delle principali visioni strategiche di *intelligence* in ambito europeo. Il progetto, partito anni prima, è stato fortemente sostenuto da una intesa franco-tedesca nata nel 2017, come dimostrato dalle dichiarazioni pubbliche proposte dai rispettivi leader Macron e Merkel in più occasioni.⁷⁶ La funzionalità progettuale si estrinseca attraverso tre direttrici, la prima delle quali è la collaborazione tra le comunità di *intelligence* e i decisori politici nell'intento di ampliare lo spettro informativo su tematiche di particolare valenza strategica. Un ulteriore passaggio prevede un dialogo sempre più diretto tra le varie agenzie di attraverso un confronto tra i rispettivi Direttori ad un livello definito "non operativo". Prevista infine una maggiore apertura all'esterno, con la creazione e la pubblicizzazione di una cultura dell'*intelligence* che attraverso il settore istituzionale, arrivi e si propaghi nei settori industriale ed accademico. Tra i documenti che ne certificano la nascita, si evidenzia la *letter of intent*, sottoscritta a Zagabria, il 26 febbraio 2020 dai rappresentanti dei Paesi entrati a farne parte, che sintetizza la *mission* e fornisce una traccia del mandato che viene così definito:

The Intelligence College in Europe is a platform for reflection, engagement and outreach. It fosters mutual understanding through strategic dialogue between:

⁷⁶ The Intelligence College in Europe was launched on 5th March 2019 in Paris. It brings together 23 member countries, which signed a Letter of Intent on 26th February 2020 in Zagreb, and 7 partner countries. <https://www.intelligence-college-europe.org/>

- *Intelligence communities in participating Countries;*
- *European intelligence communities and Academia;*
- *European intelligence communities, national and EU decision-makers.*

The College is a collective effort of the Intelligence Communities - meaning any Services and, depending on the Country, policymakers involved in the Intelligence cycle - operating in the European Countries here represented. It generates professional and academic views on a wide range of intelligence-related topics and disseminates those in order to contribute to the development of a strategic intelligence culture in Europe. The College has no legal personality or physical premises.⁷⁷

Pur avendo stabilito la sede a Zagabria, è stata prevista l'apertura di un Segretariato a Parigi mentre la presidenza, su base volontaria e per la durata di un anno, sarà esercitata a turno da ognuno dei paesi aderenti ed affiancata da un comitato costituito da esponenti della presidenza in uscita e quella subentrante. Il progetto iniziale ha visto il coinvolgimento di 30 Paesi ma alla fine, Bulgaria, Grecia, Irlanda, Lussemburgo, Polonia, Slovacchia hanno preferito un coinvolgimento meno vincolante adottando uno status di adesione "flessibile". Nello mese di settembre 2020 l'ICE ha organizzato un *webinar* aperto ai rappresentanti e responsabili di Italia, Romania e Finlandia; l'evento, dal titolo "Le sfide alla sicurezza europea" è stato incentrato sulla rispettiva visione delle sfide previste per il 21° secolo avuto riguardo all'impatto della tecnologia nel panorama della sicurezza nazionale, sulla propaganda e disinformazione, nonché sulla guerra ibrida. Dopo il primo anno di coordinamento della Croazia, nel 2021 la direzione del College è stata affidata al Regno Unito ed è interessante verificare, attraverso la dichiarazione del Vice Consigliere per la Sicurezza Nazionale britannica, Mrs Beth Sizeland⁷⁸ come nonostante le sfide, vi siano concrete e ambiziose aspettative per la piattaforma

It has been years since the conception of this strategic platform, and in that time we have faced much uncertainty. But one thing has remained clear, the threats we all face continue to diversify and we must keep pace. Our ability to collaborate as

⁷⁷<https://www.intelligence-college-europe.org/wp-content/uploads/2020/03/Lol-English.pdf>

⁷⁸ Beth Sizeland became Deputy National Security Adviser and Prime Minister's Adviser on National Resilience and Security in the Cabinet Office in February 2020 after 20 years working in the civil service, mostly on national security issues. Her previous roles in government are Director General Strategy – GCHQ; Director Modern Slavery and Exploitation - Home Office and Director Transport Security - Department for Transport. <https://www.gov.uk/government/people/beth-sizeland#biography>

*European allies is key to ensuring the safety and security of our citizens and the ongoing protection of our shared values. As our security threats continue to evolve, our collaboration must remain strong and unwavering.*⁷⁹

La Joint Eu Intelligence School

La costituzione del *college* non è una iniziativa isolata; da oltre un anno è operativa la *Joint Eu Intelligence School*, un istituto di formazione destinato a funzionari dei servizi di *intelligence* europei che possono così contare su una sede addestrativa comune e su programmi condivisi. Si tratta di una idea che trae le sue origini nel 2017 poi rientrando tra i tanti progetti approvati nell'ambito della Cooperazione Permanente Strutturata dell'Unione Europea, la cui attivazione risale al 2019. La sede della JEIS è a Cipro e la direzione del progetto è stata affidata alla Grecia, sulla base di criteri decisionali stabiliti per ognuno dei 17 progetti in ambito PESCO. Nello specifico questo progetto si propone di:

- istruire il personale dei diversi servizi di *intelligence* europei, diffondendo una visione comune legata agli interessi comunitari;
- attraverso i programmi e i corsi sviluppati, creare una dottrina di *intelligence* strategica;
- avviare sinergie e scambi di conoscenza su quanto già conosciuto in ambito NATO e ancora da creare in ambito UE, in tale senso la collaborazione con l'Alleanza Atlantica potrebbe seguire nel solco e tramite le risorse della sua Accademia con sede a Oberammergau in Germania.

Anche questo progetto risale ad alcuni anni fa, infatti nel 2017 si è sviluppato un articolato dibattito tra i principali Paesi europei circa la creazione di una eventuale *intelligence* europea, caratterizzato da una divisione di vedute per i partner che si divisero su due fronti. Da una parte quello dei favorevoli capeggiati dalla Grecia che attraverso il Commissario Europeo per gli Affari Interni, Immigrazione e Cittadinanza sosteneva una maggiore cooperazione e incoraggiava uno scambio informativo seppure il concetto si rivolgesse in realtà più a una implementazione delle strutture di *law enforcement* e non di pura *intelligence*. L'altro fronte era quello dei paesi contrari a unificare l'*intelligence*, capeggiato dai tedeschi

⁷⁹ Declaration of Mrs Beth Sizeland, Deputy National Security Advisor of Prime Minister of the United Kingdom on the occasion of the British Presidency of the College. <https://www.intelligence-college-europe.org/declaration-of-mrs-beth-sizeland-on-the-occasion-of-the-british-presidency-of-the-college/>

attraverso i responsabili dei servizi BND (*Bundesnachrichtendienst*) e BfV (*Bundesamt für Verfassungsschutz*). Ritenevano infatti che l'Europa fosse già dotata di una struttura in grado di garantire un proficuo scambio informativo; Secondo i rappresentanti tedeschi eventuali contatti bilaterali avrebbero assicurato un apporto su questioni più specifiche e delicate ma senza alcun dubbio la nascita di un nuovo servizio unificato avrebbe costituito una inutile sovrapposizione burocratica.

2.4.2 Le strutture già esistenti

La condivisione di informazioni meglio nota come *information sharing* procede verso una nuova direttrice⁸⁰; difficoltà a vari livelli e criticità spesso rilevanti potrebbero far desistere dal proseguire in uno sforzo sicuramente complesso. Quel che appare chiaro è che tale condivisione può rivelarsi determinante nell'affrontare le sfide della sicurezza che caratterizzeranno gli anni a venire. Esistono tuttavia strutture e forum di collegamento, a livello informale che hanno un'importanza notevole nelle relazioni internazionali e che spesso costituiscono il vero organo decisionale su aspetti di difesa e intelligence, specie se le tematiche si rivolgono a territori che presentano crisi o addirittura che presentino situazioni conflittuali già in atto. Tra queste si segnala:

Club di Berna

Vi sono scarsissime notizie in merito all'attività. Tuttavia, ciò che lo rende così cruciale è il concetto che il Club di Berna è strutturato come un importante forum multilaterale che dimostra una resistente capacità di *information sharing* nonostante non sia inserito organicamente nella struttura dell'UE. Ha radici profonde nella concettualizzazione "classica" dell'intelligence, ed è la risposta ai principali problemi di sfiducia culturale che solitamente sono insiti nelle comunità di intelligence poiché consente ai capi dell'intelligence di incontrarsi e rafforzare la fiducia reciproca in Europa. Fondato nel 1971, inizialmente con soli sei Stati membri, è l'organismo sotto il quale, attualmente si incontrano i capi di tutte le agenzie dei 27 Stati membri e degli Stati Uniti; dispone di un proprio sistema di

⁸⁰ Walsh J.I. "Intelligence Sharing in the European Union: Institutions Are Not Enough. JMC: Journal of Common Market Studies, 2006

comunicazione dedicato (Lefebvre 2003) Esso si concentra sulla cooperazione operativa (Müller-Wille 2008), cosa che le istituzioni o le agenzie dell'UE non fanno. Nel 2001, il gruppo di Berna ha istituito il Counter Terrorism Group, che comprende il i 27 servizi di intelligence nazionali dell'UE, più quelli di Norvegia e Svizzera. Europol e SitCen per lo scambio di informazioni nel settore, per promuovere le rispettive iniziative e condividere le principali strategie antiterrorismo.⁸¹ Compito del CTG è quello di preparare le valutazioni delle minacce relative al terrorismo islamico, che vengono poi messe a disposizione di vari organi dell'UE e dei ministeri nazionali degli interni.

2.4.3 Efficacia e criticità

Le strutture esaminate, pur nella loro diversità di funzione, contribuiscono a un sistema integrato di *intelligence* ancora non completo ma che rappresenta un grosso passo avanti rispetto al passato. Prendendo come parametri di riferimento alcune delle principali fasi di un processo di *intelligence* (*collection, processing, analysis and evaluation, dissemination, tasking and control*), si notano certamente elementi che dimostrano l'efficacia delle strutture esistenti, unitamente ad altri che rendono l'idea di quanto lavoro ci sia da fare per pervenire al completamento auspicato. Per quanto attiene alla *collection* occorre ricordare che l'UE non ha un mai istituito formalmente una agenzia unica di *intelligence*, per cui ogni Paese raccoglie informazioni nell'ambito della propria sfera di interesse; informazioni più o meno riservate ma soprattutto open-source, molto spesso utilissime se processate con la dovuta precisione. L'aspetto relativo al *processing* attualmente non è compiutamente sviluppato; in questo circuito è inclusa l'elaborazione dei dati satellitari, ambito di azione del citato SatCen che pur sviluppando delle attività di tutto rispetto, risente della mancanza di una propria rete di satelliti da gestire, limitandosi, conseguentemente ad acquisire dati provenienti da altri settori. "*Analysis and evaluation*": sono entrambi due degli aspetti che contribuiscono a gestire le crisi imminenti o addirittura di poterle prevenire. In un contesto quale

⁸¹ EU Intelligence Sharing & The Joint Situation Centre: A Glass Half-Full - Dr. Mai'a K. Davis Cross - Assistant Professor of International Relations University of Southern California Prepared for delivery at the 2011 Meeting of the European Union Studies Association March 3-5, 2011.

quello dell'Unione è indispensabile che *IntCen* e *EuMS* sviluppino al massimo tali capacità per giungere agli scopi prefissi. Come più volte detto l'Unione Europea non dispone di proprie fonti di raccolta informazioni, aspetto che la rende dipendente dalle varie organizzazioni di *intelligence* nazionali.⁸² Queste ultime sono ovviamente espressioni di sovranità nazionali dove si intersecano interessi a migliorare la propria posizione, diffidenze nei confronti di altri partner e problematiche inerenti la sicurezza delle informazioni; ne discende che anche l'aspetto della "dissemination" sia da rivedere. Le fasi del "Tasking and control" partono dallo svantaggio di essere il prodotto di un ciclo ove la capacità di analisi è limitata; nonostante questo, se ci si adopera affinché *IntCen* magari coadiuvato dalle due piattaforme produca una capacità di analisi anche di tipo strategico, allora è possibile ipotizzare un salto di qualità a beneficio del sistema.

2.5 L'UE tra status quo e maggiore autonomia

2.5.1 Obiettivi futuri

É davvero difficile immaginare, allo stato, un'*intelligence* europea vista in un contesto di struttura organica e potenzialmente in grado di operare autonomamente nei suoi aspetti principali. Come spiegato, esiste l'*IntCen* preposta alla raccolta e alla condivisione di informazioni open source; il *SatCen* che processa i dati satellitari disponibili; il *Military Staff* che fornisce il suo contributo nelle missioni a guida UE. Rappresentano invece una novità la scuola di *intelligence* europea progettata esclusivamente per i funzionari dell'Unione e l'Intelligence College, una piattaforma di confronto e programmazione strategica dell'*intelligence* di cui fanno parte anche Paesi non appartenenti all'area comunitaria. Lo sono sia perché il loro scopo è quello di contribuire ad acquisire una visione comune legata agli interessi comunitari, ma soprattutto perché nell'elaborare il concetto di formazione comune aspirano a creare una dottrina di *intelligence* strategica, momento caratterizzante di un progetto di alto livello. Non

⁸² Ates A. Erkan A. "Governing the European Intelligence: Multilateral Intelligence Cooperation in the European Union. International Journal of Politic and Security (online), 2021

vi sono elementi certi per stabilire quanto tempo occorrerà per una tale piena operatività e forse sussistono anche dei dubbi circa la piena fattibilità del progetto che prevede il superamento di logiche nazionali sempre presenti e condizionanti tale processo di evoluzione. Si tratta di tentativi che delineano un quadro in costante sviluppo. Una maggiore cooperazione di *intelligence* produrrebbe significativi vantaggi, consentendo all'UE di perseguire una politica di sicurezza e difesa più efficace ed essere un attore di maggiore speso nel panorama internazionale. Su tali considerazioni i Paesi europei dovrebbero adoperarsi nel tentativo di aumentare la cooperazione, probabilmente cominciando a elaborare riforme che investano inizialmente i singoli apparati di *intelligence* nazionali avviando quei processi propedeutici a un cambiamento conforme ai propositi iniziali.

2.5.2 La dimensione giuridica, economica e psicologica

Con riferimento alla dimensione giuridica occorre inevitabilmente fare riferimento al trattato di Lisbona che ha portato ad un aumento delle competenze e delle strategie di pertinenza di IntCen; tuttavia, non si può ignorare che lo stesso Trattato ha chiaramente sottolineato la rispettiva responsabilità degli Stati membri per garantire la sicurezza nazionale. Ne consegue che questa è ancora un'esclusiva competenza degli Stati membri, molti dei quali continuano ad avere "riserve di sovranità", rendendo meno fluida una cooperazione legata, in particolare, alla condivisione dell'intelligence. Di conseguenza, i poteri dell'UE di agire direttamente sulla produzione di intelligence o per richiedere/coordinare la condivisione, restano ancora molto limitate, nonostante l'aumento del numero di organismi europei citati. Il Trattato di Lisbona si presenta come uno strumento di blocco formale-legale, che rende impossibile raggiungere una maggiore integrazione cooperazione, lo sviluppo di reti e canali di condivisione dell'intelligence centralizzata nell'UE e una maggiore armonizzazione dei metodi di raccolta e di analisi delle tecniche di intelligence. Una revisione di questo quadro giuridico potrebbe accelerare una maggiore interoperabilità, correggere alcune delle difficoltà incontrate nel processo di condivisione all'interno dell'Europa, con assoluti vantaggi in termini di efficienza. Per quanto attiene alla dimensione

economica è indubbio che oggi si assiste ad una espansione del mercato dell'intelligence; ciò in quanto la sua importanza a livello nazionale ha oggi uno spettro più ampio rispetto al passato essendo finalizzata al raggiungimento di performance in settori che, seppur eterogenei, afferiscono comunque agli interessi nazionali. Certamente sono presenti profili di interesse comune ma parallelamente esistono (e sono preponderanti) interessi competitivi su questioni strategiche, indispensabili ai rispettivi governi nei loro processi decisionali. Si tratta di un sistema di tipo duale, all'interno del quale coesistono aree in cui gli Stati membri (e quindi i rispettivi servizi di intelligence) cooperano e altre in cui vige una serrata competizione. Tra queste ultime va annoverato il settore economico, dove l'intelligence si pone a sostegno alle principali attività governative e si esplica attraverso il supporto alle strategie commerciali nazionali, alle azioni di controspionaggio legate ai settori economici e alla conoscenza delle strategie dei competitors. Analogamente avviene per il settore energetico in cui gli interessi strategici nazionali rendono necessaria una intelligence che per ovvietà di contesto deve muoversi in ambienti di tipo competitivo. Esiste poi una dimensione che per certi versi può apparire residuale. Si tratta della dimensione psicologica generata dal principio di fiducia. Ogni Stato mette a disposizione di altri (in un'ottica ideale di information sharing) una serie di informazioni ma non sa quale sarà il loro uso da parte di altri servizi di intelligence; quale sarà l'impatto delle stesse e le ripercussioni. Si generano in questo loop una serie di interrogativi che vanno ancora oltre a quanto detto finora, fino a comprendere interrogativi sulla garanzia di sicurezza dei dati condivisi (differenti normative adottate), sulle modalità di fruizione di idonei canali di comunicazione (diversi standard adottati), il grado di reciprocità da adottare con i partner "minori" o con quelli che meno contribuiscono ad una produzione e una messa a disposizione di intelligence. Le perplessità fin qui esposte sono le principali cause che portano a prediligere i rapporti bilaterali al posto di una condivisione più ampia. Ecco che occorre far leva soprattutto sull'elemento della fiducia, per tentare di invertire questa tendenza.

2.5.3 La prospettiva di maggiore autonomia

Il 16 dicembre 2021 i Paesi UE si sono incontrati a Bruxelles in occasione della riunione ordinaria del Consiglio Europeo. Tra i vari punti in agenda un'attenzione particolare è stata riservata alla situazione geopolitica dell'est Europa e delle tensioni emergenti. Altro focus è stato costruito attorno alla situazione in Etiopia seguita con interesse. Nel complesso è risultato evidente e riconosciuto dalla stessa UE che si sta attraversando un periodo caratterizzato da una elevata confusione geopolitica in un contesto geopolitico globale dove prevalgono crescente instabilità mondiale, concorrenza strategica e minacce per la sicurezza. Proprio per questo si rende necessario perseguire gli obiettivi già indicati nel 2016 con la EU Global Strategy, costituenti un'assunzione di responsabilità e di consapevolezza che porta l'Unione a riconoscere come ineluttabile, la necessità di individuare obiettivi condivisi, delineare una strategia comune e dotarsi di strumenti idonei a raggiungerli. Si tratta dello Strategic Compass già annunciato dall'Alto Rappresentante Joseph Borrell ai ministri degli Esteri e della Difesa dei Paesi membri e ribadite nelle Conclusioni del Consiglio europeo del dicembre 2021, ovvero quello di realizzare "un dispositivo di orientamento politico-strategico condiviso che consenta di agire e che definisca una visione strategica comune per il prossimo decennio e utilizzi al meglio l'intero pacchetto di strumenti dell'UE, compresi gli strumenti e le politiche civili e militari". Doverosa la puntualizzazione, al punto 13 delle citate conclusioni, circa la complementarità alla NATO e alla prosecuzione di una proficua collaborazione con quest'ultima, considerata riferimento imprescindibile in un'ottica di strategia difensiva globale. Le risultanze fin qui esposte, in parte corredate dalla documentazione evidenziata, risultano coincidenti con i contenuti di una intervista all'Amb. Giampiero Massolo,⁸³ già Direttore del Dipartimento delle Informazioni

⁸³ Giampiero Massolo (Varsavia 1954) funzionario e Diplomatico italiano. Laureato in Scienze Politiche, indirizzo politico-internazionale, presso la Libera Università Internazionale degli Studi Sociali (LUISS) di Roma nel 1976. Da maggio 2016 è Presidente del Consiglio di Amministrazione di FINCANTIERI S.p.A. Consigliere Centrale della "Società Dante Alighieri". Membro del Consiglio Direttivo della Società Italiana per l'Organizzazione Internazionale (SIOI), del Comitato Direttivo dell'Istituto Affari Internazionali (IAI), del Consiglio d'Amministrazione dell'Università "Luiss" e del Gruppo strategico di policy della LUISS School of European Political Economy (SEP). Nel corso della sua lunga carriera diplomatica ha ricoperto numerosi incarichi in Italia e all'estero, ivi compreso quello di Segretario Generale del Ministero degli Affari Esteri (incarico più elevato della carriera diplomatica italiana), svolgendo anche la funzione di Rappresentante personale (Sherpa) del

per la Sicurezza (DIS), realizzata in esclusiva per la presente attività di ricerca. I contenuti della stessa, che viene riproposta in Appendice 2, evidenziano innanzitutto che una intelligence strutturale all'interno dell'UE così come tradizionalmente intesa non c'è, né è ipotizzabile una sua costituzione nel futuro. I motivi sono vari e spaziano dalla vacuità di un interesse comune in UE alla insussistenza di presupposti identitari mai realizzati. Esiste invece una condivisione di dati per affrontare tematiche urgenti, condivise e difficilmente affrontabili senza un proficuo scambio. Si tratta di modalità di "data sharing" già attuate nel contrasto alle minacce terroristiche di matrice jihadista, con risultati positivi. Certamente, tra servizi di intelligence dei vari Paesi si collabora ma con i dovuti distinguo e non senza difficoltà. Tra le intelligence infatti si predilige uno scambio sulla base di reciproci interessi. Dati più complessi/prodotti di intelligence possono essere condivisi in un determinato momento e allorquando vi è richiesta specifica in un settore o in un'area geografica. In questo senso anche il Paese con minore peso specifico potrebbe riuscire a dare informazioni/prodotti settoriali di alto livello e comunque di estremo interesse a Paesi più "importanti", ricevendo, a sua volta, analoghe informazioni/prodotti utili. Tra le difficoltà presenti va evidenziata una serie di differenze sostanziali tra i vari Paesi che interessano il profilo della cultura, delle tradizioni, della legittimazione generanti ovviamente diverse procedure standardizzate, diversi propensione ai fabbisogni di sicurezza, diversa gradualità nell'accettazione delle minacce e diversi approcci alla cultura della sicurezza. Con riferimento ad una eventuale autonomia strategica dell'UE, al momento non sembrano esservi i presupposti. Una direttrice praticabile può essere quella di un incremento delle capacità militari e tecnologiche al fine di poter usufruire di uno strumento militare più strutturato e in grado di affrontare maggiori sfide. Tali incrementi porterebbero dunque l'Unione a una rivalutazione del proprio ruolo e, seppure non fornendo una autonomia in termini assoluti, potrebbero portarla a operare con una relativa maggiore autonomia, ricoprendo ruoli finora non potuti svolgere. Il legame con l'Alleanza Atlantica e con gli Stati Uniti è oggettivamente indispensabile. Le minacce alla sicurezza nel frattempo si

Presidente del Consiglio dei Ministri in occasione degli incontri internazionali G8 e G20 del periodo 2008-2009. Dal 2012 al 2016 è stato Direttore Generale del Dipartimento delle Informazioni per la Sicurezza (DIS).

sono moltiplicate e diversificate. Si tratta di minacce fluide, asimmetriche e multiformi, elaborate anche attraverso tecniche legate allo sviluppo dell'intelligenza artificiale, sulla base delle quali risulta sempre più difficile l'attribuzione di azioni ostili portate avanti da "nemici" non facilmente catalogabili. In virtù di questo l'intelligence oggi è chiamata ad adeguarsi a questi mutamenti e sviluppare idonee capacità di discernimento nei settori chiave sopra riportati a cui vanno aggiunti quello economico finanziari e quello energetico e per fare questo ha necessità di un rinnovamento delle professionalità in grado di governare le molteplici innovazioni tecnologiche ma allo stesso tempo dovranno essere in grado di elaborare sofisticati processi di analisi attraverso una delle capacità più tradizionali: il fattore umano.⁸⁴

⁸⁴ 13.09.2021: annesso 2 – Intervista Amb. Giampiero Massolo

Capitolo 3. Difesa e Intelligence comuni: uno sguardo al futuro

3.1 La collaborazione UE NATO nella Difesa e la sfida alle minacce ibride.

3.1.1. terminologia e aspetti

La nozione di minaccia ibrida, sin da quando è entrata a far parte del lessico della Difesa è ritenuta molto controversa stante il profilo di astrattezza della locuzione, anche se in linea di massima si è concordi nell'includere in essa tutta una serie di operazioni/attività caratterizzate da metodi convenzionali e non convenzionali sotto il coordinamento di soggetti statali e non statali, portate avanti senza oltrepassare la soglia di un formale conflitto bellico, con l'obiettivo di provocare danni, sfruttare vulnerabilità e, in un quadro ancor più complesso, creare turbative ed ostacoli ai processi decisionali in strutture e società. Nella letteratura scientifica settoriale resta comunque un riferimento la visione proposta da Frank G. Hoffman⁸⁵ considerato uno dei maggiori teorici dello sviluppo dei nuovi concetti strategici in grado di contrastare le minacce ibride che ha proposto un elenco delle caratteristiche proprie di questo tipo di minacce, in presenza delle quali è possibile legare tale connotazione. Fanno parte di queste caratteristiche:

- insieme di tattiche di combattimento: la minaccia ibrida usa un insieme di tattiche convenzionali e non convenzionali unite ad attività criminali e terroristiche;
- simultaneità: avversari ibridi utilizzano metodologie differenti di conflitto simultaneamente ed in maniera coerente e coordinata;

⁸⁵Dr. Frank G. Hoffman serves on the Board of Advisors at the Foreign Policy Research Institute and holds an appointment as a Distinguished Research Fellow at the National Defense University in Washington, D.C., where he has served since 2011. He is a retired U.S. Marine Reserve infantry officer with service in the 2nd and 3rd Marine Divisions. His 43 years in the U.S. defense establishment includes 30 years with the U.S. Marines as an analyst and concept developer, two senior political appointments at the Department of Navy and Defense Department, and service on two Congressional commissions. He was selected and confirmed to the Senior Executive Service in 2009. During 2017, Dr. Hoffman was the Special Assistant to the Secretary of Defense and worked on the *National Defense Strategy*. <https://www.fpri.org/contributor/frank-hoffman/>

- fusione: la minaccia ibrida vede l'impiego contemporaneo di militari professionisti, terroristi, guerriglieri, e organizzazioni criminali;
- criminalità: la minaccia ibrida usa attività criminali per sostenere le proprie operazioni e, talvolta, le utilizza palesemente come metodo di conflitto.

Su tali basi è possibile affermare che possono rientrare in tale categoria, anche operazioni di tipo militare, cyber attacchi ad infrastrutture critiche, campagne di fake news, di manipolazione dei social network, ingerenze nei settori economico-finanziari di un Paese, disinformazione mediatica in occasione di consultazioni elettorali, ma anche attacchi di tipo chimico, biologico, radiologico e nucleare. Significativa appare in tal senso la definizione in ambito NATO in base alla quale l'*hybrid warfare* è definita come l'impiego di strumenti militari e non-militari e di mezzi segreti e non, quali la disinformazione, i cyber-attacchi, la pressione economica e l'uso di gruppi armati irregolari, per confondere le linee tra guerra e pace e seminare il dubbio nella mente delle popolazioni bersaglio per destabilizzarle e ottenere un vantaggio politico:

Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies. The speed, scale and intensity of hybrid threats have increased in recent years. Being prepared to prevent, counter and respond to hybrid attacks, whether by state or non-state actors, is a top priority for NATO.⁸⁶

Il carattere di questo tipo di conflitti emergenti è abbastanza complesso; non è più possibile oggi misurare il conflitto su parametri che ne indicano la grandezza o la regolarità. Unitamente alla consapevolezza che il conflitto di tipo tradizionale non è del tutto estinto va sviluppata la coscienza che gli avversari o antagonisti, oggi possono muoversi su scenari completamente diversi rispetto al passato potendo disporre di tecniche e strategie combinate: forze convenzionali, non convenzionali, combattenti regolari e non, dimensioni fisiche/cinetiche e ambiti virtuali di contrapposizione sono solo alcuni degli elementi che hanno ormai alternato i canoni classici del conflitto. Le vulnerabilità sono studiate e sfruttate

⁸⁶ https://www.nato.int/cps/en/natohq/topics_156338.htm

dai competitors a qualsiasi livello e la rigidità mentale che finora ha caratterizzato scelte e strategie, deve assolutamente lasciare spazio a una maggiore creatività nel fronteggiare un nemico in grado di insidiare l'economia, e di penetrare gli ambiti della sicurezza attraverso modalità asimmetriche e tattiche innovative. Trattandosi di attività afferenti i profili della difesa e della sicurezza, ogni Paese ma ancor più le istituzioni comunitarie e i partenariati di difesa, si sono visti costretti a elaborare politiche atte a contrastare queste nuove minacce, come spesso citato negli approfondimenti di Hoffmann:

*“They will not remain static or subject to predictive analysis, but will continuously evolve and exploit the diffusion of innovative tactics, techniques and procedures that offer the greatest return on investment. This assessment suggests an increasingly complex environment for future irregular conflicts that will require institutional adaptation and significantly more attention than it receives today”.*⁸⁷

3.1.2. La pianificazione delle politiche

Sin dal 2002, la NATO ha mosso i primi passi per la pianificazione di politiche strategiche idonee a fronteggiare le minacce ibride, seguendone la loro inarrestabile evoluzione, ponendosi immediati obiettivi quali l'accrescimento da parte dei paesi membri, della consapevolezza della loro pericolosità, l'individuazione delle stesse e il rafforzamento delle capacità di resilienza in caso di attacchi. Si tratta di politiche che investono molteplici ambiti e che si intersecano con sistemi giuridici di varia strutturazione ma che vengono portate avanti attraverso la sottoscrizione di protocolli d'intesa con tutti i partner, consapevoli dell'efficacia di un'azione comune. Sono state quindi sviluppate partnership strategiche sia in ambito privato (*Nato Industry Cyber Partnership*⁸⁸) e

⁸⁷ Hoffmann F.G.: Conflict in 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, Arlington, Virginia, December 2007

⁸⁸ The NATO Industry Cyber Partnership, endorsed by Alliance leaders at 2014 Wales Summit, fosters timely information sharing on cyber threats, allowing participants to enhance their situational awareness. The bilateral information sharing includes information on cyber threats and information security best practices, as well as cyber threat indicators and mitigation measures. Partners are also encouraged to share reports of intrusion events, participate in damage assessments with the NCI Agency and report any cyber security incident that may be of interest to NATO. The Programme aims to increase awareness of cyber threats to NATO and its partners, enhancing and supplementing everyone's capabilities to safeguard information. It is also a relevant initiative for small and medium enterprises, which can often provide innovative solutions in cyberspace. In order to join the Programme, the entity must be from a NATO member Nation.

sia in ambito UE (*Technical Arrangement on Cyber Defence*⁸⁹), il tutto finalizzato a un coordinamento più globale dell'Alleanza che fonda le sue basi nel *Nato Defence Planning Process*⁹⁰, framework che consente di pianificare le risorse e le capacità ottimali necessarie:

*Through the NDPP, NATO identifies the capabilities that it requires, and promotes their development and acquisition by Allies. The NDPP provides a framework within which Allies harmonize their national defence plans with those of NATO, without compromising their national sovereignty. The NDPP apportions requirements to each Ally as Capability Targets on the basis of a fair share of the overall requirement, facilitates their implementation and regularly assesses progress. NATO defence planning encompasses 14 different planning domains, each of which is involved in capability development. The NDPP aims to provide a common framework that can minimise duplication and maximise coherence across the various planning domains.*⁹¹

Un importante passo, sotto il profilo giuridico-istituzionale è stato compiuto nel 2014 anno in cui è stata sancita, anche per gli ambiti in esame, l'applicabilità dell'art. 5 del Trattato Atlantico che prevede l'assistenza collettiva a un Paese alleato qualora questo risulti vittima di attacco armato e infine nel 2016 con il formale riconoscimento del cyber spazio quale dominio per operazioni di guerra e in ragione di ciò è stato predisposto il *Cyber Defence Pledge* che contempla le possibilità per tutti i Paesi aderenti di dotarsi di idonee capacità organizzative e tecniche sia per proteggersi e sia per sfruttare il dominio del cyber spazio, per la conduzione di operazioni militari:

Potential partners will also need to show that they are in a position to contribute a balanced share of information. Requests for participation are reviewed by the NCI Agency on a case-by-case basis. <https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html>

⁸⁹The Technical Arrangement is a concrete example of NATO and the EU working together to enhance shared security. It is also the latest example of long-standing cooperation on cyber defence between the two organizations. In addition, cyber defence staff from the European Union have participated for several years in NATO's flagship annual cyber defence exercise Cyber Coalition. https://www.nato.int/cps/en/natohq/news_127836.htm

⁹⁰The aim of the NATO Defence Planning Process (NDPP) is to provide a framework within which national and Alliance defence planning activities can be harmonized to enable Allies to provide the required forces and capabilities in the most effective way. It should facilitate the timely identification, development and delivery of the necessary range of forces that are interoperable and adequately prepared, equipped, trained and supported, as well as the associated military and non-military capabilities, to undertake the Alliance's full spectrum of missions. https://www.nato.int/cps/en/natohq/topics_49202.htm

⁹¹Organization for Economic Co-operation and Development, "Framework for policy Coherence for sustainable development", building policy coherence, draft for discussion, 2015, <https://www.oecd.org/gov/pcsd/TOOLKIT%20FRAMEWORK%20FOR%20PCSD.pdf>

“1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea. ...”6. To track progress on the delivery of our Pledge, we task an annual assessment based on agreed metrics, and we will review progress at our next summit”.

L’Unione Europea ha mostrato di recepire tutte queste indicazioni, promuovendo anch’essa, in taluni casi anche in collaborazione con l’Alleanza, una serie di iniziative tese ad aumentare i profili della sicurezza. Il documento principale che sintetizza tale volontà politica, a cui spesso si fa riferimento anche nelle più recenti decisioni è costituito dalla *“Comunicazione congiunta al Parlamento Europeo e al Consiglio - quadro congiunto per contrastare le minacce ibride la risposta dell’unione europea Join/2016/018 del 16.04.2016”*. Da un esame dello stesso si evince la volontà di adottare un approccio globale alla problematica, tramite l’individuazione di 22 settori d’intervento, per contribuire a contrastare le minacce ibride e promuovere la resilienza dell’UE e degli Stati membri, nonché quella dei partner internazionali.

This Joint Communication aims to facilitate a holistic approach that will enable the EU, in coordination with Member States, to specifically counter threats of a hybrid nature by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors. The actions build on existing strategies and sectoral policies that contribute to achieving greater security. In particular, the European Agenda on Security, the upcoming European Union Global Strategy for foreign and security policy and European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy, the European Union Maritime Security Strategy are tools that may also contribute to countering hybrid threats. As NATO is also working to counter hybrid threats and the Foreign Affairs Council proposed stepping up cooperation and coordination in this area, some of the proposals aim to enhance EU–NATO cooperation on countering hybrid threats. The proposed response focuses on the following elements: improving awareness, building resilience, preventing, responding to crisis and recovering.

La maggior parte degli interventi riguardano il miglioramento della consapevolezza dei rischi e la creazione di una capacità di resilienza, basata su una efficace reazione; si passa dal potenziamento della capacità di analisi dell’intelligence al rafforzamento della protezione delle infrastrutture critiche, dal

miglioramento della cybersicurezza alla lotta contro la radicalizzazione e l'estremismo violento. Nel corso degli anni, le due organizzazioni hanno sottoscritto una nuova dichiarazione congiunta a conferma della consolidata condivisione di intenti nella lotta alle minacce della sicurezza comune; tra i settori di interesse ci sono ovviamente la cybersecurity, le minacce ibride, la lotta al terrorismo. A fattori comuni, tutti i documenti, evidenziano la volontà di costruire un nuovo e condiviso approccio all'emergere di tali minacce. Tra questi si ricordano:

Anno 2017

- *Communication on a strategic approach to resilience in the EU's external action.*
- *Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities (Cyber Diplomacy Toolbox).*
- *Joint communication on resilience, deterrence and defence: building strong cybersecurity for the EU.*
- *Action plan to enhance preparedness against CBRN security risks.*

Anno 2018

- *European Council conclusions on the Salisbury attack.*
- *Communication on tackling online disinformation: a European approach.*
- *Report on the implementation of the joint framework on countering hybrid threats.*
- *Communication on increasing resilience and bolstering capabilities to address hybrid threats.*
- *Joint declaration on EU-NATO cooperation.*
- *Action plan against disinformation.*

Più di recente, il documento *Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*,⁹² datato 16 giugno 2020 nel quale si dà atto dei progressi

⁹²“...The implementation of the 74 common proposals remains an on-going and long-term process. It continues to require commitment and concerted efforts from all stakeholders. Based on a pragmatic and flexible approach, EU and NATO staffs remain firmly committed to, and engaged in, taking this cooperation forward in a swift, fully coordinated and coherent way with a view to delivering further concrete results”, Sixth Progress Report, 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

fatti nel settore e si delineano i processi di coordinamento attraverso riunioni in parte tra i rappresentanti del Consiglio Atlantico e Comitato Politico di Sicurezza, ma anche attraverso briefing tematici che includono questioni relative a sicurezza marittima, difesa informatica, contrasto alle minacce ibride e CBRN. Una efficace programmazione strategica non poteva fare a meno di passare attraverso la programmazione di esercitazioni organizzate sulla base di scenari il più possibile diversificati al solo fine di verificare il livello di consapevolezza raggiunto tra i Paesi, il tempo di reazione e affinare le azioni di risposta. Tra queste la *EU-CYBRID*⁹³ e la *Parallel and Coordinated Exercise*⁹⁴, entrambe del 2017, nonché la *EU-Chimera* e la *EU Hybrid exercise* del 2018. Di interesse anche le iniziative specifiche nel settore della disinformazione con la creazione nel 2015 dell'*East StratCom Task Force* primo passo per una visione d'insieme della comunicazione strategica. Istituita per far fronte alle campagne di disinformazione inizialmente provenienti dall'Est Europa, si tratta di una divisione in grado di sviluppare campagne di comunicazione incentrate sulla spiegazione delle politiche UE tra i Paesi del partenariato orientale, capace inoltre di individuare e analizzare le principali tendenze della disinformazione nel duplice tentativo di correggere le narrazioni distorte e creare una maggiore consapevolezza della minaccia. Nel 2017, nello stesso ambito, sono state create *StratCom South e Western*. Frequenti i contatti con il NATO StratCom COE con sede a Riga, Centro di eccellenza dell'Alleanza

⁹³Circa un anno fa il ministero della Difesa estone ha iniziato a organizzare Eu Cybrid 2017, un'esercitazione per i ministri della Difesa dell'Unione europea", che si è svolta il 7 settembre scorso a Tallin "con l'obiettivo di far capire loro perché la cyber security è fondamentale". È quanto ha detto Tanel Sepp, del Dipartimento di Cyber policy del ministero della Difesa estone, intervenendo a un evento sulla sicurezza cibernetica al Centro Studi Americani di Roma nell'ambito del Festival della Diplomazia."Altro aspetto interessante", ha aggiunto, "è che tutti i ministri hanno riconosciuto la rilevanza del ruolo della Nato in campo cyber. La cooperazione tra Ue e Alleanza atlantica è quindi evidente in questo settore.CybersecurityItalia.org., <https://www.cybersecitalia.it/tanel-sepp-la-nascita-eu-cybrid-serve-aumentare-la-consapevolezza-dei-leader-europei/3707/>

⁹⁴ The EU launches today, 28 September 2017, for the first time an exercise to test its crisis response tools and mechanisms to counter cyber and hybrid threats. The Parallel and Coordinated Exercise – PACE17 – will lay out a scenario of a hybrid threat affecting the EU and its Member States and test throughout one week, until 4 October, their reactivity to such security challenges. The objective of the exercise is to enhance preparedness and evaluate the effectiveness of EU instruments and mechanisms in case of an eventual attack, as well as to consequently propose improvements where needed. A separate crisis management exercise will be conducted by NATO from 4 to 11 October 2017. NATO's CMX17 exercise and PACE are conducted independently, but in a parallel and coordinated manner, ensured by EU – NATO staff-to-staff coordination and participation throughout both exercises. The aim is to improve the synchronisation of crisis response activities between the two organizations. EEAS archives, https://www.eeas.europa.eu/node/32969_en

Atlantica, il cui compito è quello di fornire a tutti i Paesi, analisi comprensive, consigli e supporto pratico per una risposta ad attacchi sul versante della comunicazione strategica.

3.1.3. Le principali iniziative e implicazioni nelle politiche di Difesa

Tra le iniziative considerate maggiormente efficaci e rappresentative si ricorda l'istituzione nel 2016 della *Hybrid Fusion Cell* divenuta operativa nel 2017 e inserita all'interno del centro di intelligence *IntCen*, funzionale alla ricezione e all'esame delle informazioni anche riservate, sulle minacce ibride, provenienti dalle varie parti interessate.

An EU Hybrid Fusion Cell will offer a single focus for the analysis of hybrid threats, established within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). This Fusion Cell would receive, analyse and share classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU Delegations), the Commission (with EU agencies), and Member States. In liaison with existing similar bodies at EU and at national level, the Fusion Cell would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood, in order to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level. The Fusion Cell's analytical output would be processed and handled in accordance with the European Union classified information and data protection rules. The Cell should liaise with existing bodies at EU and national level. Member States should establish National Contact Points connected to the EU Hybrid Fusion Cell. Staff inside and outside the EU (including those deployed to EU delegations, operations and missions) and in Member States should also be trained to recognise early signs of hybrid threats.⁹⁵

Le analisi prodotte sono successivamente condivise con i partner e alimentano il processo decisionale contribuendo alla valutazione dei rischi relativi alla sicurezza. La direzione intelligence del *Military Staff* contribuisce alle funzioni della cellula, con un'attività di intelligence militare più specifica. Frequenti le attività di information sharing a livello del personale con la nuova sezione della NATO per

⁹⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>

l'analisi delle minacce ibride, sia per quanto concerne le conoscenze acquisite nell'attività specifica e sia quanto concerne lo scambio di informazioni riservate detenute dai singoli Paesi e funzionali alle attività. Nello stesso contesto, nel mese di aprile del 2017, si ricorda la creazione dell'*European Centre of Excellence for Countering Hybrid Threats* un centro di eccellenza sulle minacce ibride, con sede a Helsinki, inizialmente composto da 9 Paesi firmatari, che con il passare del tempo ha visto l'ingresso e la partecipazione a vario titolo di 28 Stati.

Hybrid CoE is an international, independent network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats. While understanding the changing security environment is essential, it is not enough to analyse the threats, but also to provide concrete tools for countering them. Hence, the Centre's key task is to build participating states' capabilities to prevent and counter hybrid threats. This is done by sharing best practices, testing new ideas and approaches, and providing training courses and exercises.⁹⁶

I compiti principali dell'*HybridCoE* (come viene più comunemente chiamato) sono quelli di promuovere il dialogo e le consultazioni a livello strategico tra l'UE e la NATO e adeguare le attività delle organizzazioni per affrontare meglio tali minacce, condurre ricerche e analisi su minacce ibride e sviluppare azioni tese al loro contrasto, predisporre la formazione e l'organizzazione di esercitazioni volte a migliorare le capacità individuali dei partecipanti, nonché l'interoperabilità tra gli stessi. È organizzato su tre gruppi principali o *Communities of Interest*: *Hybrid Influencing* (coordinato dal Regno Unito), *Vulnerabilities and Resilience* (coordinato dalla Finlandia) e *Strategy and Defence* (coordinato dalla Germania). Dispone inoltre di due team che lo affiancano in attività specifiche: si tratta del *training and exercises team* che promuove e pianifica esercitazioni sperimentando diversi scenari di minacce ibride e il *research team* specializzato sulla promozione e studio di ricerche accademiche e sul confronto dei principali ambiti di interesse. Nello specifico, l'attività dei tre gruppi è la seguente:

- *Hybrid Influencing*: analizza le modalità con le quali gli attori statali e non statali conducono attività di disinformazione destinate a Stati membri e istituzioni; si concentra sulle modalità con le quali usano i loro strumenti di influenza al fine di creare instabilità o nell'intento di ridurre la sovranità o

⁹⁶ <https://www.hybridcoe.fi/who-what-and-how/>

l'indipendenza delle istituzioni. Il focus dell'analisi comprende quindi i comportamenti, le attività e gli strumenti utilizzati dai potenziali attori ostili, nell'intento di fornire gli strumenti necessari, di volta in volta, per rispondere o scoraggiare le minacce ibride. Questo gruppo è ripartito in un gruppo secondario che rivolge la sua attenzione agli attori non statali spesso in azione per conto di soggetti terzi.

- *Vulnerabilities and Resilience*: opera una accurata valutazione delle vulnerabilità degli partner e delle istituzioni e interviene sul miglioramento della loro capacità di resilienza attraverso la condivisione di *best practices*, lo sviluppo di nuove proposte politiche e l'identificazione di argomenti da approfondire. L'obiettivo è anche quello di migliorare il partenariato pubblico-privato e civile-militare per contrastare le minacce ibride.
- *Strategy and Defense*: si occupa della guerra ibrida, delle strategie correlate e delle conseguenti implicazioni per la politica di sicurezza, militare e di difesa. Studia l'essenza e la natura della guerra ibrida, nonché la logica e il modello delle strategie ibride al fine di sviluppare un quadro analitico per la valutazione delle attuali e future minacce e delle loro implicazioni pratiche. L'obiettivo generale è quello di contribuire a formare e accrescere una cultura comune nei partecipanti (UE e NATO) verso tale realtà, indispensabile quale condizione preliminare per un'azione congiunta ed efficace sia in un'ottica di difesa e sia in risposta ad attacchi.

Le minacce ibride non sono un fenomeno nuovo ma col tempo hanno assunto una strategica importanza nel contesto delle politiche di difesa, rimettendo in discussione vecchi schemi e comportamenti consolidati, non più idonei a fronteggiare tali emergenze. Certamente l'efficacia di un conflitto condotto attraverso metodologie sinergiche di questo tipo, dipende in gran parte dalla superiorità attestata al regime politico del paese oggetto di interesse ma anche questo criterio presenta delle riserve nel momento in cui deve essere opportunamente considerata l'interazione combinata di tecnologie digitali emergenti, delle attività di informazione/disinformazione e non ultime delle operazioni condotte nel dominio cyber. Proprio per tali ragioni è fondamentale per ogni paese, dotarsi di misure proattive e strategiche per prevenire con efficacia scenari con operazioni ibride, aumentando la capacità di riconoscere tali

minacce. Tendenzialmente si è portati a pensare che solo le grandi potenze siano in grado di porre in essere tali tipologie di operazioni e portare avanti conflitti su larga scala. In realtà una caratteristica delle minacce ibride è quella di poter essere attuate anche da piccoli paesi, gruppi non statali e persino singoli elementi che in qualche modo hanno interessi a sovvertire o colpire il paese o il gruppo definito come bersaglio. La presenza di minacce ibride pone un quesito essenziale nei processi decisionali strategici, e cioè quale tipo di politiche di difesa adottare per contrastare tali emergenze. Questa difesa, come più volte accennato, deve essere mutevole, non dogmatica e aperta a soluzioni e prospettive diverse. Probabilmente si potrà anche ricorrere al termine di “difesa ibrida” già usato da Brin Najzer. Non è certamente semplicistico affrontare la tematica. Il comparto della Difesa dovrebbe occuparsi della sicurezza nel suo complesso e sforzarsi di individuare le criticità delle forze militari convenzionali, nel tentativo di correggerle, parallelamente a ciò dovrà saper intervenire su settori quali politiche sociali, economiche e di sviluppo, settori dai quali possono arrivare le più gravi minacce. Altro sforzo dovrà essere fatto relativamente al dominio cyber e a un processo di intelligence sharing frutto di un sistema cooperativo di tipo inter-organizzativa che NATO e UE perseguono da tempo seppure con evidenti limiti dovuti in parte a una strategia frammentaria e in parte a politiche di breve o medio termine che mal si conciliano con tematiche da affrontare in un lasso di tempo ancora più lungo. Strategiche si dimostreranno le future politiche imperniate sulla difesa delle infrastrutture critiche digitali, prescindendo dalle “transizioni digitali” che ogni paese si preparerà ad affrontare. Anche in questo caso diventerà indispensabile una collaborazione tra settore Difesa e Pubblica Amministrazione che, insieme, potranno confrontarsi per una più efficace tutela, che avrà un senso, quanto più ci sarà precisione nell’individuazione delle IC per una migliore attività di prevenzione e di pianificazione. Determinante, si rivelerà, una adeguata politica spaziale perché si tratta di altro dominio operativo strettamente connesso a quello cyber.

3.2 La collaborazione UE-NATO nell’intelligence

3.2.1. L’esigenza di maggiore cooperazione

Nel dibattito accademico in corso si apprezza una collaborazione NATO-UE nel settore dell'intelligence, seppure limitata, non adeguata ai tempi e comunque ancora non sviluppata.⁹⁷ Attualmente, l'UE deve affrontare una serie di sfide e minacce inimmaginabile fino a poco tempo fa. Sostanzialmente l'Europa corre il rischio di diventare un soggetto irrilevante nel panorama internazionale e allo stesso tempo oggetto di grande potere attrattivo da parte di potenze esterne. Le sfide alla sicurezza hanno fissato le tre priorità strategiche per la PSDC dell'UE che consistono nella risposta a conflitti e crisi esterne, nel sostenere i partner e, infine, nel fornire sicurezza alla propria popolazione e proteggere l'Unione e i suoi cittadini. Per mantenere fede a tali propositi ha elaborato e sta sviluppando lo strumento dello "Strategic Compass"⁹⁸ per la sicurezza e la difesa, che contribuirà allo sviluppo di un approccio coerente e strategico alle iniziative esistenti e rafforzerà la politica di sicurezza e di difesa dell'UE, tenendo conto delle minacce e sfide che l'Unione sta attualmente affrontando. Definerà una analisi, valida per tutti i Paesi facenti parte, delle principali minacce, determinando gli orientamenti politici e gli obiettivi specifici in quattro ambiti: gestione della crisi, resilienza, sviluppo delle capacità e partenariati. A fattore comune comunque, mira a promuovere lo sviluppo di un comune Cultura europea della sicurezza e della difesa. Non va sottaciuto che il dibattito interno all'Unione su una gestione unitaria alle risposte di crisi è in corso da tempo. Secondo il Prof. Cesare La Mantia,⁹⁹ è interessante osservare come l'attuale pressione statunitense e la situazione conflittuale venutasi a creare nell'est Europa, stiano determinando una risposta

⁹⁷ Walsh J.I. "The International Politics of Intelligence Sharing", Columbia University Press, 2009.

⁹⁸On 21 March 2022, the Council of the European Union released the Strategic Compass for Security and Defence. The document provides a thorough assessment of international affairs and is meant to guide the development of the EU security and defence agenda for the next decade. The Strategic Compass has been hailed as a framework for coherence and convergence of the Union's foreign policy but has also been criticized for its lack of concrete goals, for being a "wind chime" rather than a "compass". Here the focus is on the apparent change of direction in EU foreign policy – at least when compared to the direction taken in the Global Strategy (2016) and the Integrated Approach to Conflicts and Crises (2018). While these documents have their own specific logic and focus, comparing them is useful to understand where the Compass is guiding Europeans to. P. Bargues, The EU Strategic Compass: A Blueprint for a European Defensive and Securitization Policy, IAI, Istituto Affari Internazionali, joint papers, <https://www.iai.it/en/pubblicazioni/eu-strategic-compass-blueprint-european-defensive-and-securitisation-policy>

⁹⁹ Prof. Cesare La Mantia: professore associato presso l'Università degli Studi di Trieste, Storia dell'Europa Orientale, <https://dispes.units.it/it/dipartimento/persona/personale-docente?q=it/node/1232>

quasi unitario che potrebbe in qualche modo favorire la realizzazione del modello unico di Difesa auspicato in più sedi. Tale parere, espresso nel corso di una intervista realizzata in esclusiva per la presente attività di ricerca, riprodotta come allegato, in annesso 3, rappresenta una chiave di lettura interessante sotto certi profili. A fronte di un'esigenza imprevista, di portata storica è stato registrato uno sforzo inimmaginabile prima d'ora da parte dell'Unione che tuttavia continua ad avere un rapporto con la NATO su una base non paritaria ma soggetto ad essa.¹⁰⁰ Nei prossimi anni l'Europa dovrà affrontare nuove e decisive sfide chiave, ancor più decisive se intende realizzare quell'autonomia strategica europea che da tempo viene proposta; in questo contesto e nell'ambito della citata Strategic Compass, è necessaria una maggiore cooperazione per la sicurezza e la difesa, e di una intelligence più adeguata ai tempi e alle sfide. Tuttavia non va sottaciuto che le attività di intelligence sono al centro della sovranità nazionale e questo probabilmente, può essere considerato l'ostacolo più difficile da superare. Tuttavia, nel corso degli anni l'UE ha sviluppato diverse istituzioni per facilitare la condivisione dell'intelligence tra i suoi Stati membri e queste istituzioni svolgono la funzione di creare meccanismi per la diffusione dell'intelligence tra le autorità nazionali. Inoltre, l'intelligence come processo e prodotto è stato fortemente promosso dall'UE come uno strumento utile nella lotta al terrorismo, alla radicalizzazione, alla criminalità organizzata. Ed è stata costituita una serie di agenzie che raccolgono, analizzano e rendere operativa l'intelligence in vista di queste principali minacce alla sicurezza. Esempi sono i citati: INTCEN, Europol e lo stesso SIAC, tutte a sostegno dell'elaborazione delle politiche da parte dell'azione esterna europea Servizio (SEAE). All'interno di questo contesto istituzionale è certamente possibile valutare il miglioramento della cooperazione sull'intelligence europea. Si tratta di un concetto che va al di là della semplice cooperazione interna all'UE perché afferisce sia al profilo civile e sia a quello militare e deve essere affrontato anche dai Paesi, quali il Regno Unito, che pur essendosi chiamati fuori dall'Unione sono comunque interessati a una difesa programmata e interconnessa. Per non parlare di singoli Paesi, esistenti nella regione del Pacifico, che hanno un interesse a cooperare nei settori dell'intelligence e della sicurezza. va da sé che occorre individuare i punti di contatto (o di interesse) comuni a questi

¹⁰⁰ 25.10.2022: Annesso 3, intervista al Prof. Cesare La Mantia

paesi, meritevoli di spingerli a una maggiore collaborazione. Molte sono le domande che gli analisti si sono posti al riguardo e tra le più importanti emergono quelle che cercano di capire in che modo la cooperazione di intelligence nel campo dell'early warning può aiutare l'UE a rispondere a conflitti e crisi esterne, sostenere la protezione dell'Unione e dei suoi cittadini e promuovere lo sviluppo di una cultura europea dell'intelligence comune, e quali sono le opportunità per il continuo impegno dell'intelligence britannica e dei servizi di intelligence di quel Paese, negli accordi di cooperazione europea per affrontare le sfide alla sicurezza dell'UE, concentrandosi sulle dimensioni dei partenariati di intelligence.

3.2.2. Spinte endogene, spinte esogene e slancio cooperativo

Sostanzialmente esistono tre fattori che seppur in modo diverso l'uno dall'altro, influenzano i vari Paesi inducendoli a cercare gli aspetti positivi della cooperazione di intelligence, accettandone contestualmente costi e rischi:

- la domanda interna,
- la pressione esterna
- lo slancio cooperativo in vista di obiettivi futuri.¹⁰¹

Per quanto riguarda la domanda interna, è evidente che essa si fonda sulla consapevolezza che la ragione principale della scelta collaborativa sia da ricercarsi nei meccanismi interni ad ogni paese cooperante. Si tratterebbe per lo più di istanze provenienti sia dal settore pubblico e sia da quello privato che tuttavia investono oltre che il singolo Stato anche la comunità, pertanto è demandata all'istituzione che sovrintende la partnership, la cooperazione che diventa in tal modo funzionale alle esigenze di un singolo che da solo non è in grado di rispondere ad una determinata esigenza, ma anche alla comunità che beneficerebbe comunque di risorse comuni. Notevoli possono essere le esigenze emergenti quali ad esempio il deterioramento della situazione afferente la sicurezza in ragione di nuove sfide o di emergenze contingenti. Bisogni funzionali

¹⁰¹“...As well as generating a more thorough understanding of the costs and benefits of international intelligence cooperation, the study offers important insights into future directions of cooperation and its connection to both national security and international policy-making”. In The theoretical framework constructed in this chapter is based on the work of Björn Fägersten, *Sharing Secrets: Explaining International Intelligence Cooperation* (Lund Political Studies, 2010).

che visti in un'ottica cooperativa assumono lineamenti diversi se si pensa al fatto che il mettere a disposizione risorse comuni potrebbe costituire un vantaggio per tutti con riduzione dei costi diversamente non sopportabili da un singolo paese partner; il prodotto finale risulterebbe fruibile all'intera comunità, con conseguente risparmio sui costi. I principi appena riassunti sono peraltro alla base delle attuali politiche di sicurezza e difesa comune. Con pressione esterna, ci si riferisce a quel fattore, o a quell'insieme di fattori, in base ai quali ogni singolo paese, è chiamato a una scelta di intelligence nuova e imprevedibile che deriva anche da mutamenti dell'ordine internazionale che, pertanto, inducono il singolo paese ad un mutamento nel contesto del sistema stesso. Posto come punto di partenza il dato rappresentativo che tutti gli Stati, anche i più piccoli hanno un margine di manovra all'interno del sistema internazionale e che tale sistema è destinato a modificarsi, va da sé che la postura degli Stati anche dei più piccoli può variare in tale ambito e pertanto varia anche l'interesse e il focus verso il quale dirigere gli sforzi di intelligence in base ad alleanze o situazione di conflittualità. Ad esempio gli equilibri geopolitici di appena venti anni fa sono all'evidenza mutati e pertanto molti Stati si trovano costretti a fare altre scelte rispetto al passato. In tale contesto uno solo o gruppi di essi possono decidere di unire i propri sforzi e proprio a causa della mutazione esogena, far convergere i propri sforzi su un'intelligence che colga opportunità in zone geografiche diverse rispetto al passato o in contesti socio-politici nuovi anche per riequilibrare o dare un assetto di sicurezza adeguato al proprio sistema Paese. Lo slancio cooperativo costituisce uno dei fattori determinanti e, a volte, poco considerati, nelle dinamiche di sviluppo di modelli innovativi, pur riunendo in sé delle caratteristiche determinanti per uno sviluppo innovativo settoriale. In realtà il concetto di cooperazione può essere visto attraverso varie prospettive e cioè sia dal punto di vista qualitativo e sia dal punto di vista quantitativo. Vi è senza dubbio la tendenza a concepire, concettualmente, la collaborazione come risultante da un processo organizzativo e quindi quale momento di conclusione di un meccanismo ideato e organicamente strutturato: ad esempio quando si decide di istituire una struttura cooperativa in ambito di una alleanza esistente o tra diverse partnership, si moduleranno i meccanismi di ingresso, di cooperazione e su tali basi sarà più facile procedere secondo linee guida appositamente predisposte. Tuttavia occorre premettere che

nel settore dell'intelligence tale processo presenta delle differenze proprio in ragione dell'essenza intima trattata ovvero la sicurezza totale del paese. È perciò determinante che il requisito base per poter intraprendere un rapporto di collaborazione sia la fiducia, termine che nel mondo dell'intelligence è pressoché sconosciuto dal momento che viene costantemente sostituito molto più pragmaticamente da una fiducia a scambiarsi dati, prospettive e analisi solo su conveniente convincimento che possa servire a entrambi, oppure nell'ottica di del *"do ut des"* e comunque, in tutti i casi, ciò avverrà in maniera limitata e contingentata all'obiettivo che una delle parti (solitamente quella che gioca su un piano più rilevante) vuole raggiungere. In tale ambito si interseca l'elemento della fiducia spesso sottovalutato, e che invece può coesistere con le dinamiche sopra accennate e che può costituire una spinta propulsiva ad un efficace processo di collaborazione. La fiducia si costruisce col tempo e un partner occasionale o strategico, per essere definito affidabile deve dare garanzie che non si limitino a un lasso di tempo particolare. Spesso si discute su certe alleanze strategiche che vedono la collaborazione di un gruppo ristretto di partner (ad esempio i cd Five Eyes¹⁰²) e qualcuno, erroneamente, si stupisce sulla scelta e sulla ristrettezza del gruppo di partecipanti. La realtà è profondamente diversa e supportata da dati oggettivi abbastanza chiari: si tratta di Paesi che per ragioni storiche, politiche, ideologiche, prospettive, interessi economici sostanziali e scelte strategiche di Difesa, sono intimamente e storicamente legati tra loro da più vincoli difficilmente superabili e non sono soggette a "variazioni d'umore" che potrebbero metterne in discussione la fiducia reciproca. Altro punto da valutare con attenzione nella visione di tali processi è quello della costituzione delle alleanze e del ruolo giocato dai diversi partner. Pur stabilendo le regole in base alle quali, in linea teorica tutti

¹⁰²The Five Eyes (FVEY) is widely regarded as the world's most significant intelligence alliance. The origins of it can be traced back to the context of the Second World War and by its necessity of sharing vital information mainly between Britain and the United States so both countries could enhance their close war effort. The Five Eyes was formally founded in the aftermath of the Second World War, through the multilateral agreement for co-operation in signals intelligence (SIGINT), known as the UKUSA Agreement, on 5 March 1946. Initially, comprising only the UK and the United States, it expanded to also include Canada in 1948 and Australia and New Zealand in 1956, all of these last three English-speaking countries, members of the Commonwealth of Nations and with similar political systems when compared to Britain. Thereby, the 'Five Eyes' term was created from the lengthy 'AUS/CAN/NZ/UK/ Eyes Only' classification level that included the 'eyes' that could have access to high profile papers and information. "The Five Eyes. The intelligence Alliance of the Anglosphere", J.V.Tossini, april 2020, <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>

gli appartenenti alla struttura cooperativa idealmente dovranno muoversi (qualsiasi paese è membro a pieno titolo con pari status formale), è fin troppo evidente che nella realtà ci sono e ci saranno paesi che rivestiranno un ruolo preminente perché preminente è il peso strategico assunto a livello internazionale. Si riscontra quindi all'atto pratico una gerarchia che in qualsiasi momento della vita di questa o quella organizzazione cooperativa, determinerà una maggiore incidenza rispetto alle decisioni e alle priorità degli altri; tale aspetto potrebbe rivelarsi determinante in particolari circostanze in cui il paese che ricopre un ruolo minore potrebbe addirittura vedere limitate le proprie possibilità a beneficio del partner con maggior peso fino a subirne scelte e condizionamenti anche in termini di rischi ed effetti negativi.

3.2.3. Intelligence warning system

Il rafforzamento della collaborazione nell'ambito dell'intelligence europea può essere la risposta alla percezione degli Stati membri dell'UE di dover affrontare problemi che diversamente non sarebbero in grado di affrontare unilateralmente. Sottende, evidentemente, a una maggiore capacità di intelligence in quanto gli Stati membri dell'UE percepiscono che solo in tal modo possono raggiungere una maggiore efficienza se dovessero operare in uno sforzo comune. La motivazione di fondo delle richieste interne, va certamente a vantaggio di una cooperazione nel settore degli early warning che può aiutare l'UE a rispondere meglio ai conflitti esterni e alle crisi, ma allo stesso tempo potrebbe essere in grado di sostenere la protezione dell'Unione e dei suoi cittadini e infine di promuovere lo sviluppo di una cultura comune dell'intelligence europea. In quest'ultimo aspetto dovrebbero rientrare in una componente unica e omogenea, le norme di comportamento condivise, la capacità di pensare collettivamente alle future sfide e alle minacce della sicurezza.¹⁰³ Gli apparati di intelligence affrontano oggi nuove priorità che si affiancano a quelle più tradizionali, proprio perché si configurano nuove minacce alle quali non sempre è facile fornire una risposta: cambiamenti climatici,

¹⁰³ Van Puyvelde D., "European Intelligence Agendas and the Way Forward," *International Journal of Intelligence and Counterintelligence* 33, no. 3 (2020): 508; Yvan Lledo-Ferrer and Jan-Hendrik Dietrich, "Building a European Intelligence Community," *International Journal of Intelligence and Counterintelligence* 33, no. 3 (2020): 440-451.

pandemie, conflitti ibridi, richiedono nuove forme di cooperazione e le soluzioni a queste minacce non sempre sono facili da trovare e quando vengono prospettate non sempre c'è una volontà politica di affrontarle. Allo stesso tempo va considerato il numero crescente di rischi transnazionali derivanti dalla trasformazione delle nostre società, anch'esse in rapida trasformazione, tali da richiedere una sempre maggiore collaborazione a livello internazionale. Vista da questa prospettiva, la cooperazione dell'intelligence europea potrebbe essere considerata come una naturale estensione dell'alto livello di interconnessione che caratterizza il continente europeo e le sue politiche di integrazione comunitarie. Nel processo di gestione delle crisi, diventa indispensabile fornire ai decisori politici un qualificato alert, circa un potenziale scoppio, escalation e recrudescenza di una situazione di criticità e promuovere, conseguentemente, una migliore comprensione di quanto stia per verificarsi e dei potenziali impatti. È indispensabile arrivare in anticipo: prima viene rilevata una potenziale crisi, più facile diventerà impostare una strategia che tenda a ridurre gli effetti o a prevenirla laddove sia possibile farlo.¹⁰⁴ La maggiore complessità dell'ambiente di sicurezza sottolinea la necessità che i responsabili politici e la comunità dell'intelligence inizino a pensare su sistemi di alert precoci e più sofisticati ma soprattutto condivisi. Sarà compito dell'intelligence, in questo caso, di fornire un'analisi più complessa, sondare e cercare di identificare e dare un senso a fenomeni insoliti e non ancora definiti nel tempo, ovvero poter dare senso a possibili scenari multipli. In tale contesto, analisti e politici dovranno giudicare e valutare insieme quali dovranno essere gli interventi di risposta immediata e quali cominciare a costruire in prospettiva. Finora l'UE aveva guardato ai conflitti, più o meno violenti in varie aree del mondo. Oggi probabilmente deve correggere quest'ottica e non sottovalutare aree più vicine e altrettanto sensibili (Balcani e Europa orientale) impegnandosi a fondo se vuole mantenere il desiderato ruolo di attore della sicurezza. Un esempio pratico di sforzo comune per una collaborazione settoriale è stato operato già da alcuni anni proprio nel settore degli alert. Già a partire dal 2014, al fine di rafforzare le capacità predittive e preventive, il SEAE e la Commissione europea hanno implementato il sistema di

¹⁰⁴ Gaub, F. "Enhancing early warning and preparedness," in *Crisis Rooms: Towards a global network?*, eds. Patryk Pawlak and Andrea Ricci (Paris: European Union Institute for Security Studies, 2014)

allerta precoce (EWS Early Warning System) in caso di conflitto. L'istituzione di questo sistema trae origine da quanto sancito all'art. 21 del Trattato dell'Unione Europea, nella parte in cui recita che la prevenzione dei conflitti è uno degli obiettivi principali di politica estera dell'UE. Un chiarimento del dispositivo è stato dato nel corso del 2019 dal SEAE che così ne ha discusso parlando del *“Sistema di allerta precoce dei conflitti dell'UE: obiettivi, processo e linee guida per l'attuazione”*:

Article 21(2)(c) of the Treaty on European Union explicitly names conflict prevention as one of the EU's foreign policy goals. The 2011 Council conclusions on Conflict Prevention have elaborated this point and provide a strong mandate for the EU to engage in conflict prevention. In order to identify structural risk of conflict and prevent the emergence or escalation of violent conflict and prevent the emergence, re-emergence or escalation of violent conflict, early warning capabilities are indispensable. In its conclusion, the Council considers that conflict early warning needs to be further strengthened within the EU and that output from all sources, including from Member States, should be better integrated; conflict early warning should draw more extensively upon field-based information, including from EU Delegations and civil society actors, in order to provide a more solid foundation for conflict risk analysis. Enhancing conflict early warning will also enable the EU to work more effectively with partners on issues regarding the responsibility to protect and the protection of human rights. Finally, Council conclusions stress that more emphasis needs to be put on early action to mitigate the risks of outbreak and recurrence of conflicts. In follow-up to these conclusions, the European External Action Service (EEAS) and Commission Services have put in place the EU conflict Early Warning System (EWS) as part of their broader activities in the field of security policy. The procedures and methodology of the system were tested in two regional pilot studies in 2012 and 2013, before the system was rolled out in September 2014 for all non-EU countries. The EWS is a key component of the EU's Comprehensive Approach to External Conflict and a key component of the EU's Comprehensive Approach to External Conflict and Crises (2013) and applies to the complex context of EU external action implemented by the EU and Member States. This Joint Staff Working Document is a deliverable of the 2015 Action Plan for the Comprehensive Approach. The purpose of this Joint Staff Working Document is to serve as basis for the interservice collaboration for

*the functioning of the EWS. To this end, this document describes EWS objectives and scope, components and stakeholders*¹⁰⁵

In tale contesto, ma soprattutto nell'ambito dell'intensificata collaborazione tra l'UE e la NATO, è importante esaminare le aree in cui entrambe le organizzazioni potrebbero imparare l'una dall'altra. Per eseguire questo parallelismo occorre prendere in considerazione il sistema di alert precoce predisposto dalla NATO, ovvero il NATO Intelligence Warning System (NIWS). Da un lato quindi abbiamo il sistema europeo, all'interno del quale, al fine di aiutare a informare il ciclo di allerta, il SIAC¹⁰⁶ ha il compito di sviluppare analisi specifiche per l'EWS. Queste analisi sono sviluppate seguendo un criterio di tipo geografico, concentrandosi su sei regioni del mondo, in un arco di tempo di tempo a medio-lungo termine (fino a 4 anni). Le analisi SIAC si concentrano sui fattori di rischio strutturali e sui fattori di resilienza, nonché sul ruolo degli attori esterni e il rischio di ricadute. La NATO ha ridisegnato i suoi NIWS nel 2002 allo scopo di condividere le conoscenze acquisite e le informazioni, in maniera sintetica e fruibile.¹⁰⁷ La metodologia NIWS si estrinseca attraverso una formulazione di un "warning problem": una dichiarazione chiara e concisa, descrivendo il problema di avvertimento di interesse per l'Alleanza. Si fa una distinzione tra problemi di allerta convenzionali (riguardanti un singolo paese) e transnazionali. Il ciclo di allerta della NATO è diviso in cinque fasi:

- *definire la minaccia*
- *sviluppare scenari*
- *sviluppare indicatori di criticità*

¹⁰⁵ SEAE site "EU Conflict EWS – objectives, process and guidance for implementation, https://knowledge4policy.ec.europa.eu/publication/eu-conflict-early-warning-system-objectives-process-guidance-implementation_en

¹⁰⁶ Since 2007, the EU INTCEN is part of the Single Intelligence Analysis Capacity (SIAC), which combines civilian intelligence (EU INTCEN) and military intelligence (EUMS Intelligence Directorate).

¹⁰⁷ NCRS is a comprehensive Crisis Management system and all planning processes shall comply with it. Furthermore, the system is linked with other key systems, processes and procedures, such as: • NATO Intelligence Warning System - NIWS; • NATO Operations Planning Process; • NATO Civil Emergency Planning; • Rules of Engagement. NCRS's aim is to help prepare the system forces and resources needed to prevent and manage crises and conflicts in the spectrum of operations under article 5 of the Washington Treaty, and beyond it. It improves the capability of NATO and its partner nations to prepare to respond to the full spectrum of possible crises, in which they may be involved. Thus, the system has a full range of measures for timely response. NATO and National CNRS, Analysis, file:///C:/Users/255793cz/Downloads/20150311055641_NATO_And_National_CRMS_EN_Report_v6_4.pdf

- *raccogliere informazioni*
- *inviare avvisi.*

Gli avvisi o report vengono elaborati, solitamente, con cadenza mensile, secondo una struttura orientata su tre livelli. Ad un primo livello si offre una sintetica panoramica della situazione e una valutazione preliminare utile ai decisori; al secondo livello vengono approfondite le tematiche ritenute più aderenti e vengono esplicitati i vari aspetti delle minacce; l'ultimo livello prevede un elenco di indicatori critici costituenti i potenziali risvolti cruciali della situazione e di come possono essere valutati. Tali indicatori possono coprire un'ampia gamma di aspetti e afferiscono a diversi settori quali quello economico, politico, militare, sociale etc. Sostanzialmente la procedura insita nel sistema NIWS ha lo scopo di alimentare il processo di valutazione delle crisi in ambito NATO: qualora uno di questi avvisi risulti essere significativo, si attiverà il sistema conseguente, attraverso il quale, tramite interlocuzione con il Comitato Nord Atlantico, dovrà essere predisposta una adeguata risposta. Una immediata comparazione tra il sistema di allerta Ue e quello NATO, potrebbe istintivamente portare a ritenerli molto simili, mentre in realtà la prima ma sostanziale differenza si intravede nel fatto che mentre il sistema NATO focalizza la sua attenzione su un fattore specifico, quello dell'Unione opera su un contesto geografico abbastanza ampio, come detto suddiviso in sei macroregioni, attraverso un approccio più geografico che su scenari specifici. Altra differenza è costituita dal fatto che, a monte, troviamo due strutture o meglio due alleanze profondamente diverse tra loro: da una parte l'Unione Europea che ha interesse a valutare anche situazioni di instabilità economica o politica, mentre dall'altra parte troviamo l'Alleanza Atlantica, struttura tipicamente militare, con obiettivi, partecipazioni e interessi più strategico-tattici e con una struttura di intelligence settoriale. Altra differenza risiede nella durata del ciclo di "alert" nel senso che per essere completato, il ciclo EWS ha bisogno di due anni e mezzo. Al contrario i rapporti NIWS sono progettati su un lasso di tempo di novanta giorni con aggiornamenti mensili da parte dei Paesi interessati e peraltro spesso confortati da concomitanti analisi areali rientranti in una strategia NATO che annualmente rivede priorità e focus di interesse. Nel corso degli anni si è assistito ad un percorso parallelo su più sfide che certamente accomunano UE e NATO: gli alert sulle aree di crisi costituiscono certamente un

tema da affrontare con prontezza e sinergia. Tanto più che le minacce col passare del tempo si sono diversificate e, solo a titolo di esempio, da pochi anni è entrato prepotentemente nel linguaggio comune il termine di minaccia ibrida spesso con significati e interpretazioni diverse da paese a paese ma sempre con la consapevolezza che la presenza di questo tipo di minaccia obblighi a tenere un atteggiamento diverso dal passato, al fine di adottare le idonee misure di contrasto. In tal senso il Centro di eccellenza europeo di Helsinki, per le minacce ibride (Hybrid-CoE), in ambito NATO si è rilevato fondamentale nel produrre un consolidamento delle basi concettuali relativamente alle varie forme di minacce ibride, anche attraverso numerose pubblicazioni e analisi a beneficio di istituzioni accademiche e politiche europee. Questo è uno degli elementi più qualificanti della produzione di analisi di intelligence e lo è ancor più perché alcune di queste analisi sono state condivise con la cellula Hybrid Fusion Cell interna all'INTCEN, evidenziando una stretta collaborazione tra UE e NATO. La prospettiva di una intelligence comune o ancor meglio di una comune cultura dell'intelligence è molto lontana. Si potrà obiettare che molti servizi di intelligence di vari paesi lavorano assieme ma tuttavia si tratta per lo più di casi singoli e legati a una logica binaria che interseca gli interessi reciproci e che al variare delle condizioni sociali, economiche, politiche, può con altrettanta facilità variare, ribaltando i rapporti. Restano ammirevoli i tentativi di cercare uno spazio comune di dialogo tra le intelligence, come già citato in questa ricerca, relativamente alla struttura denominata ICE ovvero l'Intelligence College Europe. Pur non trattandosi in senso stretto di un'accademia o di un college può definirsi come piattaforma di dialogo e di confronto, a livello non operativo, tra le comunità di intelligence di 23 paesi che hanno sottoscritto la lettera di intenti, resa ancor più preziosa dalla partecipazione di esperti, accademici e decisori di vari paesi. Nonostante le strette relazioni tra le due organizzazioni, la doppia appartenenza e i legami funzionali (la NATO ha fornito il fondamento della difesa collettiva degli Stati membri dell'UE), la cooperazione di intelligence è stata probabilmente molto assente, negli anni passati, dalle relazioni euro-atlantiche. La limitazione delle capacità militari dell'UE e la minore portata delle attività (gestione della crisi, operazioni di pace, missioni umanitarie) ha creato un ampio divario tra l'UE e la NATO che invece, sotto la forte guida degli Stati Uniti ha avuto modo di sviluppare interi settori dell'intelligence.

È stato solo all'inizio degli anni 2000 che entrambe le organizzazioni hanno iniziato a intraprendere consultazioni regolari in gruppi di lavoro, comprese le questioni di sicurezza delle informazioni e lo scambio di classificate documenti. Un accordo di sicurezza provvisorio sull'accesso e lo scambio di informazioni classificate e relative il materiale è stato concluso nel maggio 2000. In seguito all'11 settembre 2001, i paesi dell'UE hanno iniziato a fornire alle autorità statunitensi preziosi informazioni e competenze antiterrorismo nel frattempo acquisite, compresi alcuni prodotti di intelligence. I piani dell'UE per il lancio delle prime missioni nell'ambito della politica di sicurezza e di difesa europea (PESD) sono state sostenute dagli Stati Uniti e ha portato al cosiddetto quadro completo UE-NATO "Berlin Plus" per la cooperazione militare permanente. Poiché la prima missione pianificata dell'UE nei Balcani implicava un'acquisizione da parte delle forze a guida NATO, nel marzo 2003 la NATO e l'UE hanno concluso un accordo sulla sicurezza dell'informazione, integrato da disposizioni su standard comuni per la protezione delle informazioni classificate. Questo accordo ha stabilito una comune veduta e applicazione di regole nei campi delle tutele legali, responsabilità nella gestione dello scambio delle informazioni riservate, definizione degli standard per l'ottenimento dei nulla osta di sicurezza, l'uso della crittografia nelle trasmissioni elettroniche e il controllo dello scambio di informazioni classificate nel sistema UE-NATO. Va comunque dato atto che l'UE ha cercato comunque di accelerare l'iter di innovazione, tendano di recuperare il gap con l'Alleanza Atlantica così come dimostrato da molti paesi UE che già a partire dal 1990 hanno iniziato un percorso di cooperazione comune, inizialmente limitatamente all'intelligence geospaziale ritenendola di importanza strategica. Come detto nel capitolo 2 della presente ricerca, in quella fase si decise di istituire una divisione di intelligence e un'unità di allerta precoce nelle strutture militari che poi sfociò nel Centro di Situazione SITCEN, responsabile del monitoraggio delle aree di crisi e quindi della sicurezza, incaricato di predisporre analisi e valutazioni situazionali soprattutto in aree interessate alle politiche o agli interventi della PESD. Nel 2007 ulteriori modifiche condussero alla creazione dell'INTCEN con l'obiettivo di disporre di ulteriori potenzialità e di un'intelligence sharing tra i partner europei. La struttura nascente era in grado di produrre analisi approfondite basate sull'open source ma contemporaneamente di vagliare analisi di intelligence militare degli stati membri

e dell'ambiente diplomatico. Nonostante il costante sviluppo delle capacità di intelligence della NATO e dell'UE, gli scambi di informazioni e di intelligence tra le due organizzazioni è stata caratterizzata da complessità di vario genere. In questo certamente ha pesato il diverso ruolo delle due alleanze e la diversa collocazione strategica che le vedono rispondere a interessi profondamente diversi se pure in alcuni caso complementari. In questo contesto, la dichiarazione congiunta NATO-UE adottata nel 2016 a Varsavia è da considerarsi un promettente passo verso un approccio collaborativo che può essere prodotto in tutti i settori di competenza: l'ambiente di sicurezza nel suo complesso, le più specifiche minacce del terrorismo, dell'estremismo, della guerra ibrida e delle operazioni informatiche offensive. Il nuovo assetto istituzionale nella NATO, così come le linee guida adottate a Varsavia nel 2016,¹⁰⁸ fino ad arrivare alla novità costituita dal nuovo Concetto Strategico espresso al vertice di Madrid del 2022,¹⁰⁹ hanno aperto nuove opportunità per una più ampia condivisione delle informazioni allo scopo di una migliore consapevolezza situazionale, valutazioni più accurate delle minacce e una maggiore resilienza anche per le minacce ibride/asimmetriche.

¹⁰⁸The 27th North Atlantic Treaty Organization (NATO) Summit was held in Warsaw, Poland on 8-9 July 2016. Termed as a "landmark"¹ summit, it was a crucial gathering of NATO member-states to decide the next course of security policy in Europe and beyond. Broadly, the stated objective of the Warsaw Summit was to take decision on enhancing 'the Alliance's security by strengthening its deterrence and defence, and projecting stability beyond its borders.'² A number of issues, ranging from the political and security situation in Eastern Europe, Middle East and North Africa to relations with Russia, Afghanistan and non-traditional security threats, including cyber security, and NATO-European Union (EU) cooperation were discussed for future course of policy orientation. Security situation in Eastern Europe and relationship with Russia figured high on the NATO agenda. Poland and Baltic states were expecting declaration of military measures to counter "assertiveness" of Russia in Eastern Europe. They often voice their concerns over Russian military build-up, exercises and its 'irredentism'.
https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=1782&lid=785

¹⁰⁹At the Madrid Summit, 29-30 June 2022 NATO Leaders took important and transformative decisions that set the Alliance's strategic direction for the near and long-term future. At the Madrid Summit, NATO adopted its new Strategic Concept. This key document reaffirms NATO's values, purpose and tasks. It provides a collective assessment of the security challenges facing the Alliance and outlines the political and military tasks NATO will carry out to address them.
https://www.nato.int/cps/en/natohq/news_196144.htm

3.3 Intelligence e grey zone

3.3.1 Sfida alle funzioni principali

La moderna era della competizione è dominata da attori che promuovono i propri interessi e perseguono i propri obiettivi con ogni mezzo. Negli ultimi anni questi sono stati perseguiti anche attraverso attività condotte nell'ambito della cosiddetta "grey zone", ovvero quella zona caratteristica, collocabile in linea teorica, tra la pace e la guerra.¹¹⁰ Alcuni studi hanno analizzato i modi specifici in cui gli attori internazionali di maggior peso operano ormai di consueto al di sotto della soglia della guerra convenzionale e mescolano strumenti politici, economici, informativi e militari per aumentare la loro legittimità globale e far avanzare i loro interessi.¹¹¹ D'altronde ci sono validissime ragioni strategiche per comprendere che il fatto di prediligere tali scelte è significativamente quello di riuscire comunque a raggiungere gli obiettivi prefissati, alcune volte limitati, altre volte di notevole importanza, senza incorrere nel rischio di escalation in una guerra costosa e potenzialmente devastante.¹¹² L'intelligence dunque si trova davanti a

¹¹⁰K. Hicks et al., *By Other Means Part I: Campaigning in the Gray Zone* (Washington, DC: CSIS, July 2019), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf; and Michael Mazarr, *Mastering the GrayZone: Understanding a Changing Era of Conflict* (Carlisle Barracks, PA:United States Army War College Press, December 2015), 39, <https://publications.armywarcollege.edu/pubs/2372.pdf#page=39>.

¹¹¹ Gray is used for things that are gloomy, cloudy, dark and grim. It is an ambiguous space. Not easy to visualize, it is cloaked making things beneath not always what they seem. Competitive actions between nations and actors are not always clear. They can be misread, misunderstood, and misleading. There is no denying that a missile hit a target, however, offensive rhetoric, cyber infiltration or a malicious messaging may be interpreted differently by those who send it and those who receive it. Thus, it is often problematic to interpret the meaning of a non-lethal act by friend and adversary alike. In pre and post war, or what is now being categorized as *The Gray Zone*, military intelligence teams struggle to define how to interpret such actions and categorize them as friendly, neutral or threat. The United States Special Operations Command (SOCOM) defines *gray zone* challenges as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. The U.S. Army War College combines this definition with "purposeful, high-stakes employment of aggressive statecraft-employing all available coercive instruments-in a deliberate campaign-like persistent pressure and intimidation that achieves war-like ends through ways and means short of open conflict. Grey zone competition is not war by a classical definition but via miscalculation and unintended escalation threatens to transition to open conflict. P. De Gennaro, *The Gray Zone and Intelligence Preparation of the Battle Space*, august 2016, <https://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space>

¹¹² Schelling, T. *The Strategy of Conflict* (Cambridge, MA. Harvard University Press, May 1981); Robert Jervis, "Deterrence Theory Revisited." *World Politics* 31, no. 2 (January 1979), doi:10.2307/2009945; and Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, November 2008).

una sfida epocale perché nel doversi adeguare a questa realtà, deve assolutamente inserirsi nello spettro delle citate attività per svolgere appieno alle sue funzioni fondamentali ovvero quelle di “rilevare” e “comprendere”. Questo perché il successo dell'intelligence nella grey zone richiede un feedback continuo e simultaneo tra gli sforzi per identificare le attività ostili (rilevare) e per contestualizzarle all'interno di un'analisi più ampia delle intenzioni e della strategia dell'attore proponente (comprendere). Riguardo alla funzione del “rilevare” occorre sottolineare lo stato delle cose, da un esame del quale è possibile comprendere le difficoltà che una moderna intelligence continuamente affronta. In tale contesto è un dato pacifico che le attività ostili della grey zone sono progettate per eludere il rilevamento o per vanificare gli sforzi dell'intelligence che, al contrario, servono per attribuirne la riconducibilità, stabilirne la quantificazione del rischio e produrre, su tali basi, le decisive risposte. Spesso, nel promuovere le azioni ostili, i vari attori prediligono associare tecniche secolari, come le campagne di influenza, con tecnologie moderne che consentono loro di svolgere le loro attività in segreto. Allo stesso modo, perseguono anche operazioni che sfruttano aspetti che agenzie di intelligence difficilmente possono rilevare appieno. Anche quando rilevate, le operazioni della grey zone creano intenzionalmente ambiguità e confusione per limitare la capacità degli apparati di intelligence di attribuire responsabilità, aggregare comportamenti e sviluppare una comprensione coerente della strategia di un aggressore. Spesso, dietro ad apparenti normali comportamenti/decisioni in ambito politico, economico, energetico e di difesa si registrano deboli indicatori di manovre ben più complesse e che preludono ad attività ostili in grado di svilupparsi anche a distanza di tempo. Tali indicatori, definiti in gergo “segnali deboli”, sfidano gli sforzi dell'intelligence che non può o non è in grado di analizzarne e valutarne appieno le potenzialità.¹¹³ Tra le motivazioni rientra certamente il sovradimensionamento dei dati a disposizione destinato ad aumentare, stante un incremento esponenziale degli stessi che, solo a titolo di esempio, nell'ultimo decennio sono cresciuti di trenta volte e, stando alle

¹¹³ Sheppard L., Conklin M., “Warning for the Gray Zone,” in Hicks et al., *By Other Means Part II*, <https://www.csis.org/analysis/warning-gray-zone>.

previsioni potrebbero raddoppiare entro il 2025.¹¹⁴ Vi è sostanzialmente un rapporto segnale-*rumor* (inteso come voce non confermata ma da analizzare) che non può essere assolutamente sottovalutato e che costituisce una vera e propria sfida del rilevamento; sfida resa ancor più impari stante la varietà di metodi sofisticati usati che prevedono tra l'altro anche l'immissione di *rumors* tendenti a confondere la percezione dei dati e, conseguentemente, ad amplificare la difficoltà di discernere gli elementi idonei a produrre una efficace analisi di intelligence.¹¹⁵ Esiste inoltre un'ulteriore area che ha provocato non poche discussioni e divergenze di opinioni nelle comunità di intelligence, costituita dai cd "segnali sconosciuti" ovvero quei segnali che per natura e caratteristiche sono difficilissimi da identificare poiché provenienti da ambiti nuovi o diversi da quelli in cui l'intelligence era in precedenza abituata a esaminare. Il riferimento è alle attività di telerilevamento o commercial remote sensing¹¹⁶ al monitoraggio dei social media, degli archivi pubblici e dell'area dell'informatica forense, tutte potenziali fonti di informazione a cui inevitabilmente se ne aggiungeranno altre atteso che la diversità dei dati sta procedendo parallelamente allo sviluppo delle tecnologie IoT e dell'Artificial Intelligence. Un aspetto insolito di tale evoluzione consiste nel fatto che le tecnologie emergenti, oltre a introdurre un volume di dati senza precedenti e nuove fonti dalle quali attingere, sfidano il ruolo dei servizi di intelligence come autorità principali nel rilevamento delle minacce. Nuovi assetti quali il cloud computing commerciale, i satelliti privati e tutta una serie di tecnologie sempre più accessibili stanno erodendo radicalmente i monopoli degli

¹¹⁴ "...The total amount of data created, captured, copied, and consumed globally is forecast to increase rapidly, reaching 64.2 zettabytes in 2020. Over the next five years up to 2025, global data creation is projected to grow to more than 180 zettabytes. In 2020, the amount of data created and replicated reached a new high. The growth was higher than previously expected caused by the increased demand due to the COVID-19 pandemic, as more people worked and learned from home and used home entertainment options more often". A. Holst, "Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025," Statista, June 2021, <https://www.statista.com/statistics/871513/worldwide-datacreated/>.

¹¹⁵ Jervis R., *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, February 2010).

¹¹⁶ Commercial remote sensing is remote sensing that produces information intended for sale on open commercial markets. It is generally performed by companies or through public-private partnerships rather than by governments. The commercial market includes remote sensing performed primarily from aerial and space borne platforms. Due to the strategic nature of remote sensing, commercial interests are nearly always intertwined with national interests, at least for space borne systems. Governmental policies authorizing and regulating commercial remote sensing generally reflect objectives for national security, technology development, international relations, and economic positioning. The history of the industry, and its current configuration, reflect this tension between economic and national interests.

stati-nazione sulla raccolta di informazioni nei domini spazio, aria, mare, terra e cyber. In tale ambito gli apparati di intelligence subiscono continue sfide a trovare nuove forme di collaborazione con le maggiori entità commerciali, detentrici di apparati di raccolta informazioni uniche e preziose. Analogamente, devono collaborare con quei settori e quelle entità commerciali che detengono tecnologie che sono o che possono essere sfruttate dagli avversari, allo scopo di avere un controllo su tali attività usandole come veicolo per l'attuazione di strategie per operazioni in zone grigie. Spesso i due ambiti descritti possono risultare coincidenti, è questo il caso dei social media, luogo virtuale dal quale attingere preziose informazioni e all'interno del quale è possibile operare con le più raffinate tecniche oggi esistenti nell'ambito dell'information disorder.¹¹⁷ È indispensabile pertanto recuperare il gap esistente circa la detenzione del monopolio dell'informazione, al fine di riappropriarsi del controllo anche sui social media, oltretutto degli spazi legali che consentono di operare in una sorta di ambiguità utile per le operazioni ostili che sfruttano questa e altre falle dei sistemi nazionali. Per le comunità di intelligence e per i decisori politici internazionali è indispensabile pertanto affrontare con incisività le implicazioni legali, politiche e sociali delle sfide concernenti i rapporti con le nuove tecnologie per giungere ad un superamento degli attuali limiti che, nel contesto della sicurezza nazionale possono costituire un limite.¹¹⁸ Resta infine da risolvere un problema pressante e spesso sottovalutato. Esiste infatti una criticità sotto il duplice profilo semantico e tassonomico. Occorre cioè dare chiarezza ai significati di "grey zone", "minacce ibride", "operazioni irregolari", "competizione strategica", "minacce asimmetriche" e condurle ad un significato unico e universalmente accettato, a fronte dell'attuale diversificazione terminologica che, in quanto tale, si presta a interpretazioni diverse, così come diverse potrebbero essere le risposte ritenute adeguate (ad esempio una minaccia generica avrà come conseguenza un certo tipo di risposta mentre se la stessa viene definita quale minaccia diretta e ostile avrà certamente conseguenze più pesanti). Sotto il profilo tassonomico il chiarimento è altrettanto importante allo scopo di

¹¹⁷ Information Disorder. Toward an interdisciplinary framework for research and policy making. Report to the Council of Europe, 2017, <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>

¹¹⁸ "Hearing to examine worldwide threats," Hearing before the U.S. Senate Select Committee on Intelligence, 117th Cong., 2nd sess., April 14, 2021, <https://www.intelligence.senate.gov/hearings/openhearing-worldwide-threats-1>.

dare con certezza, una classificazione e una tipizzazione, funzionale alla comprensione dell'accaduto e alla predisposizione delle attività di contrasto da attuare in risposta. La seconda funzione principale dell'intelligence, ovvero quella della comprensione, presenta anch'essa una sfida di notevole impatto. In particolare come si è già avuto modo di ricordare, le strategie usate per operare in "grey zone" sono progettate per vanificare gli sforzi, volti a comprendere chiaramente la vera natura e la consistenza delle minacce. Anche nel caso in cui vengono rilevate le minacce, le fasi successive relative all'attribuzione, all'individuazione dei responsabili e nel dare il giusto grado di pericolo rappresentato, è spesso accompagnata da diversi livelli di incertezza e tale stato è ancora più labile nella cd "fascia bassa" dello spettro della grey zone dove tali attività diventano addirittura impossibili. Nella cd "fascia alta" l'attribuzione, l'individuazione dei responsabili e il grado di pericolosità giungono con maggiore facilità ma vi sono spesso profili di incertezza e confusione che rendono il processo di difficile attuazione. Per entrare a fondo delle dinamiche legate all'aspetto della comprensione, occorre valutare l'insieme di attività di diversa tipologia e in ambienti multidominio. Quest'ultimo aspetto genera parecchia confusione dal momento che se da un lato è possibile parlare di dominio politico, economico, informativo, diplomatico, commerciale, dall'altro occorre comprendere che oggi, tali domini sono indissolubilmente legati tra di loro, o comunque interdipendenti, stante una pervasione di tecnologie che ne affievoliscono i parametri distintivi. In sintesi, l'esame di un dominio rimanda automaticamente a un altro o addirittura si presenta influenzato e interdependente da un altro apparentemente diverso. In tale ambito riuscire a comprendere la portata di una o più attività ostili, risulta evidentemente molto difficoltosa ed eventuali azioni ostili, nella loro prima fase, potrebbero non essere per nulla interpretati come propedeutici ad attività in grey zone, cosa che diventa chiara soltanto in un secondo momento. Una corretta comprensione dell'intelligence nella grey zone è necessaria principalmente per due scopi. Prioritariamente perché fa crescere la base di conoscenza che circonda la strategia e il processo decisionale di un avversario. Ciò può facilitare la produzione di forme di analisi più complesse, come identificare dove si trovano e dove verranno spostate le azioni di un avversario nello spettro della grey zone o determinare previsioni, rischi e opportunità a lungo termine. In secondo luogo,

una comprensione della più ampia strategia della grey zone può essere tradotta in narrazioni convincenti e coerenti che possono essere utilizzate per richiamare e contrastare pubblicamente la strategia della grey zone di un attore.¹¹⁹ Come ha osservato una recente nota firmata da nove comandanti combattenti, la campagna nella grey zone richiede fatti tempestivi e pubblicamente utilizzabili per tagliare l'ambiguità e la confusione intenzionalmente create dagli avversari.¹²⁰ Comprendere la grey zone richiede un rilevamento tempestivo e accurato, ma per poter "rilevare", i servizi di intelligence devono sapere cosa cercare e dove cercare. In questo modo, il rilevamento e la comprensione non sono solo ciclici, ma devono costantemente e simultaneamente confrontarsi tra loro. Devono anche rimanere equilibrati. Gli sforzi che enfatizzano eccessivamente l'osservazione degli indicatori, nel tempo, potrebbero portare a delle errate valutazioni. Il processo di rilevazione e comprensione di una minaccia pur se corretto in tutte le sue fasi, potrebbe essere vanificato se il suo ciclo si protrae per un lungo periodo o se la fase della comprensione giunge in ritardo, consentendo cioè all'attore di portare a compimento l'azione. I processi di pianificazione e decisione degli attori ostili sono spesso non riconoscibili; senza una comprensione sufficiente di ciò che un avversario vuole ottenere e di come intende raggiungerlo, gli sforzi di rilevamento possono sfociare in un esercizio di selezione che fa ben poco per anticipare un avviso credibile.¹²¹ È essenziale integrare perfettamente gli sforzi per rilevare e comprendere il comportamento

¹¹⁹ Knoll, D. "Story Telling and Strategy: How Narrative is Central to Gray Zone Warfare," Modern War Institute at West Point, August 24, 2021, <https://mwi.usma.edu/story-telling-and-strategy-how-narrative-is-central-to-gray-zone-warfare/>.

¹²⁰ "...four-star commanders "need more tools that empower them" as they wage a "war of information." "Our inability to speak publicly about the real threats coming from China and Russia means many Americans don't truly know everything we're up against," Inhofe said in a statement. "It makes it easier to argue to cut the defense budget when we can't have an honest discussion about these threats." "I know this frustrates many of my colleagues on both sides of the aisle — and we need to get better at fighting in this space," he added. "Our adversaries like to operate in the shadows, and the best way to combat them is to call out their lies." This battle of ideas is viewed as only widening. In a new threat assessment published this month, the DNI highlighted the aggressive campaigns by both Russia and China to shape global public opinion." <https://www.politico.com/news/2021/04/26/spychiefs-information-war-russia-china-484723>.

¹²¹ "...The comprehensive and synchronized use of strategic lines of action combined with the different levels of escalation offers advantages to an actor who resorts to the gray zone over a rival whose defensive strategy is based on classic, linear, and inflexible military deterrence rather than on the gradualism and ambiguity of gray zone conflict". Javier Jordan, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict," *Journal of Strategic Security* 14, no. 1 (November 2020), doi:10.5038/1944-0472.14.1.1836.

delle zone grigie e creare un circuito di feedback efficace tra queste linee di impegno.

3.3.2 Percorsi di ottimizzazione

Quanto esposto nei paragrafi precedenti è sufficiente a delineare un diverso approccio futuro per l'intelligence applicato alla grey zone e più specificamente alle attività di rilevamento e comprensione. Occorre procedere a miglioramenti a livello tattico che consentano all'intelligence di migliorare l'accesso a dati, strumenti e analisi frutto di miglioramenti strutturali e culturali più ampi e più rispondenti alle caratteristiche delle citate zone. Sebbene la tecnologia sia fondamentale per molte delle attività menzionate, quello che risulta indispensabile è che l'innovazione e l'approccio futuro dipenderà dalla creazione delle giuste condizioni culturali e organizzative che consentano alle persone delle strutture di intelligence di sfruttare la tecnologia mentre sviluppano un'analisi strategica ponderata. In tale senso, un passo importante verso un percorso di innovazione, potrebbe essere costituito dalla creazione di un catalogo dati provenienti dalla ricerca OSINT, a beneficio dell'intelligence. Strumenti di catalogazione destinati a organizzare e facilitare l'accesso e l'utilizzo di dati, sono essenziali per qualsiasi organizzazione e ancor più per quelle che si basano sull'analisi di una mole imponente di essi, con positive implicazioni derivanti dalla conoscenza degli stessi, utili a individuare anche i segnali più labili di nuove ed emergenti sfide. La funzione di una tale strutturazione va al di là della semplice catalogazione. L'aspetto più importante è quello di poter sfruttare set di dati OSINT di assoluto livello funzionale sia in ambito locale e sia in quello internazionale o comunque più globale. Le informazioni OSINT, come tutte le informazioni di intelligence, sono soggette a vari livelli di qualità, affidabilità e tempestività. Storicamente, l'analisi dei mezzi di comunicazione esteri - la loro proprietà, struttura, relazioni con i partiti politici e altre informazioni sull'obiettività e l'affidabilità - è stata cruciale per la disciplina OSINT. L'aspetto innovativo è rappresentato da varie sfaccettature, una fra tutte quella di un continuo aggiornamento e qualificazione delle fonti. Negli ambienti dell'intelligence infatti è nota l'importanza di una continua rivalutazione della struttura dei dati, della tempestività, dell'affidabilità e della sicurezza, che sono

soggette a modifiche nel tempo. Ad esempio, la disponibilità e l'utilità dei registri pubblici sulle imprese o sugli indicatori economici possono variare sostanzialmente da un paese all'altro e in periodi diversi. Ciò dipende da fattori quali i requisiti legali di un paese, le normative sulla trasparenza e la frequenza con cui tali dati vengono resi disponibili. Se un analista sta monitorando determinati indicatori economici in più paesi, è essenziale capire come tale comportamento potrebbe manifestarsi in modo diverso a seconda dei dati disponibili, dove viene generato, come viene acquisito e chi vi ha accesso. In sintesi, per essere sicuri e utili, i dati open source devono essere accuratamente e continuamente contestualizzati. Questa contestualizzazione dei dati può emergere da più fonti, incluso il personale interno al paese che ha familiarità con il governo e la cultura ospitanti, nonché gli analisti delle sedi centrali responsabili della conduzione dell'analisi a livello strategico. Su altro versante, è opportuno procedere a implementare le capacità di analisi dei dati provenienti dalle applicazioni low-code e no-code. Preso atto della necessità di monitorare volumi e tipologie di dati sempre più crescenti e finalizzati alla rilevazione di segnali deboli di attività ostili è inevitabile che questo richiederà analisi molto più avanzate rispetto a quelle attuali e soprattutto sviluppate nell'ambito Artificial Intelligence/Machine Learning, già da tempo usate e seriamente prese in considerazione nel mondo dell'intelligence,¹²² tanto da costituire uno degli elementi più significativi dei processi innovativi attraverso i quali si stanno sviluppando strumenti analitici low-code e no-code che consentono di creare soluzioni a problematiche emergenti e per specifici ambiti di mission.¹²³ In tal modo è possibile predisporre lo sviluppo di vari modelli di rilevamento delle modifiche che si basano sulla diversità dei dati geospaziali o di telerilevamento, monitorando in tal modo i cambiamenti in ogni singola area geografica oppure la creazione di uno o più modelli di comportamento su scala globale.¹²⁴ Lo sviluppo funzionale di tali modelli è interessante specie nella parte in cui i sistemi vengono predisposti per avvisare gli

¹²²“Artificial Intelligence Ethics Framework for the Intelligence Community,” Office of the Director of National Intelligence, June 2020, <https://www.intelligence.gov/artificial-intelligence-ethicsframework-for-the-intelligence-community/>;

¹²³ Katz, B. “The Analytica Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis,” CSIS, *CSIS Briefs*, October 2020, <https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologiestransform-intelligence-analysis/>;

¹²⁴National Security Commission on Artificial Intelligence, *Final Report* (Washington, DC: March 2021), <https://www.nsc.gov/2021-final-report/>.

utenti di potenziali cambiamenti, introducendo gli elementi ritenuti utili a dare maggiore flessibilità nel determinare le soglie e la tolleranza allo specifico modello di riferimento. Notevoli vantaggi possono essere ricavati da una maggiore autonomia degli strumenti legati all' AI/ML stante la loro potenzialità di fornire aggiornamenti e avvisare gli utenti di potenziali cambiamenti in un modello; attività questa, che può consentire agli esperti una maggiore flessibilità nella determinazione delle soglie e delle tolleranze al rischio funzionali alla loro specifica missione. Ad esempio, un modello può focalizzare il proprio punto-soglia quando rileva un numero specificato di navi entrare in un'area circoscritta e per un periodo stabilito. Un altro modello può essere distribuito in un'area specifica di interesse ed essere così predisposto per fungere da monitoraggio ed acquisizione di informazioni open source, attivandosi sia nei confronti dei mezzi di trasmissione, ma anche verso i social media o i registri pubblici. In alcuni casi, qualora la tolleranza al rischio sia vicina allo zero e gli avvisi di soglia bassa risultino essere abilitati, tutti i risultati reattivi verranno esaminati attentamente con evidenti maggiori possibilità di interpretare anche un segnale minimo di attività ostile. In altri casi, le tolleranze al rischio potrebbero essere rilevate con un margine maggiore e gli avvisi generati solo quando un modello ha sviluppato un livello di acquisizione e controllo dati basato su soglie di tipo diverso. In entrambi i casi diventa preziosa e determinante la capacità di adeguare le soglie in tempo reale grazie allo sviluppo delle tecnologie che, in prospettiva, consentiranno di impiegare un numero sempre minore di personale specializzato (ingegneri elettronici, data scientist, informatici etc) a vantaggio del personale che opera nel settore intelligence che può così perseguire gli obiettivi individuati. Un sicuro prossimo obiettivo dell'intelligence applicata alle grey zone sarà lo sviluppo delle capacità analitiche di sistemi in grado di condurre forme sempre più complesse di analisi di modelli e comportamenti. Seppure i tradizionali modelli AI/ML di rilevamento delle modifiche siano già in grado di indirizzare gli analisti ai cambiamenti in base agli indicatori noti, l'introduzione di modelli comportamentali più complessi possono aiutare a scoprire nuovi modelli di attività della grey zone. Si tratterebbe di un percorso di ottimizzazione prodotto grazie anche alle tecniche di deep learning integrate dalla supervisione umana che consentirebbero di esaminare i dati disponibili a livello globale per modelli di

comportamento potenzialmente simili. Questi approcci sono già comuni nei settori della sicurezza informatica e dell'intelligence finanziaria. Ad esempio, gli algoritmi per rilevare le frodi finanziarie sono addestrati per monitorare continuamente le transazioni finanziarie sospette in tutto il mondo e adattarsi ai cambiamenti noti o sospetti nelle firme e nelle tecniche di coloro che si occupano di finanza illecita.¹²⁵ Allo stesso modo, gli sforzi di sicurezza informatica per sviluppare e addestrare modelli per rilevare gli zero-day exploit sconosciuti o non definiti, potrebbero essere ampliati nel più ampio dominio della concorrenza per la sicurezza interstatale. Ulteriori miglioramenti sono auspicabili nei settori del “forecasting” e del “warning”. Da un recente studio sull’argomento svolto dall’Università della Pennsylvania, si rileva che l’intelligence USA per oltre 20 anni ha valutato varie piattaforme di previsione geopolitica.¹²⁶ Ma questo evidentemente non basta in un processo innovativo che dovrà portare l’intelligence a esplorare degli approcci innovativi nei settori della previsione e dell’allertamento, allo scopo di renderli più funzionali alle esigenze attuali.¹²⁷ E’ fondamentale quindi disporre di esperti provenienti anche da ambienti esterni alle comunità di intelligence che portino i loro contributi di conoscenze, professionalità e capacità di sintesi anche legate all’esame di dati open source, il tutto a beneficio della sicurezza. Una delle sfide concettuali più significative nella grey zone è quella di superare la mancanza di una tassonomia standardizzata di categorie e tipi di comportamenti specifici. Da questo problema si estendono numerose difficoltà di raccolta, analisi e avviso, poiché approcci incoerenti per acquisire e classificare le attività delle zone grigie minano gli sforzi per identificare, aggregare e misurare tali attività rispetto a una metodologia oggettiva e coerente. Per rafforzare la capacità di rilevare e comprendere le attività delle zone grigie, occorre lavorare anche in questo settore e sforzarsi di esplorare le opzioni per classificare i tipi di comportamento delle zone grigie. Tale sforzo potrebbe essere in linea con i

¹²⁵ Stojanović B. et al., “Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications,” *Sensors* 21, no. 5 (February 2021), doi:10.3390/s21051594.

¹²⁶ Horowitz M. et al., *Keeping Score: A New Approach to Geopolitical Forecasting* (Philadelphia: Perry World House, University of Pennsylvania, February 2021), <https://global.upenn.edu/sites/default/files/perry-world-house/Keeping%20Score%20Forecasting%20White%20Paper.pdf>.

¹²⁷ McHenry, J. “Three IARPA forecasting efforts: ICPM, HFC, and the Geopolitical Forecasting Challenge,” (presentation, Federal Foresight Community of Interest 18th Quarterly Meeting, January 26, 2018), https://www.ffcoi.org/wp-content/uploads/2019/03/Three-IARPA-Forecasting-Efforts-ICPM-HFC-and-the-Geopolitical-Forecasting-Challenge_Jan-2018.pdf.

processi esistenti che regolano la creazione di priorità di raccolta e analisi.¹²⁸ Una standardizzazione del genere, è funzionale a molteplici scopi, incluso quello di individuare cosa raccogliere nella grey zone e come caratterizzare e misurare il livello di minaccia di un'attività. Le agenzie di intelligence dovrebbero quindi basarsi su questo quadro e valutare nuove tecniche per fornire informazioni, giudizi e avvisi di intelligence efficaci in grado di ridurre al minimo i rischi di fallimento dell'intelligence. Per sviluppare una strategia coerente, una coerenza analitica e un gergo comune tra intelligence e stakeholder politici, tutti gli attori interessati dovrebbero collaborare con alleati internazionali per promuovere un lessico comune delle attività delle zone grigie nei vari domini in cui possono emergere. La capacità di applicare una terminologia comune tra attori, regioni e attività aiuterebbe gli sforzi tecnici per sviluppare modelli in grado di rilevare modelli di comportamento nuovi o imprevedibili a livello globale. Infine, la grey zone è un sistema complesso di sistemi, in cui gli avversari opportunisti sfruttano le vulnerabilità quando si presentano, imparano dal comportamento dell'altro e adattano costantemente le tecniche in risposta al rilevamento. Pertanto, gli sforzi per definire, classificare o modellare il comportamento delle zone grigie devono bilanciare la necessità di creare una struttura rispetto a un campo di attività in continua evoluzione.

3.3.3 La trasformazione digitale

Qualsiasi processo di ottimizzazione venga determinato in qualsiasi contesto operativo, non può prescindere dalla previsione su sviluppo delle tecnologie e problematiche emergenti negli anni a venire. Gli sforzi progettuali, devono essere fatti tenendo conto di cosa ci aspetta in previsione futura; in quel futuro in cui le battaglie potrebbero svolgersi utilizzando armi e tattiche che molte delle attuali potenze sono mal preparate a rilevare o contrastare. I missili balistici di oggi impiegano decine di minuti per attraversare un oceano, ma le armi ipersoniche di domani (già in sperimentazione) potrebbero richiedere solo pochi minuti. La

¹²⁸Un approccio in tal senso è stato fatto nell'ambito del National Intelligence Priorities Framework, "ICD 204 - National Intelligence Priorities Framework," Office of the Director of National Intelligence, January 7, 2021, https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

guerra urbana potrebbe svolgersi in città iperconnesse dove molteplici sensori, provenienti da molteplici fonti, fornirebbero una mole di dati troppo grande per essere estratta ed esaminata dagli analisti. Nel dominio cibernetico, nel momento in cui un operatore rileva un "lancio", un pacchetto di armi potrebbe aver già raggiunto l'obiettivo e ottenuto l'effetto desiderato. Attacchi contro satelliti, attacchi economici e campagne di influenza segrete possono essere tutti impercettibili ai sensi umani o comunque se rilevati potrebbe essere già troppo tardi. Il vettore, il volume, la velocità, la varietà, e l'ubiquità dei dati stanno sconvolgendo gli strumenti e i metodi tradizionali della politica, delle operazioni e dell'intelligence e della sicurezza nazionale nel suo complesso. La società in cui viviamo è consapevole che "l'informazione è potere", e per questo ha creato tecnologie in grado di creare volumi di dati strutturati e non strutturati così grandi da sopraffare tutte le precedenti forme di approccio analitico. Emblematiche in tal senso appaiono alcune delle raccomandazioni assunte dal Defense Innovation Board degli Stati Uniti, nel corso di un incontro del 2017¹²⁹, secondo cui *“chiunque accumuli e organizzi la maggior parte dei dati, su noi stessi e sui nostri avversari, sosterrà la superiorità tecnologica”*. Il mancato trattamento dei dati come una risorsa strategica cederà tempo e spazio prezioso a concorrenti o avversari. Tuttavia, i dati attualmente sono generati in troppi formati diversi tra loro, in troppi sistemi disconnessi o difficilmente accessibili, senza strutture standardizzate e senza un'ontologia globale concordata. Questa situazione rischia di sprecare raccolte, provoca mancanza di tempestività, mancate indicazioni e avvertenze e incide negativamente nel processo decisionale. Il risultato è l'impossibilità di fondere i dati per creare intelligence e di farlo nel più breve tempo possibile. Il compito degli analisti è connotato da sempre maggiori difficoltà, troppo ingombrante e con troppi ostacoli da superare per fornire giudizi analitici tempestivi e pertinenti o informazioni utili a decisori politici e combattenti. In un contesto più ampio è auspicabile che l'intelligence proceda celermente ad affrontare le nuove sfide legate alla trasformazione digitale e all'aumento esponenziale dei dati, attraverso le seguenti direttrici:

¹²⁹ As part of their recommendations from the January 2017 public meeting, the U.S. Defense Innovation Board asserted that whoever amasses *and organizes* the most data—about ourselves as well as our adversaries—will sustain technological superiority. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1566262/intelligence-in-a-data-driven-age/>

- abbracciando algoritmi di apprendimento automatico in grado di analizzare i dati, estrapolare i contenuti in essi più importanti e quindi rispondere più celermente alle richieste;
- incoraggiare la creatività e il pensiero profondo da parte dei professionisti dell'intelligence;
- progettare la politica, la tecnologia dell'informazione e costruire un adeguato sistema di sicurezza.

Stante la loro complessità, questi ambiti meritano di essere affrontati in contesti molto ampi perché probabilmente hanno bisogno di un maggiore coinvolgimento che va al di là della singola agenzia o del singolo programma portato avanti da un solo paese. Si assiste a un bisogno impellente di costruire approcci creativi per adattarsi a questo nuovo ambiente che deve includere il miglioramento dei vantaggi tecnologici e operativi con sistemi e macchine in grado di manipolare e comprendere i big data, oltre a far progredire la collaborazione uomo-macchina e macchina-macchina, così gli analisti possono sfruttare al meglio il loro tempo lavorando sui problemi più complessi. Restano molte perplessità su alcuni aspetti tutt'altro che secondari e che riguardano principalmente il connubio Artificial Intelligence e Machine Learning. Algoritmi e apprendimento automatico sono indubbiamente utili ma è lecito porsi qualche dubbio circa le ripercussioni impreviste di macchine e sistemi in grado di generare soluzioni attraverso modalità che potrebbero non essere facilmente spiegabili a operatori umani; peraltro tali sistemi hanno creato i propri linguaggi che gli stessi programmatori potrebbero a breve avere difficoltà a riconoscere¹³⁰ e hanno imparato a giocare secondo schemi, modalità e tattiche che gli operatori umani potrebbero non comprendere o addirittura non governare.¹³¹ Si tratta di ripercussioni sconosciute, non testate, in gran parte non esplorate e in parte non previste ma che potrebbero avere effetti devastanti sullo stesso sistema di sicurezza nazionale se non governate. Il futuro spazio di battaglia è costituito non solo da navi, carri armati, missili e satelliti, ma anche da algoritmi, reti e griglie di sensori. Come nessun altro

¹³⁰ Wilson, M. "L'IA sta inventando linguaggi che gli esseri umani non possono capire. Dovremmo fermarlo?" *Co.Design*, 14 luglio 2017, disponibile all'indirizzo < www.fastcodesign.com/90132632/ai-is-inventing-its-own-perfect-languages-should-we-let-it >.

¹³¹ Greenemeier, L. "AI versus AI: Self-Taught AlphaGo Zero Vanquishes Its Predecessor", *Scientific American*, 18 ottobre 2017, disponibile su < www.scientificamerican.com/article/ai-versus-ai-self-taught-alpha-go-zero-vince-il-suo-predecessore/ >.

momento nella storia, le guerre future saranno combattute su infrastrutture civili e militari di sistemi satellitari, reti elettriche, reti di comunicazione e sistemi di trasporto e all'interno delle reti umane. Entrambi questi campi di battaglia, elettronici e umani, sono suscettibili alla manipolazione da parte di algoritmi avversari. Negli ambienti elettronici, gli algoritmi sono già utilizzati per monitorare e mantenere il controllo sulla maggior parte delle aree delle infrastrutture critiche (elettrica, idrica, alimentare, finanziaria, delle comunicazioni e così via) e le agenzie di intelligence hanno bisogno della capacità di fondere i dati su più fonti per comprendere le attività dell'avversario e i risultati previsti. Tra le tecnologie emergenti poi non va sottovalutato l'impatto della cosiddetta "rivoluzione quantistica" all'interno della quale si muovono concetti di particolare interesse che afferiscono a molteplici ambiti di studio. Ci troviamo di fronte a discipline che si fondano su principi complessi. Le leggi quantistiche, ad esempio non sono "deterministiche" ma "probabilistiche", nel senso che sono in grado di prevedere le probabilità con cui gli eventi di diverso tipo potranno verificarsi. Tale approccio ha così determinato una migliore comprensione di alcune proprietà chiave delle particelle quantistiche che sono alla base delle tecnologie quantistiche. Pur non addentrandoci a fenomeni quali l'entanglement¹³² è doveroso sottolineare che l'arrivo di computer quantistici, dei dispositivi di posizionamento e temporizzazione (PNT) quantistici, l'introduzione della navigazione inerziale quantistica e l'imaging quantistico, costituiranno delle nuove opportunità per i comparti della Difesa e dell'intelligence. Tutti gli attori internazionali sono consapevoli di tali innovazioni, ma ovviamente pochi hanno le opportunità per grossi investimenti che dovranno supportare la creazione di futuristici sistemi avanzati. Per quanto riguarda l'intelligenza artificiale, la Cina ha una strategia nazionale per con impegni commisurati a investire miliardi di dollari in tecnologie di intelligenza artificiale nei prossimi 5 anni.¹³³ I ricercatori cinesi pubblicano

¹³² L'entanglement quantistico, un complesso e misterioso fenomeno della meccanica quantistica, definito da Einstein come "spaventosa azione a distanza", è stato oggi fotografato per la prima volta da un team di fisici dell'università di Glasgow, nel Regno Unito. Il gruppo ha mostrato la prima immagine della strana interazione fra le particelle che è alla base del fenomeno e del funzionamento dei computer quantistici. Viola R.: Ecco la prima immagine dell'entanglement quantistico, wired review, <https://www.wired.it/scienza/lab/2019/07/15/prima-immagine-entanglement-quantistico/>

¹³³ Webster G. et al. , "Il piano della Cina per 'guidare' nell'intelligenza artificiale: scopo, prospettive e problemi", *New America* , 1 agosto 2017, disponibile all'indirizzo

frequentemente più articoli e saggi sull'IA rispetto alle loro controparti statunitensi,¹³⁴ e gli strateghi dell'Esercito popolare di liberazione si stanno preparando per un mondo in cui gli esseri umani non possono tenere il passo con il processo decisionale sul campo di battaglia.¹³⁵ Sul versante della citata tecnologia quantistica, gli Stati Uniti fino al 2021 avevano stanziato circa 1.2 miliardi di dollari con incrementi del 30% previsti fino al 2026. La Cina ha reso il Quantum Computing una priorità strategica nazionale, investendo l'equivalente di circa 10 miliardi di dollari per la realizzazione di diversi laboratori dedicati all'informatica quantistica.¹³⁶ Il futuro mondo dell'intelligence dipenderà dall'accesso ai dati, modellando la giusta architettura ad essi, sviluppando capacità basate sull'intelligenza artificiale per accelerare notevolmente la loro contestuale comprensione attraverso il binomio uomo-macchina e macchina-macchina e una crescente esperienza analitica in grado di orientarsi nella realtà naturale e in quella virtuale. Dovrà inoltre sviluppare tecniche e metodologie per l'accesso, l'organizzazione e l'analisi, comprese le tecniche analitiche strutturate e gli standard delle tecniche analitiche per l'intelligenza artificiale. La nuova tecnologia si sta evolvendo più velocemente della capacità delle varie comunità di intelligence di implementarla, darle una connotazione funzionale e usarla in modo efficace. Una volta raggiunta una siffatta capacità analitica, viene spontaneo chiedersi come impiegarla al meglio. Il comparto militare dell'intelligence sta sviluppando e acquisendo sistemi di combattimento con un maggiore accumulo di dati e di intelligence analitica rispetto al passato, e i dati delle missioni delle intelligence devono essere trasferiti a questi sistemi il prima possibile affinché siano funzionali al ciclo di acquisizione e quindi aggiornati frequentemente e abbastanza velocemente per essere utilizzati in combattimento, in strutture capaci di contenerli e a livelli di classificazione che i sistemi di combattimento

< www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-scopo-prospettive-e-problemi/ >.

¹³⁴ "China May Match or Beat America in AI", *The Economist*, 15 luglio 2017, disponibile all'indirizzo < www.economist.com/news/business/21725018-its-deep-pool-data-may-let-it-lead-intelligenza-artificiale-china-may-match-or-beat-america >.

¹³⁵ Kania, E. B. "Artificial Intelligence and Chinese Power," *Foreign Affairs*, 5 dicembre 2017, disponibile all'indirizzo < www.foreignaffairs.com/articles/china/2017-12-05/artificial-intelligence-and-chinese-power >.

¹³⁶ Quantum Computing, USA e Cina si contendono la leadership. In ballo un business da 1,77 miliardi di dollari. <https://www.corrierecomunicazioni.it/digital-economy/quantum-computing-usa-e-cina-si-contendono-la-leadership-in-ballo-un-business-da-177-miliardi-di-dollari/>

possono gestire. Parallelamente, all'interno della comunità politica, i responsabili politici fanno sempre più affidamento su informazioni pubblicamente disponibili e non classificate quando l'intelligence classificata è troppo lenta per arrivare o troppo altamente classificata per essere utile.¹³⁷ Spesso nell'ambito delle strategie militari, ricorrono i presupposti della teoria pionieristica espressa negli anni 50 dal colonnello USAF John Boyd, denominata OODA (observe, orient, decide, act)¹³⁸. In questo lavoro, lo stratega Boyd aveva sottolineato l'importanza di operare a un tempo o un ritmo che un avversario non può comprendere o eguagliare. Operare all'interno del ciclo OODA di un avversario aiuta a raggiungere i propri obiettivi disorientando o deformando le immagini mentali di un avversario in modo che non possa né apprezzare né far fronte a ciò che sta accadendo intorno a lui. Tali presupposti possono essere messi in relazione alle nuove esigenze e in parte alle nuove tendenze, in base alle quali, nell'odierna era frenetica e in continua evoluzione basata sui dati, i termini *dominanza* dell'informazione o *superiorità dell'informazione* sono chimerici; invece, termini come *vantaggio temporale* potrebbe essere il miglior risultato possibile avendo certamente un impatto diverso. Eppure anche questo potrebbe essere sufficiente per prendere il sopravvento, se i combattenti possono rimanere all'interno del circuito OODA dell'avversario mentre allo stesso tempo utilizzano i dati in modi fantasiosi per distorcere l'orientamento dell'avversario. L'intelligenza artificiale e l'apprendimento automatico offrono l'opportunità di accelerare in ogni fase del

¹³⁷ Grossman, D. "Keeping Up with the Policymakers: The Unclassified Tearline," *War on the Rocks*, 28 luglio 2016, disponibile su < <https://warontherocks.com/2016/07/keeping-up-with-the-policymakers-la-linea-di-lacrima-non-classificata/> >.

¹³⁸ The OODA Loop strategy is a concept of situational awareness first developed in the mid-1950s, by USAF Colonel John Boyd. While the origins of the OODA Loop lie in strategic military operations, the concept has been applied with great success in the realms of business, litigation, intelligence and information gathering, law-enforcement and even advanced medical treatment. For the modern risk manager, this concept will seem extremely familiar. The OODA Loop is simply a recurring cycle of reassessment and reaction to unfolding events. Where the OODA Loop process differs from other similar decision making processes is that we are now viewing the snowpack as an opponent, or in the military sense, an enemy, which we must defeat to protect personnel and facilities. Utilization of the OODA Loop is intended to help direct a team or individuals resources in order to "defeat" the "enemy" and "survive". In the world of the avalanche forecaster, "victory" is avoiding injury to personnel or damage to facilities and infrastructure. The "Loop" is actually a series of loops that are constantly circulating and interacting throughout "combat operations" and assists in the allocation of energies and resources dependent upon the current phase of the "battle". By applying the OODA Loop to risk management programs, there is potential to observe and correct potential deficiencies in the program or, conversely to enhance processes that are efficient and effective. The OODA loop may be equally useful for the individual or operational team settings.

ciclo OODA dando un senso ai dati in tempo reale man mano che i dati arrivano, valutando le opzioni e avviando un'azione in millisecondi e agendo. Tali decisioni possono includere la risposta a indicazioni e avvisi prima che gli operatori umani abbiano il tempo di leggere un avviso o avviare una risposta entro un insieme predeterminato di parametri approvati. L'apprendimento automatico offre nuove opportunità per ridurre le prime due fasi del ciclo OODA, aumentando notevolmente il potenziale per gli esseri umani di accelerare il processo decisionale e l'azione. Le agenzie di intelligence possono e devono investire in capacità di apprendimento automatico tra domini, programmi e discipline diverse e richiedono ai funzionari dell'intelligence di utilizzare queste capacità al massimo delle loro potenzialità. Tutti i dati che rimangono intrappolati in compartimenti, database proprietari e su domini classificati che gli algoritmi non possono raggiungere richiederanno l'integrazione manuale da parte degli agenti dell'intelligence, ritarderanno le valutazioni dell'intelligence e creeranno bolle di dati protette in cui gli agenti potrebbero non essere in grado di vedere all'interno per portare tutte le fonti occuparsi di problemi analitici. Questa visione minaccia i concetti di "bisogno di sapere" e costringerebbe la raccolta e le comunità analitiche - con i loro fratelli negli uffici di controspionaggio e sicurezza - a conciliare le minacce dall'esterno con le minacce dall'interno. Per creare questo stato terminale, dovrebbero essere considerate diverse attività. In primo luogo, trovare la risposta a qualsiasi domanda di intelligence dovrebbe iniziare con la proposizione che ogni analista ha bisogno di tutti i dati potenzialmente rilevanti, da ogni possibile fonte.¹³⁹ Ciò suggerisce di trovare un diverso equilibrio tra l'approccio analitico deduttivo (ricerca delle incognite conosciute) e induttivo (sintetizzare per scoprire le incognite sconosciute). Richiede anche un approccio diverso alla raccolta perché tutti i dati possono essere rilevanti molto tempo dopo la raccolta e dovrebbero essere accessibili in archivi rilevabili; i processi per fare ciò dipenderanno fortemente dal fatto che i set di dati includano informazioni su persone statunitensi e altre entità protette, mentre i controlli dei dati e la garanzia della qualità dei dati diventano funzioni essenziali. L'integrazione diffusa di AI e ML presenterà nuove opportunità di inganno derivanti da dati che sono stati

¹³⁹ *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004), disponibile su < www.9-11commission.gov/ >.

alterati o manipolati. La counter-AI¹⁴⁰ diventerà prevalente mentre le operazioni di influenza assumeranno nuove dimensioni che devono ancora essere esplorate, richiedendo una rinnovata enfasi sulle operazioni cognitivo-centriche sia offensive che difensive. Gli analisti dell'intelligence devono essere formati su come riconoscere i tentativi di un avversario di utilizzare dati alterati o manipolati, inclusa la comprensione di come utilizzare l'IA al massimo vantaggio per impedire che anche le operazioni di influenza più sofisticate influiscano sui risultati operativi desiderati. Concettualmente occorrerà ripensare ai dati non soltanto come prodotto di un sistema informatico; andranno visti nell'ottica di una nuova architettura, che tenga conto della risoluzione di problematiche anche operative con il concorso dell'AI, secondo un'architettura infrastrutturale agile e attraverso soluzioni innovative, in modo tale che qualsiasi dato, proveniente da qualsiasi fonte possa essere inglobato in tali nuovi sistemi e sfruttato da qualsiasi analista che potrà così usufruire di maggiore ottimizzazione in processi che vedano non soltanto l'inserimento di dati negli algoritmi ma anche in senso opposto. L'accesso ai dati e la loro elaborazione, dovrà avvenire con maggiore semplicità e dovrà concretizzarsi attraverso una migliore padronanza dei processi che regolano le dinamiche del machine-learning tra uomo e macchina, prevedendo anche l'inserimento di figure quali data architect e data scientist. Questo perché l'accesso alla rete in tutti i domini legati alla sicurezza, l'accesso a tutti i dati rilevanti e l'agile integrazione delle tecnologie emergenti, sono fondamentali per ottenere e mantenere un vantaggio decisionale. L'open source dovrà essere maggiormente presa in considerazione, in modo tale da riuscire a fornire il primo livello di base della conoscenza di intelligence. Concettualmente questo passaggio avrà bisogno di tempo per essere assimilato dal momento che, nella galassia dell'intelligence considerata di più alto livello in cui sono contemplati dati e fonti classificate, dovranno trovare spazio fonti e dati open source quindi non classificati e di dominio pubblico, seppure altrettanto importanti se abilmente sfruttati. Si

¹⁴⁰ A counter-AI strategy would seek to harden the United States as a target for AI-enabled attacks, reduce the advantages of AI to an adversary, and predict and adapt to changes in behavior that are consequences of reliance on AI. Among other measures, the United States could take more aggressive steps to protect US data that could be used for training AI models, invest in counter-AI tactics, and change how it comprehends AI behavior. M.A. Thomas, "Time for a Counter AI Strategy" in Strategic Studies Quarterly – Policy Forum, spring 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Thomas.pdf

tratta certamente di un passaggio epocale poiché per la prima volta la classificazione (sia della fonte e sia della notizia) non diventerebbe un requisito di valorizzazione.¹⁴¹ Altro aspetto che in prospettiva potrebbe essere meritevole di miglioramento è quello legato ad una ipotesi di spostamento della forza lavoro legata all'analisi (intesa come settore lavorativo congiunto), da una visione tipica dell'era industriale (ovvero elaborazione della linea di produzione e sfruttamento dei singoli flussi di raccolta dati), a un modello più innovativo, di tipo aziendale, orientato al futuro (in cui analisti di diversa estrazione e con diverse professionalità, siano in grado di condurre analisi correlate, esplorare focus di interesse multisettoriali, e interagire nella galassia delle fonti, integrandosi anche con partner internazionali. Le implementazioni e i processi di ottimizzazioni richiederanno una revisione dei consueti canoni relativi ai cicli di formazione e addestramento del personale dedicato ai settori dell'intelligence interessati. Analogamente si dovrà ripensare ai budget per acquisizione, ricerca e sviluppo. L'introduzione di metodologie più flessibili di impiego e interazione tra diverse professionalità può essere avviata ma avrà bisogno di tempo per completarsi.

3.4 La dimensione dello Spazio e quella dei fondali marini

3.4.1. Spazio e supremazia

Parlare dello spazio quale ulteriore dimensione di difesa, sicurezza e conflitti può apparire un azzardo se si considera la galassia immaginaria che ruota intorno ad esso, seppure la realtà spesso risulta essere davvero complessa e si presti a interpretazioni fantasiose. Nel dicembre del 2019 gli Stati Uniti hanno preso la decisione di creare una Space Force¹⁴²; nello stesso anno la Francia ha creato il suo CDE ovvero il Commandement de l'Espace¹⁴³ che ha seguito la creazione di un

¹⁴¹ Girven R., Beaghley S. e Weinbaum C., "A New Paradigm for Secrecy", *US News & World Report*, 13 ottobre 2015, disponibile all'indirizzo < www.usnews.com/opinion/blogs/world-report/2015/10/13/definire-un-nuovo-paradigma-per-il-segreto-di-governo >.

¹⁴² "...The United States Space Forces is a separate and distinct branch of the armed services, organized under the Department of the Air Force in a manner very similar to how the Marine Corps is organized under the Department of the Navy". Official site, <https://www.spaceforce.mil/About-Us/About-Space-Force/>

¹⁴³ "...Le Commandement De l'Espace (CDE) a été créé par arrêté le 3 septembre 2019. Il succède au Commandement interarmées de l'espace (CIE). Il rassemble désormais, au sein d'un unique grand commandement de l'armée de l'Air, la majorité des acteurs experts du domaine spatial

Comando Spaziale avvenuto nel 2019, mentre la Germania nel 2020 ha deciso di creare il WeltraumKommando der Bundeswehr¹⁴⁴. Un mese dopo la NATO ha deciso di creare il suo primo Space Center in Germania, mentre un CCDCOE è sorto in Francia. Dietro tutto questo ovviamente c'è un interesse strategico verso una dimensione indispensabile per la correlazione di nuove tecnologie quali 5G e 6G per testare nuovi lanciatori e per contrastare l'ascesa di nuove potenze che guardano allo spazio, quali la Cina, l'India e gli Emirati Arabi Uniti, per un potere politico ma anche economico, potenzialmente in grado di variare gli equilibri futuri. È sostanzialmente una dimensione nella quale l'Unione Europea deve inserirsi per poter disporre di tecnologia e spazi senza i quali rischierebbe di soccombere a spese di altri paesi. Una iniziale enfasi, l'Unione l'aveva già posta con riferimento alla dimensione economica dello spazio, come indicato nella Space Strategy del 2016 supportata dal fatto che in un computo operato in quel periodo, l'economia spaziale europea era stata valutata tra 53-62 miliardi di euro¹⁴⁵. Lo spazio è, quindi, una parte fondamentale per il particolare settore economico, ma lo è sempre più anche per i comparti sicurezza e difesa, come dimostrato dall'interoperabilità dei programmi spaziali dell'Unione: Copernicus, Galileo e EGNOS. Copernicus mira a fornire informazioni precise ed attendibili di osservazione della Terra nei settori dell'ambiente, dell'agricoltura, del clima, della sicurezza, della sorveglianza marittima e di altri settori d'intervento dell'UE. Costituisce il più vasto programma mondiale di questo tipo ed il contributo dell'UE al Sistema di sistemi per l'osservazione globale della Terra (GEOSS). È diventato operativo con il lancio del suo primo satellite nel 2014. Attualmente dispone di otto satelliti ("Sentinels") in orbita, e altri Sentinels che saranno lanciati in futuro.

militaire". Quiquet F., Qu'est-ce que le grand Commandement De l'Espace (CDE) créé par la France pour la défense de l'espace, jun 2020, Space and Cyber Security, <https://www.spacesecurity.info/quest-ce-que-le-grand-commandement-de-lespace-cde-cree-par-la-france-pour-la-defense-de-lespace/>

¹⁴⁴ "...Dabei stimmt sich das WRKdoBw mit den anderen Dimensionen, vor allem mit dem Kommando Cyber- und Informationsraum (KdoCIRKommando Cyber- und Informationsraum), ab. Es arbeitet übergeordneten Dienststellen – wie etwa dem Einsatzführungskommando der Bundeswehr oder künftig dem Territorialen Führungskommando der Bundeswehr – fachlich zu. Daneben stehen die Sicherheit deutscher Weltraumsysteme und die Warnung sowie der Schutz der deutschen Bevölkerung vor sicherheitsrelevanten Weltraumereignissen im Fokus". Official site, <https://www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/das-weltraumkommando-der-bundeswehr-5443406>

¹⁴⁵ European Global Navigation Satellite Systems Agency, 'EU Space Ambition in Focus in Prague', 4 December 2019 (<https://www.gsa.europa.eu/newsroom/news/eu-space-ambition-focus-prague>).

Galileo è un sistema globale di navigazione satellitare (GNSS) civile europeo. Avviato nel 1999, il programma mira a fornire segnali di navigazione e di sincronizzazione oraria molto precisi, indipendenti da altri sistemi esistenti grazie ai 26 satelliti in orbita. Dal 2016, Galileo fornisce i servizi iniziali: un segnale di servizio aperto per applicazioni di radionavigazione satellitare di massa, come la navigazione di veicoli a motore o servizi di telefonia mobile, un “servizio pubblico regolamentato” (public regulated service – PRS) per utenti governativi nel settore della sicurezza e della difesa, un servizio di ricerca e salvataggio, che contribuisce a localizzare e salvare più rapidamente persone in situazioni di emergenza. Più servizi dovrebbero essere disponibili nei prossimi anni, una seconda generazione di Galileo con nuove funzionalità è già in corso di preparazione e i primi satelliti dovrebbero essere lanciati a partire dal 2024. EGNOS è il Servizio europeo di copertura per la navigazione geostazionaria, fornisce dal 2009 servizi di navigazione agli utenti nei settori dell’aviazione, marittimo e terrestre, migliorando la precisione dei dati provenienti dal sistema di posizionamento globale (GPS) americano; attualmente comprende tre satelliti geostazionari e 40 stazioni terrestri.¹⁴⁶ Un ruolo fondamentale in questa architettura spaziale è dato dall’Agenzia Spaziale Europea (ESA), un’organizzazione intergovernativa istituita nel 1975 con ampie competenze nel settore spaziale; pur non essendo un organismo dell’UE, svolge un ruolo essenziale nei programmi dell’Unione, mettendo a disposizione le proprie competenze in materia di coordinamento tecnico dei programmi nonché di progettazione, sviluppo, appalto e funzionamento dei sistemi satellitari. Parallelamente, segue i propri programmi che sostengono lo sviluppo di tecnologie di posizionamento, navigazione e misurazione del tempo che utilizzano segnali GNSS e promuovono l’uso dell’osservazione della Terra in applicazioni scientifiche o commerciali. Affiancata all’ESA ha operato la GSA (Autorità di vigilanza europea sui sistemi GNSS), responsabile della supervisione delle infrastrutture, della fornitura dei servizi e del monitoraggio e sviluppo dei mercati di Galileo ed EGNOS. Nel mese di maggio del 2021, la GSA è stata sostituita da una nuova agenzia ovvero la European Union

¹⁴⁶ Le disposizioni relative a EGNOS e Galileo sono stabilite dal regolamento (UE) n. 1285/2013 del Parlamento europeo e del Consiglio, dell’11 dicembre 2013, relativo all’attuazione e all’esercizio dei sistemi europei di radionavigazione via satellite (GU L 347 del 20.12.2013, pag. 1).

Agency for the Space Programme (EUSPA).¹⁴⁷ Creata dal Parlamento Europeo e dal Consiglio col regolamento 696/2021 del 28 aprile 2021. Ha il compito di “governare” non solamente i programmi di navigazione satellitare dell’Unione Europea ma anche quelli di osservazione della Terra e di telecomunicazione; in generale, gestisce i programmi spaziali dell’Unione finora portati avanti da altri organi europei portando con sé un cospicuo bagaglio di know-how e di integrazione delle tecnologie utilizzate dalle industrie della filiera *downstream* che hanno fatto la differenza nella gestione delle missioni e degli altri programmi spaziali. Ad integrazione delle peculiarità descritte, offre molteplici servizi di posizionamento, navigazione e cronometraggio con le componenti Galileo ed EGNOS ed è incaricata di comunicare, promuovere e sviluppare il mercato dei dati, delle informazioni e dei servizi derivanti da Copernicus e GOVSATCOM. Operando in sinergia con altre strutture, è in grado di dare attuazione ai programmi spaziali dell’Unione fornendo servizi affidabili, massimizzando i benefici economici e sociali per le imprese e le società europee, migliorando la competitività, promuovendo e rafforzando l’autonomia, lo sviluppo e l’indipendenza tecnologica dell’Unione e degli Stati membri, anche nell’ottica di realizzare un sistema di difesa comune. Tra i focus vi è quello di sostenere lo sviluppo di un ecosistema spaziale europeo più ampio, con attenzione all’imprenditorialità e all’innovazione negli Stati membri e nelle regioni dell’Unione. L’Unione Europea, successivamente all’uscita del Regno Unito, ha dovuto riconsiderare l’evoluzione di programmi spaziali di sicurezza in sede dell’Agenzia Spaziale Europea (ESA) e ricollocarli presso enti sotto diretto controllo degli organi dell’Unione. Questo anche in relazione al fatto che il Regno Unito, è uno dei maggiori contributori dell’ESA, pertanto, potrebbe rimodulare i suoi programmi per una visione chiaramente più egoistica. Esistono tuttavia sfumature da non sottovalutare nella gestione di ESA e EUSPA, anche nella prospettiva di evitare sovrapposizioni e diverse impostazioni che devono obbligatoriamente coordinarsi per affrontare una sfida epocale caratterizzata da implicazioni di tipo

¹⁴⁷ L'EUSPA gestisce gli interessi pubblici connessi ai programmi del sistema globale di navigazione satellitare dell'UE (GNSS) EGNOS (Servizio europeo di copertura per la navigazione geostazionaria) e Galileo, al programma Copernicus di osservazione della Terra e al programma di comunicazione satellitare governativa dell'Unione europea (GOVSATCOM). https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/euspa_it

sia industriale e sia giuridiche tra i paesi membri. Riuscire a equilibrare questi due elementi significa condividere e difendere le capacità presenti, mantenendo un grado di autonomia il più possibile elevato. La comunanza di intenti consentirà alle due agenzie di essere competitive nello scenario globale per combinare assieme tutte le competenze e le tecnologie disponibili.¹⁴⁸ Altro aspetto da non sottovalutare è quello della definizione di prerogative certe e complementari alle due agenzie allo scopo di pervenire a una chiara identità delle stesse esaltando una maggiore valorizzazione delle rispettive peculiarità. Come detto in premessa, parlare di politiche spaziali e di interesse al dominio spazio, in Europa è complicato, dal momento che spesso non appaiono coincidere tra i vari Paesi, neppure i minimi presupposti riguardanti i prodotti e le attività essenziali frutto delle citate agenzie. Ad esempio, esistono delle differenze notevoli circa il modo di sostenere la diffusione dei servizi spaziali. La Germania e la Francia avevano adottato programmi di lavoro nazionali per assistere le amministrazioni nazionali nell'utilizzare Copernicus ed altri servizi, ma non avevano condotto un'analisi esaustiva di come tale utilizzo potesse accrescere l'efficienza e l'efficacia delle rispettive amministrazioni pubbliche. La Repubblica Ceca aveva incluso nel piano nazionale per lo spazio l'utilizzo di tali servizi da parte degli utenti, seppur in assenza di un programma di lavoro specifico. In Francia, il programma riguardava solo i servizi di responsabilità di due ministeri. Tuttavia, l'agenzia spaziale francese CNES, che inizialmente si occupava della sola promozione dei servizi spaziali, ha quindi definito partenariati specifici con le amministrazioni pubbliche, le agenzie per lo sviluppo economico e le iniziative a sostegno delle start-up per facilitare la diffusione, l'adozione e la commercializzazione delle applicazioni spaziali, per creare un miglior collegamento tra il settore spaziale e gli attori non spaziali e facilitare il trasferimento di conoscenze come fonte di innovazione. Sotto il profilo della sicurezza e della difesa, osservando la situazione attuale e, in prospettiva quella futura, è probabile che le attuali strutture e le risorse spaziali dell'UE possano essere soggette ad attacchi e operazioni cinetiche o cyber tali da comprometterne la funzionalità. Tali nuove esigenze impongono la

¹⁴⁸ Il Financial Framework Partnership Agreement dello scorso 22 giugno tra ESA e UE (e quindi EUSPA), che cerca di definire i compiti sui progetti comuni, è solo il primo passo nella definizione precisa dei compiti di EUSPA e ESA.

modernizzazione delle reti satellitari e una pianificazione operativa più efficace attraverso una progettazione preparativa che riesca a integrare nel modo più completo possibile la dimensione spazio nelle future esercitazioni per la gestione delle crisi, proponendo specifiche esercitazioni spaziali UE. Potrebbe aiutare in tal senso la predisposizione di uno "strategic compass dello Spazio" appositamente dedicato, che aiuti i paesi a meglio comprendere le minacce spaziali, identificare le lacune emergenti dalle capacità spaziali, pianificare le future politiche geospaziali e di intelligence, migliorare la formazione operativa e elaborare una guida tattica per garantire una strategia dell'UE nello spazio con un migliore margine di autonomia. Si tratterebbe di produrre una "strategia spaziale e di difesa" in grado di guidare meglio le strutture militari e civili dell'UE e il conseguente dispiegamenti di gestione delle crisi e contribuire per inquadrare le esigenze dell'Unione. Inoltre, una tale Strategia inviterebbe anche a riflessione che si rende necessaria circa l'evoluzione futura del SatCen (sul quale si è avuto modo di parlare nei precedenti capitoli), soprattutto alla luce delle future esigenze operative. In particolare, è necessario garantire che il SatCen continui a essere un pilastro della strategia dell'UE autonomia; si tratta di un aspetto costituente un presupposto fondamentale nell'ottica della gestione e della destinazione di future risorse che consentirebbero al Centro di disporre di tecnologie all'avanguardia, indispensabili a operare anche in un contesto di intelligence geospaziale complesso. Tali considerazioni valgono ancora più se si considera che, secondo alcune stime attuali, nei prossimi anni il ruolo del SatCen nella fornitura di informazioni per missioni e operazioni PSDC (e per la sicurezza e difesa dell'UE) aumenterà in maniera considerevole, parallelamente ad una maggiore visibilità operativa, producendo una maggiore richiesta da parte dei paesi membri. L'Italia ha adottato una strategia nazionale per sfruttare le potenzialità dei programmi spaziali dell'UE ricercando contemporaneamente decisi margini di miglioramento sia nel settore aerospaziale e sia in prospettiva a una migliore crescita economica; si tratta di una strategia incentrata sullo sviluppo economico e sugli investimenti del settore privato e ha previsto di accorpare le domande degli enti locali o regionali che non sfruttano le potenzialità dei servizi spaziali. La finalità di tale approccio è quella di creare sinergie tra le autorità pubbliche, che potrebbero consentire loro di trarre vantaggio da soluzioni efficaci in termini di costi. Spazio e

difesa sono ormai un binomio che si rafforza e si espande su più livelli e il nostro Paese, che è secondo in UE per numero di satelliti in orbita e terzo investitore nei programmi della European Space Agency, ne è consapevole. Nel settore Difesa e Spazio, le nostre forze armate operano già dal 2001, anno in cui venne lanciato il Sicral,¹⁴⁹ primo satellite per comunicazioni sicure, il cui programma continua a essere riconfermato e che ha permesso al nostro Paese di mettere a disposizione anche in ambito NATO, importanti servizi, garantendo una posizione di prestigio in ambito internazionale. Ma una decisa azione di cambiamento è avvenuta nel 2018, anno in cui il Ministero della Difesa ha intrapreso una sostanziale riorganizzazione del settore che ha visto l'istituzione, nel 2019, ad opera dello Stato Maggiore della Difesa, dell'Ufficio generale Spazio (Ugs),¹⁵⁰ responsabile della politica di pianificazione, dei programmi spaziali e della cooperazione internazionale. Nel 2020 è stato creato il Comando operazioni spaziali (Cos)¹⁵¹ per

¹⁴⁹ Il SICRAL (Sistema Italiano per Comunicazioni Riservate ed Allarmi) è un sistema di comunicazioni militari via satellite che assicura le comunicazioni strategiche e tattiche sul territorio nazionale e nelle operazioni fuori area e le comunicazioni mobili con piattaforme terrestri, navali ed aeree. Il SICRAL è composto da due sottoinsiemi: il segmento spaziale ed il segmento terrestre. Il segmento spaziale è costituito sostanzialmente dal satellite con le facilities associate. Il segmento terrestre è composto dal Centro di Gestione e Controllo di Vigna di Valle, e dai terminali utenti. L'Amministrazione della Difesa, in particolare con il Reparto TEI (Telecomunicazioni Elettronica Informatica) dello Stato Maggiore della Difesa, ha gestito tutte le attività di preparazione all'impiego del satellite tra le quali l'evoluzione del sistema di logistica integrata, preparato dal consorzio SITAB (Telespazio - Alenia Spazio - BPD FIAT Avio), e la formazione del personale che dovrà operare con il sistema. <https://www.difesa.it/Content/Manifestazioni/FORUMPA/2004/SistemaSICRAL/Pagine/default.aspx>

¹⁵⁰ L'Ufficio Generale per lo Spazio si compone di due uffici: il 1° Ufficio "Innovazione per l'Aerospazio" e il 2° Ufficio "Politica Spaziale e Operazioni". Nell'ambito dello Stato Maggiore dell'Aeronautica l'Ufficio Generale per lo Spazio si configura come l'elemento di Organizzazione che gestisce attività ed esigenze nel settore spaziale di interesse dell'Aeronautica Militare, coordinandosi sia con gli Enti interni alla Forza Armata che quelli esterni. Si occupa principalmente di: definire la policy e la strategia dell'AM nel settore spaziale in coordinamento con il 3° Reparto dello Stato Maggiore; seguire ed indirizzare le attività di cooperazione internazionale d'interesse dell'AM nel settore, ricercando la valorizzazione delle competenze disponibili in ambito Forza Armata; assicurare, in coordinamento con il 3° Reparto dello Stato Maggiore, l'utilizzo integrato, coordinato e sincronizzato dei servizi e delle capacità spaziali proprietarie e non, a supporto delle capacità operative della Forza Armata; garantire le massime sinergie anche a livello interforze rendendo disponibili le competenze AM nel settore, anche attraverso il mantenimento dei rapporti con le Università, gli Enti di Ricerca e le Istituzioni Nazionali ed Internazionali coinvolte nello sviluppo ed ammodernamento dei sistemi spaziali. <https://www.aeronautica.difesa.it/organizzazione/loStatoMaggiore/organigramma/Pagine/UGS.aspx>

¹⁵¹ Il COS è stato costituito l'8 giugno 2020, in attuazione degli indirizzi del Capo di Stato Maggiore della Difesa, con l'obiettivo di potenziare la capacità nazionale di operare nel dominio spaziale, assicurando la protezione e la difesa degli assetti spaziali nazionali e integrandone efficacemente i servizi nelle operazioni. A seguito di tale riorganizzazione, tale Comando è diventato l'unico elemento di organizzazione a livello operativo nello specifico settore, costituendo l'interfaccia di riferimento operativa sia verso le F.A. sia in campo interministeriale e internazionale. Il COS ha alle

sviluppare le operazioni nel nuovo dominio e consentire alle forze armate operanti nei domini più tradizionali, di poter fruire con maggiore facilità, dei prodotti provenienti dal settore spaziale. L'esistenza di queste due strutture segna un'architettura basata su un equilibrio concreto tra le due strutture citate; l'Ugs ha il compito di sviluppare la prospettiva strategica e il Cos di aumentare la capacità operativa. È sostanzialmente un primo passo verso la definizione di una strategia della Difesa per lo spazio comprensiva di una dottrina militare e delle linee guida che condurranno ad una adeguata collocazione delle Forze Armate, all'interno di questo dominio. Più di recente, il 31 gennaio 2022 è stato lanciato da Cape Canaveral il secondo satellite italiano di nuova generazione COSMO-SkyMed,¹⁵² parte di una costellazione composta da sei assetti per l'osservazione radar della Terra. Tra le caratteristiche del programma ci sono quelle di oltrepassare i limiti ottici imposti da ostacoli naturali (ad esempio dalla meteorologia, dalla vegetazione e dall'assenza di luce), e l'introduzione di nuove tecnologie che hanno determinato una migliore performance in termini di qualità e quantità dell'osservazione. Lo sviluppo di questo progetto coinvolge buona parte del nostro settore aerospaziale comprese Thales Alenia Space Italia, Telespazio, Leonardo ed e-Geos, dai segmenti di *upstream* (manifattura e lancio) al *downstream* (gestione e commercializzazione dei dati), passando per il comando e controllo del segmento di terra. Considerato un programma all'avanguardia in Europa e nel mondo, pioneristico nello sfruttare un approccio duale che vede coinvolti Ministero della Difesa e Agenzia Spaziale Italiana (ASI) nello sviluppo di un assetto condiviso, come ampiamente sperimentato da

dirette dipendenze il Centro Interforze Gestione e Controllo SICRAL. Il Centro Interforze Telerilevamento Satellitare (CITS) e il neo-costituito Centro SSA (Space Situation Awareness) hanno un collegamento tecnico-funzionale con il COS. https://www.difesa.it/SMD_/Avvenimenti/giornata_nazionale_spazio/Pagine/Comando_Operazioni_Spaziali.aspx

¹⁵² COSMO-SkyMed è la prima missione di Osservazione della Terra concepita per scopi duali, civili e militari. I suoi satelliti di prima e seconda generazione sono 'occhi' in grado di scrutare la Terra dallo spazio metro per metro, di giorno e di notte, con ogni condizione meteo per aiutare a prevedere frane e alluvioni, a coordinare i soccorsi in caso di terremoti o incendi, a controllare dall'alto le aree di crisi. Sviluppato dall'Agenzia Spaziale Italiana in cooperazione con il Ministero della Difesa, COSMO-SkyMed si basa su una costellazione di satelliti dotati di radar ad apertura sintetica (SAR) che lavorano in banda X (in grado, quindi, di vedere attraverso le nuvole e in assenza di luce solare). Il 18 gennaio 2021 COSMO-SkyMed Seconda Generazione (CSG) è diventato operativo con il primo di quattro satelliti previsti, ed è andato ad affiancare i quattro di prima generazione. La costellazione COSMO-SkyMed può dunque vantare oggi ben cinque satelliti in orbita ed operativi. <https://www.asi.it/scienze-della-terra/cosmo-skymed/>

numerosi impieghi civili e militari in un vasto campo di applicazioni, quali lo studio del cambiamento climatico, il monitoraggio delle infrastrutture critiche, la gestione delle emergenze e l'osservazione di aree sensibili e strategiche. Tutti i progetti nazionali al momento rispondono a esigenze specifiche, legate alla crescente necessità per il mondo militare, di fruire dei servizi di Earth Observation, ritenute essenziali per le attività di sorveglianza e ricognizione e più in generale per le attività di intelligence, a supporto dei processi decisionali in ambito politico-militare.

3.4.2 Tecnologie e sistemi antisatellite

Da parecchi anni Stati Uniti, Russia, Cina e India svolgono attività spaziali che comprendono anche la sperimentazione di sistemi missilistici antisatellite, con la conseguente produzione di migliaia di detriti che vagano nello spazio creando non pochi problemi alla sicurezza dei satelliti in orbita. La materia è da lungo tempo dibattuta e affrontata a seconda delle circostanze e delle convenienze stante i cori di disapprovazione che si sollevano ogni qualvolta a seguito di test viene distrutto un satellite o attraverso altri esperimenti vengono prodotti detriti vaganti. Sotto il profilo storico, tale situazione è il frutto di una corsa agli armamenti, intrapresa agli inizi del XXI secolo, quando ancora la dimensione strategica dello spazio era limitata all'intelligence stante la presenza dei satelliti spia che faceva sì che lo spazio continuasse ad essere una frontiera libera per le applicazioni militari. In effetti, e ciò può essere riscontrato da un esame di trattati e accordi internazionali, gli assetti spaziali sono sempre stati esclusi dai negoziati per il disarmo, occasioni che invece vedevano al centro dei colloqui le tematiche afferenti alle armi nucleari. Sempre ai margini della Guerra Fredda e più precisamente negli ultimi decenni, si sviluppò la tematica della superiorità strategica nello spazio, stante lo sviluppo soprattutto delle armi nucleari, anche se e in questo periodo, Stati Uniti e Unione Sovietica avevano avviato diverse discussioni mirate anche alla limitazione di armi ASAT¹⁵³ di cui tuttavia nessuno voleva fare a meno. Iniziò così un percorso attorno

¹⁵³ Le armi Anti Satellite (ASAT) sono sistemi progettati per danneggiare o colpire i satelliti impiegati per scopi militari e strategici. USA e URSS hanno sviluppato e testato questi dispositivi durante la Guerra Fredda. Tuttavia una moratoria internazionale, de facto, è stata rispettata dal termine del

al quale nonostante si registrassero significativi risultati nella riduzione delle armi nucleari, nessun passo avanti veniva fatto circa i sistemi ASAT. Gli Stati Uniti in particolare non volevano assumere un ruolo secondario e non volevano assolutamente perdere una superiorità (o presunta tale) nel settore. In una riunione alla Casa Bianca del National Security Planning Group del dicembre 1984 tenutosi in preparazione del round di colloqui START (*Strategic Arms Reduction Talks*) di Ginevra del gennaio 1985, Kenneth L. Adelman, Direttore dell'United States Arms Control and Disarmament Agency (ACDA), sosteneva l'importanza di proteggere la Strategic Defence Initiative (SDI) del Presidente Ronald Reagan dalle questioni ASAT, "... negoziando regole di comportamento per sistemi anti-satellitari e per gli stessi satelliti... rendendo il mondo più sicuro attraverso l'uso controllato dello spazio...". Nello stesso *meeting* l'allora Segretario di Stato George P. Shultz disse che era stato concordato anche un forum per le armi ASAT e in generale gli armamenti spaziali ma che esisteva il problema "di una sovrapposizione tra ASAT e SDI".¹⁵⁴ Alla fine, quindi, prevalse l'approccio di non includere i sistemi d'arma spaziali nei negoziati per non indebolire sia la posizione USA che gli stessi negoziati¹⁵⁵. La consapevolezza di aver conseguito un momentaneo predominio nello spazio¹⁵⁶ era sufficiente per gli USA a tenere questa linea politica, peraltro sostanzialmente mantenuta nel corso degli anni. La realtà odierna invece è molto più complessa, le applicazioni civili per lo spazio si sovrappongono a quelle militari portando alla conseguenza che la supremazia nella space economy diventa anche una supremazia strategica. Proprio in funzione di questo, stante il fatto che molti satelliti svolgono ruoli essenziali non solo nei settori militari ma anche nei settori civili, i paesi concorrenti nella corsa allo spazio, continuano a sviluppare e sperimentare sistemi missilistici anti satellite (ASAT) che

confronto bipolare. Attualmente si ritiene che i paesi ad aver sviluppato tali dispositivi siano gli Stati Uniti, la Russia e la Cina.

¹⁵⁴ Foreign Relations of the United States – 1981–1988, volume IV – Soviet Union, January 1983 – March 1985. <https://history.state.gov/historicaldocuments/frus1981-88v04>

¹⁵⁵ Foreign Relations of the United States – 1981–1988, volume IV – Soviet Union, January 1983 – March 1985

¹⁵⁶ Nell'estate del 1960, gli Stati Uniti avevano lanciato in orbita Corona, il loro primo satellite di *intelligence* per immagini. Nella sua prima missione, aveva ripreso l'Unione Sovietica più di tutti i precedenti voli di ricognizione U-2 messi insieme, i satelliti erano diventati in breve tempo la più grande fonte di informazioni sull'Unione Sovietica. I *leader* della sicurezza nazionale americani temevano che un programma USA di armi ASAT avrebbe rischiato di spronare i sovietici ad agire in modo aggressivo contro i sistemi spaziali statunitensi, mettendo a rischio i vulnerabili satelliti dell'*intelligence*. A.Zanini: Armi antisatellite: la nuova corsa agli armamenti spaziali, Aspenia online, 31 gen. 2022, <https://aspeniaonline.it/armi-antisatellite-la-nuova-corsa-agli-armamenti-spaziali/>

possano portarli a un ruolo di leader con conseguente potere contrattuale maggiore. A nulla finora sembrano essere valse le raccomandazioni politiche a sopersedere da una corsa ai sistemi ASAT proprio perché l'interesse è comune e nessuno vuole restare indietro in questa corsa. La caratteristica già accennata della "dualità" dei sistemi, contribuisce ad arricchire l'interesse da parte dei più svariati attori operanti in diversi settori, grazie anche ad una inarrestabile evoluzione tecnologica. Sostanzialmente sono poche ormai le differenze tra le applicazioni civili e quelle militari, come era facilmente intuibile già a partire negli anni '90 con lo sviluppo del sistema di satelliti noto con il nome di Iridium.¹⁵⁷ Il sistema doveva sopperire alle difficoltà dei segnali per le comunicazioni dei satelliti geostazionari, troppo deboli per raggiungere efficacemente le alte latitudini. Il servizio satellitare Iridium lo ha risolto grazie a decine di satelliti aggiuntivi in orbite inferiori, raggiungendo una copertura veramente globale e diventando per tali ragioni, di estremo interesse per le comunità militari che usufruiscono, in tal modo, di una complementarietà di dati provenienti sia dal settore civile e sia da quello militare, fruibili nel contesto della sicurezza militare e nei settori dell'economica e dello sviluppo. Spesso l'infrastruttura spaziale viene definita, non a caso, "l'infrastruttura delle infrastrutture" essendo essa il fulcro gestionale dei sistemi di comunicazione, navigazione, dei sistemi di intelligence economica e scientifica e di quella militare. Da essa dipendono soprattutto le capacità militari e strategiche ma anche quelle economiche e finanziarie, potendo contare su una pervasività notevole e sfruttando quelle caratteristiche che la rendono unica poiché senza confini e in grado di arrivare a qualsiasi utente sia esso una figura istituzionale o un privato cittadino. Nello spazio attualmente operano numerose società come la statunitense SpaceX con circa 40 mila satelliti in orbita, la britannica OneWeb con 6.400, la Kuiper Systems (collegata ad Amazon) con 3.400,

¹⁵⁷ Iridium è un sistema basato su 66 satelliti LEO la cui copertura è globale ed include le regioni Polari: la più vasta costellazione al mondo di satelliti per le telecomunicazioni ad uso privato. Il progetto "Iridium" viene annunciato da Motorola nel 1990 con una conferenza stampa simultanea da Pechino, Londra, Melbourne e New York. Il nome prende spunto dall'Iridio, elemento identificato con il numero 77 nella tavola periodica: il disegno iniziale infatti prevedeva la messa in orbita di 77 satelliti. Il 1° Novembre 1998, con i suoi 66 satelliti, la rete Iridium è completata ed il servizio operativo. L'operatore Iridium Communication Inc., è una società quotata in borsa situata nel Maryland, Stati Uniti. Iridium è l'unico sistema di telefonia satellitare che supporta comunicazioni voce e dati da e verso qualsiasi punto della Terra, compresi i Poli. L'architettura di rete della costellazione garantisce una buona qualità della voce ed una grande affidabilità del servizio, tanto da poter essere equiparata ad una comunicazione mobile terrestre. <https://www.intermatica-shop.it/it/content/operatore-satellitare-iridium>

la canadese Telsat con 1.600, la statunitense Mangata con 800, con un volume d'affari che nel 2020 è stato quantificato in circa 450 miliardi di dollari secondo fonti della Space Foundation. Cifre destinate a vertiginosi aumenti che indicano tutti i Paesi a incrementare gli sforzi di investimento che ritengono, a ragione veduta, questo settore, di importanza strategica per il futuro.¹⁵⁸ Tuttavia la notorietà della Space X e del sistema Starlink tutti che conferma l'assunto appena esposto ma soprattutto evidenzia l'integrazione assolutamente indispensabile tra il settore privato e quello pubblico è il caso della rete satellitare Starlink creata dallo statunitense Elon Musk, nell'ambito della società SpaceX. Si tratta di decine di migliaia di satelliti già in orbita e altri che verranno lanciati a breve, che presto costituiranno una costellazione pari a circa 40 mila unità. Intanto si sono rivelati indispensabili per le operazioni belliche in corso in Ucraina assumendo addirittura un ruolo nel contesto geopolitico più globale, capace di spostare peso specifico, capacità e effetti a seconda delle decisioni prese circa il loro uso nel contesto tattico specifico. Stante il ruolo oggi assunto dall'infrastruttura spaziale nel contesto dei moderni conflitti è lecito pensare che le forze armate di tutto il mondo svilupperanno i mezzi per interferire con i satelliti in tempo di guerra e, preventivamente, in tempi di pace. La lezione della Guerra Fredda è che è molto probabile che le proposte volte a limitare i comportamenti nello spazio siano più facilmente raggiungibili rispetto alle limitazioni o divieti di classi di sistemi d'arma con applicazioni anti-satellite. Nonostante l'attuale enfasi sul divieto dei test spaziali per la produzione di detriti, enfasi paradossalmente avanzata anche da coloro che producono quei test e quei detriti, non è detto che in futuro non ci possano essere negoziati su applicazioni militari spaziali di diverso genere. Un esempio in tal senso potrebbe essere fornito dalle discussioni volte a prevenire l'interferenza cinetica e non cinetica con i satelliti utilizzati per il comando e il controllo nucleare e l'allerta precoce, accordi che potrebbero ridurre la probabilità di un'escalation nucleare. Si tratta solo di un'ipotesi semplicistica poiché sono

¹⁵⁸ I governi hanno invece investito nel settore 92,4 miliardi di dollari nel 2021, secondo la società di ricerca Euroconsult: 54,6 gli Stati Uniti, 10,3 la Cina, 4,2 il Giappone, 3,9 la Francia, 3,6 la Russia, 2,4 la Germania, 2,0 l'India, 1,5 l'Italia e il Regno Unito. I denari spesi dall'Amministrazione di Washington sono andati per circa la metà in operazioni civili della Nasa o di aziende commerciali, il resto a programmi della Space Force, dell'Air Force e di altre parti del Dipartimento della Difesa. "Il boom dei satelliti: affari e geopolitica" Taini D., aprile 2022, https://www.corriere.it/opinioni/22_aprile_20/boom-satelliti-affari-geopolitica-c4d14ef4-c0d6-11ec-a9eb-2524bc1194db.shtml

tante le variabili che incidono su negoziazioni e accordi. Sostanzialmente, per promuovere una vera stabilità operativa e strategica nello spazio, le citate Potenze quali gli Stati Uniti, la Russia, la Cina, l'India e altri paesi dovrebbero moltiplicare gli sforzi per arrivare ad un bando definitivo contro le sperimentazioni in grado di produrre detriti. Una *road map* diplomatica che dovrebbe ripartire, almeno formalmente, dall'UNOOSA di Vienna. Anche l'Unione Europea vuole ritagliarsi un suo ruolo in questo dominio. Alle dichiarazioni del 2021 dell'Alto Rappresentante J. Borrel sono seguiti precisi impegni legati ad affrontare le tematiche legate alla sicurezza e difesa dello Spazio, tutte inserite nell'Agenda europea. Il duplice obiettivo è quello di sviluppare una strategia ad hoc e, contemporaneamente, di muoversi verso una sempre maggiore riduzione delle dipendenze tecnologiche e strategiche nel settore. "Lo spazio sarà il nuovo campo di battaglia con la guerra dei satelliti, così come quello cibernetico", ha sottolineato Borrell. I due nuovi domini operativi saranno, quindi, tra gli elementi principali su cui si concentrerà la nuova strategia di Bruxelles, sempre più indirizzata all'autonomia strategica in questi campi. Sarà necessario un confronto tra i Paesi europei per garantire la sicurezza dello spazio e dei suoi molti satelliti, contro le crescenti minacce. Per far questo l'UE ha già previsto uno stanziamento pari a un miliardo di euro da distribuire fino al 2027, nell'ambito del Fondo Europeo per la Difesa, per far avanzare gli armamenti dei 27 più la Norvegia, svincolarsi dalla fornitura di altri Paesi e dotarsi di armi tecnologicamente avanzate. Varato lo scorso anno e gestito dalla Direzione generale per l'industria e lo spazio, il veicolo di investimento serve a foraggiare progetti di ricerca, prototipi e alleanze industriali per esplorare le frontiere dei futuri sistemi d'arma: droni, difese cibernetiche, nuovi materiali, sensori avanzati e contraerea per proteggersi da missili ipersonici. Uno stanziamento per le esigenze citate è stato fatto nella misura di 150 milioni di euro, di cui 20 per organizzare un'indipendenza in ambito spaziale dell'Europa, dal lancio dei satelliti alla gestione del dato. Altri 40 sono dedicati alla realizzazione di una costellazione di mini-satelliti con funzioni di intelligence, sorveglianza e riconoscimento di minacce, con una risoluzione inferiore a mezzo metro. Infine 90 milioni servono a realizzare un sistema

spaziale che identifichi minacce missilistiche, a cominciare dalle nuove armi ipersoniche.¹⁵⁹

3.4.3 Geopolitica dei fondali marini

La nascita dei cavi sottomarini può essere fatta risalire al 1842, con l'invenzione del codice Morse e la posa di un cavo nelle acque del porto di New York. Nel 1850, la compagnia anglo-francese *Channel Submarine Telegraph Company* posò il primo cavo commerciale tra l'Inghilterra e la Francia,¹⁶⁰ mentre nel 1858 ci fu la posa del primo cavo telegrafico transatlantico, ad opera della *Atlantic Telegraph Company*, che collegava Terranova (Trinity Bay, nell'attuale Canada) a Valentia, nell'Irlanda occidentale. Il cavo rimase attivo per sole tre settimane prima di rompersi irreparabilmente, ma in questo breve lasso di tempo riuscì a trasmettere la prima comunicazione ufficiale tra due continenti, ossia un messaggio di congratulazioni della regina Vittoria al presidente degli Stati Uniti James Buchanan. Nel 1866, la *Anglo-American Telegraph Co.* costruì un cavo in grado di collegare stabilmente le due sponde dell'Atlantico.¹⁶¹ La riuscita dei progetti sopra elencati contribuì a incrementare la posa di molti altri cavi, rendendo i progetti particolarmente interessanti sotto diversi profili. Dal punto di vista tecnologico, i cavi sottomarini entravano nel novero delle infrastrutture essenziali per gli scopi commerciali, geopolitici e di cooperazione regionale delle grandi potenze, mentre dal punto di vista politico, la loro esistenza, rafforzava la cooperazione tra il Regno Unito e gli Stati Uniti, contribuendo a consolidare quella *special relationship* che ancora oggi caratterizza le relazioni bilaterali tra Londra e Washington. Il progresso

¹⁵⁹ A new arms race is afoot. China, Russia, and the United States are aggressively pursuing the development and deployment of advanced hypersonic weapons, while other states are starting or scaling up their own programs. But what are these weapons? Who's working on what? And what are the implications for global security? A strategy for managing the race toward these weapons—which combine speed with maneuverability and long ranges—has never been more crucial. <https://carnegieendowment.org/programs/npp/hypersonic/>

¹⁶⁰ The submarine telegraph company. Brothers Jacob Brett and John Watkins Brett formed the English Channel Submarine Telegraph Company after obtaining landing rights from the French and British authorities allowing them to lay a submarine cable between the two countries. The French concession was conditional on telegraphic communication being established by 1 September 1850. <https://atlantic-cable.com/stamps/Cables/hips/indexstc.htm>

¹⁶¹ After the loss of the 1865 Atlantic cable steps were taken to raise capital for a further attempt to span the Atlantic. A new company, The Anglo-American Telegraph Company, was set up with a capital of £600,000. Most of the money was raised in England with the Telegraph Construction and Maintenance Company (Telcon) supplying the cable in return for shares in the new company. The new company took over the assets of the New York, Newfoundland and London Telegraph Company which owned the cables laid between Newfoundland and Canada and the landline from St. Johns to Cape Ray. <https://atlantic-cable.com/CableCos/AngloAmerican/>

tecnologico ha infine consentito l'evoluzione della loro struttura e il miglioramento delle prestazioni, portando, nel 1940, all'introduzione dei ripetitori, potenzialmente in grado di aumentare il segnale lungo tutto il percorso dell'infrastruttura, e nel 1955 alla posa del primo cavo telefonico sottomarino, TAT-1.¹⁶² Soltanto molti decenni dopo, più precisamente negli anni 80, si perfezionò la posa dell'ottavo cavo di comunicazione transatlantico, TAT-8, questa volta per la prima volta in fibra ottica. Attualmente risultano essere operativi nel mondo più di 400 cavi sottomarini. Si tratta di un mercato con forti barriere all'ingresso, dati gli altissimi costi di produzione e manutenzione. Si stima, infatti, che i costi per chilometro oscillino da 28.000 a 90.000 dollari. Le aziende attive nel settore sono dunque le Telco, le aziende specializzate nella costruzione e nella manutenzione dei cavi, molto spesso consorziate alle prime, e più di recente le compagnie Big tech statunitensi, in particolare *Facebook*, *Google*, *Amazon* e *Microsoft*. Diverse, poi, sono le criticità in ordine alla sicurezza dei cavi, trattandosi di infrastrutture esposte a una serie di fattori, come eventi naturali (terremoti o danni dovuti ai morsi degli squali) o legati ad attività umane (pesca), che possono minacciare l'integrità fisica del cavo e il suo funzionamento. Un caso emblematico è rappresentato dal terremoto del Hengchun che nel 2006 ha colpito lo stretto di Luzon, tra Taiwan e le Filippine, importante punto di strozzatura con il passaggio di molti cavi sottomarini.¹⁶³ Le frane innescate dal terremoto hanno provocato il danneggiamento di 8 cavi, bloccando le comunicazioni Internet per 49 giorni e impattando fortemente sull'economia dei Paesi dell'area (Taiwan, Cina, Hong Kong, Giappone, Singapore e Corea del Sud). Nonostante gli sviluppi tecnologici in corso e le tendenze verso soluzioni che puntano a device wireless, gran parte della connettività globale odierna passa attraverso cavi di connessione sottomarini costituenti un'immensa infrastruttura critica che si estende per 1,2 milioni di chilometri di lunghezza che consente la quasi totalità del traffico internet globale e che, in un'ottica futura, stante l'avvento di nuovi standard di comunicazione e dell'affermazione del 5G e delle tecnologie correlate, assumerà un'importanza

¹⁶² Transatlantic Telephone Cable System 1 (TAT-1) was inaugurated on 25 September 1956 with a three-way telephone conversation between New York, Ottawa, and London. Many distinguished guests participated in this first official call over the new circuit, the first Atlantic cable of its generation. <https://atlantic-cable.com/Cables/1956TAT-1/>

¹⁶³ Tshunami: danneggiati metà dei cavi sottomarini, marzo 2011, corriere comunicazioni, <https://www.corrierecomunicazioni.it/telco/tsunami-danneggiati-meta-dei-cavi-sottomarini/>

strategica fondamentale. Proprio in funzione di tale importanza, si cerca di valutare attentamente quali possono essere i rischi e le vulnerabilità della stessa che risulta comunque essere costantemente presa di mira, come dimostrato da interruzioni, incidenti e anomalie frequenti, nonostante uno standard di affidabilità definito di livello “cinque nove” (ovvero pari al 99,999%). Nel complesso circa un terzo delle interruzione/anomalie è il frutto di danni non intenzionali, a volte dovuti ad attività legate al transito marittimo e alle attività di pesca, generalmente interessanti un singolo cavo o parte di esso con danni che non ne compromettono la funzionalità. Altra percentuale è legata a fenomeni naturali, quali eruzioni vulcaniche, frane, terremoti, che possono interessare più cavi, con conseguente criticità di funzionamento più elevata. Altri incidenti/anomalie sono invece causati da azioni dirette e consapevoli rientranti in operazioni di militari o atti di terrorismo, comunque portati avanti da attori statali e non, per interessi di varia natura. I cavi sottomarini rimangono tuttora un punto focale delle dinamiche internazionali. Ad esempio, le tensioni tra Stati Uniti e Cina, con quest’ultima determinata a mettere in discussione la globalizzazione statunitense tramite il progetto delle Nuove Vie della Seta, passano anche attraverso questa infrastruttura. Il progetto PEACE, per esempio, è da inquadrarsi in tale iniziativa: una rete di cavi a trazione cinese che già connette il Pakistan all’Africa orientale e che mira ad estendersi fino alle coste francesi.¹⁶⁴ Risulta inoltre interessante come le agenzie governative statunitensi non abbiano autorizzato l’attivazione di una parte di un cavo patrocinato da Google e Facebook che avrebbe connesso la California a Hong Kong, proprio per la minaccia che ciò avrebbe comportato per la sicurezza nazionale. Questi eventi dimostrano come, nonostante il business dei cavi sottomarini sia svolto da attori e aziende del settore privato, le decisioni a riguardo non avvengono in completa autonomia. Tutt’altro: esse sono profondamente influenzate da tensioni e ambizioni geopolitiche. Le minacce ai cavi non si limitano all’ambiente sottomarino, ma possono riguardare anche i punti di atterraggio sulla terraferma. Si tratta di stazioni ubicate spesso in

¹⁶⁴ Questo tipo di infrastruttura è diventato sempre più strategico con l’aumento della dipendenza delle economie e delle società dal Web e perché costituisce la dimensione territoriale della Rete. L’egemonia sui mari, condizione necessaria per quella globale, comporta dunque garantire l’ininterrotto flusso non solo di merci, ma pure di dati. Canali L. “L’interesse cinese a connettere Pakistan, Africa orientale e Europa. 14 agosto 2019, Limes, <https://www.limesonline.com/carta-cavi-sottomarini-internet-come-armi-il-progetto-peace-di-hauwei/114005>

piccole città costiere in cui il personale di vigilanza potrebbe non essere sufficientemente armato o qualificato per garantire la sicurezza. Inoltre, tali stazioni spesso ospitano più cavi e costituiscono punti di strozzatura la cui protezione fisica contro disastri naturali, atti terroristici e operazioni di intelligence finalizzate a installare dispositivi per registrare o sottrarre dati (c.d. tapping) è una parte fondamentale della sicurezza, che richiede investimenti e cooperazione. Come noto, i punti di atterraggio sono stati al centro del caso datagate. Lo scandalo, scoppiato nel 2013 a seguito di scoop giornalistici basati sulle rivelazioni di Edward Snowden, ha portato alla luce le attività di spionaggio condotte dalla NSA statunitense e dalla GCHQ britannica e dirette a intercettare enormi quantità di dati, comprese le comunicazioni riservate di Capi di Stato e di Governo di Paesi europei, utilizzando gli snodi dei cavi sottomarini di Mazara del Vallo, in Sicilia, e di Ayios Nikolaos, nell'isola di Cipro. I cavi sottomarini sono infrastrutture essenziali per le comunicazioni e per l'economia globale. Tuttavia, a tale ruolo strategico corrispondono fattori di rischio che peseranno sempre di più sulla sicurezza, considerando il prevedibile aumento della competizione e della conflittualità tra le grandi potenze intorno a queste infrastrutture. Sul piano della regolazione, il principale strumento convenzionale che disciplina la materia, ossia l'UNCLOS, è uno strumento ormai datato, risalendo a circa sei anni prima della costruzione di TAT-8,¹⁶⁵ il primo cavo in fibra ottica transatlantico al mondo, e necessiterebbe di un adeguamento a una realtà estremamente mutata nel corso degli ultimi anni. Sul piano operativo, invece, la tendenza a seguire percorsi predefiniti, creando in alcune zone punti di strozzatura con un'alta concentrazione di cavi, rappresenta certamente un fattore di rischio. In caso di eventi naturali o di attacchi, intere reti di cavi potrebbero collassare e bloccare in tutto o in parte le comunicazioni tra una miriade di Paesi, con conseguenze di varia natura e

¹⁶⁵ On 14 December 1988, TAT-8, the first transatlantic [optical fiber](#) cable system was completed across the Atlantic. The 3,148 mile line was capable of handling 40,000 telephone calls simultaneously. TAT-8 was built as a joint venture of AT&T, France Télécom, and British Telecom to connect the communications systems of France, Britain, and the United States. It could serve all three countries with a single line through the creation of an underwater branching unit on the continental shelf on the coast of Great Britain. Built at the cost of \$335 million and operating from 1988 to 2002, TAT-8 revolutionized communications by employing two working pairs of optical fibers, rather than traditional copper coaxial cables, to carry voice and data across the ocean. Its capacity lowered the cost of communications across the globe and provided indispensable infrastructure for the development of the Internet. Transatlantic Optical Cable, official site, https://ethw.org/Transatlantic_Optical_Cable

potenzialmente drammatiche sotto il profilo economico, sociale e politico. Al riguardo, come evidenziato da molti esponenti dell'industria, una possibile soluzione in ottica di prevenzione potrebbe risiedere nell'adozione di un approccio basato sulla ridondanza e sulla diversificazione sia delle rotte che dei punti di atterraggio. Considerata la rilevanza dei cavi sottomarini nel contesto geopolitico moderno e le minacce a cui sono esposti, appare chiara la necessità di uno sguardo più attento al settore. Questa necessità interessa in particolar modo l'Italia dove, nonostante si siano registrati dei passi avanti nel campo della difesa cibernetica, l'importanza dell'infrastruttura dei cavi sottomarini rimane ancora poco discussa. Per il sistema-Paese Italia, adottare una strategia a riguardo è fondamentale. Tale strategia deve essere mirata sia alla minimizzazione delle vulnerabilità sopracitate, sia alla valorizzazione della posizione strategica dell'Italia nell'hub del Mediterraneo, dove il Paese occupa un ruolo centrale rispetto alle rotte dei cavi sottomarini. In tal senso, approfondire il legame fra infrastrutture digitali e stabilizzazione politica nei paesi nordafricani e mediorientali sarebbe, per esempio, un ottimo inizio. Nel mondo delle telecomunicazioni vi è da qualche anno gran fermento in merito ai cavi a fibre ottiche appositamente posati in fondo al mare per tratte o dorsali, finalizzati a trasportare informazioni telefoniche o internet, o potenzialmente di altra natura. Durante l'ultimo vertice dei cosiddetti sette grandi, tenutosi lo scorso mese di giugno al Castello di Elmau in Germania, è stata perfezionata una nuova iniziativa denominata in sigla PGII (Partnership for Global Infrastructure and Investment),¹⁶⁶ da intendersi come risposta, già lanciata negli ultimi due G7 su impulso statunitense, alla ormai datata BRI (Belt and Road Initiative) di marca cinese.

¹⁶⁶ The PGII is an ambitious \$600 billion funding initiative to spearhead infrastructure projects in the developing world with a special emphasis on transparent, sustainable, and democratically driven methods of engagement. This collective effort by the world's leading democracies is an attempt to balance and hopefully offset China's multi-trillion-dollar Belt and Road Initiative (BRI), which has a global span encompassing more than 100 countries. McLain D.J.: Will the partnership for Global infrastructure and investment be a game-changer in the Indo pacific? July 2022, East-West Center, <https://www.eastwestcenter.org/publications/will-the-partnership-global-infrastructure-and-investment-be-game-changer-in-the-indo>

3.5 Processi decisionali ed esigenze di sicurezza

3.5.1. Difesa totale e resilienza

Il concetto di Difesa totale più volte emerso e teorizzato a partire dal XX secolo, assume oggi degli aspetti in parte nuovi e comunque dettati da diverse esigenze di difesa. Gli attuali conflitti e prima ancora le tensioni registrate sul continente europeo hanno determinato in molti paesi, la una necessità di rivedere le proprie strategie di difesa ritenute ormai deboli, caratterizzate da complessità di attuazione con conseguente inadeguatezza nel disporre in tempi brevi di strumenti efficaci. Un caso significativo è rappresentato dai paesi dell'area baltica¹⁶⁷ e scandinava¹⁶⁸ che col passare del tempo hanno adottato un nuovo concetto di difesa totale che coinvolge (seppure in parte) anche altri paesi non dell'Unione. Lo studio di tali approcci risulta ancor più interessante se correlato al fatto che mentre i paesi baltici indicati fanno parte della NATO, non così si può dire per i paesi scandinavi (Finlandia e Svezia) seppur rientranti in un'ottica di allargamento NATO già predisposta da molti anni. Questa rivisitazione del vecchio concetto di difesa totale, che include anche ambiti non solo prettamente militari ma soprattutto civili, rende l'idea di un approccio caratterizzato dalla combinazione di attività militari convenzionali e resilienza civile, completata da un quadro dove i settori pubblico e privato partecipano nell'architettura governativa con compiti singoli ma convergenti verso una difesa della sovranità nazionale. Nella sua prospettiva concettuale, la *Difesa Totale* comprende l'insieme delle attività indispensabili a una nazione e funzionali alla difesa della sua indipendenza, sovranità e integrità territoriale, dove convergono gli apparati di difesa civile e militare nonché le imprese private, le organizzazioni di volontariato e singoli individui.¹⁶⁹ La funzione sottesa a tale approccio è quella di mobilitare tutto il supporto necessario per difendere la nazione, compresa la cooperazione con altri

¹⁶⁷ Petroni F., "Il Baltico è un mare caldo", LIMES, 27/04/2018, <https://www.limesonline.com/cartaceo/il-baltico-e-un-mare-caldo>

¹⁶⁸ Totalförsvaret: la Difesa Svedese tra Minaccia Russa ed Adesione alla NATO, 23/02/2022, Mondo Internazionale, <https://mondointernazionale.org/focus-allegati/totalf%C3%B6rsvaret-la-difesa-svedese-tra-minaccia-russa-ed-adesione-alla-nato>

¹⁶⁹ Wither J.K., "Back to the Future ? – Nordic total defence concept", jan 2020, Defence Studies series, vol. 20, iussue 1, <https://doi.org/10.1080/14702436.2020.1718498>

Stati sul territorio nazionale in cui è essenziale disporre di una capacità di resistenza programmata e idonea a fronteggiare il nemico, dimostrando a quest'ultimo che un eventuale invasione e/o occupazione risulterebbe dispendiosa in termini materiali e morali, così da fungere anche quale deterrente. In questo quadro, riveste una certa importanza, il raggiungimento di una adeguata preparazione della popolazione, da eseguirsi in tempo di pace, al fine di contribuire alla resilienza nazionale durante una crisi o una guerra. Compito delle autorità militari e di protezione civile è quello di stabilire e mantenere la capacità di condurre attività di resistenza militare e civile, il tutto all'interno di un quadro giuridico e politico di indirizzo governativo. Dal 2014 in poi tale dottrina si è sempre basata sull'ipotesi di un attacco o di una occupazione da parte della Russia, di un paese baltico o scandinavo o comunque dell'area confinante. Nel corso di questi anni, ipotesi, test, studi ed esercitazioni sono stati condotti in quest'unica direzione, con la previsione di adottare un approccio asimmetrico per compensare le schiacciati capacità convenzionali russe e coinvolgere tutte le parti interessate in una strategia di difesa, elemento questo costituente un punto di partenza certamente positivo, seppure è nell'ottica di una seconda fase che esso risente di qualche imperfezione. La previsione di utilizzare le forze militari convenzionali esistenti nei paesi, come punto centrale e assegnare ad esse la parte più significativa nella difesa dell'integrità e della sovranità nazionale potrebbe costituire una criticità proprio sul piano pratico. Nel caso specifico, pur ammettendo che le capacità militari convenzionali degli stati baltici possano essere racchiuse in un'unica forza militare (nella migliore delle ipotesi, ovvero qualora si riuscisse con uno sforzo a dispiegarle congiuntamente), esse sarebbero comunque inferiori risultando quindi perdenti rispetto alle forze russe dispiegate e/o impiegabili nel settore geografico¹⁷⁰. A questa conclusione è giunto uno studio della Rand Corporation, pubblicato nel 2017,¹⁷¹ la cui previsione più nel dettaglio

¹⁷⁰ Currently, all Baltic armed forces combined comprise around 22,000 troops, with 448 heavy artillery pieces but no tanks or warplanes. The Russian conventional capability in the Western Military District alone is assessed at approximately 300,000 troops, while the total Russian conventional capability is estimated to be around 845,000 troops, 5,436 heavy artillery pieces, 2,550 tanks and 1,389 warplanes. <https://smallwarsjournal.com/jrnl/art/total-defense-how-the-baltic-states-are-integrating-citizenry-into-their-national-security>

¹⁷¹ Kepe M., Osburg J.: "Total Defense – How the Baltic States are Integrating Citizenry into their National Security Strategies", Rand Corporation, Small War Journals, sept. 2017

prevede anche che le forze russe, nel giro di pochi giorni, riescano a occupare e sconfiggere le forze armate baltiche, occupando una buona parte dei territori oggetto dell'invasione ma in virtù delle prospettive teorizzate dal concetto di difesa totale, si innescherebbe subito la fase della resistenza locale, nel corso della quale le forze armate residue e le reclute della società civile, inizierebbero ad organizzarsi per combattere la forza di occupazione russa fino all'arrivo degli aiuti internazionali. Una maggiore partecipazione civile alla difesa può essere promossa attraverso l'impegno con le organizzazioni sociali e professionali esistenti e con gli individui a tutti i livelli della società. La coscrizione, oltre al suo ruolo nel generare forze militari in servizio attivo, può essere considerata parte dell'impegno civile e dell'addestramento per la difesa. Aumenta le risorse umane disponibili per la mobilitazione, aumenta la preparazione generale alle situazioni di emergenza e può aumentare l'apprezzamento del proprio paese e delle sue forze armate. L'Estonia ha continuato la coscrizione dall'inizio del 1990 e la Lituania ha ripristinato una forma di coscrizione nel 2016, solo otto anni dopo che era stata abolita nel 2008. La coscrizione in Estonia ha una durata da 8 a 11 mesi e mira a fornire al coscritto le conoscenze necessarie per contribuire all'esercito in tempo di guerra. Allo stesso modo, la Lituania ha un programma di coscrizione della durata di nove mesi, con un'ampia percentuale dei circa 3.000 coscritti all'anno che partecipano al programma come volontari. La Lettonia è l'unico stato baltico che attualmente non ha alcuna forma di coscrizione poiché è stata sospesa nel 2006. Lo sviluppo più recente negli Stati baltici volto ad aumentare la capacità dei civili di rispondere alle crisi, proteggersi e aiutare a sostenere la difesa nazionale è lo sforzo del governo lettone verso la reintroduzione dei corsi di difesa nazionale e di protezione civile nelle scuole. Se implementata, questa iniziativa aumenterà la conoscenza della popolazione su come riconoscere le minacce e rispondere ad esse. Un tale impianto per essere funzionale ha però bisogno di esercitazioni che consentano di testare praticamente professionalità, procedure, metodologie che effettivamente ricalchino le situazioni emergenziali a cui si fa riferimento. In tale ambito nel 2015 si è svolta l'esercitazione "Siil" considerata come l'esercitazione più grande organizzata in Estonia in materia di difesa nazionale integrata, che ha coinvolto circa 13.000 riservisti, membri dell'organizzazione di volontari "Defence

League”, oltre che coscritti, militari professionisti e tecnici vari.¹⁷² Anche la Lituania nel 2017 ha svolto esercitazioni tra le forze armate e le truppe della riserva promuovendo la “Lightning Strike 2017”.¹⁷³ A fattor comune, in tutti gli stati baltici si sono svolti alcuni corsi di formazione ed esercitazioni per alti funzionari governativi, politici, rappresentanti di istituzioni educative, ONG e giornalisti, con l'obiettivo di informarli e formarli per varie situazioni di crisi civile. Tale formazione contribuisce anche a costruire le reti interpersonali e inter-organizzative necessarie per l'efficace attuazione di un sistema di difesa totale. Ciò significa dare a persone di diversa estrazione e reti professionali l'opportunità di connettersi tra loro e creare così reti sociali e di comunicazione sia formali che informali. Un esempio di tale formazione è il corso di difesa nazionale estone che si tiene dal 1999. Riunisce un'ampia varietà di partecipanti, tra cui politici estoni, militari, rappresentanti del governo e del governo locale, nonché individui che lavorano nel settore privato e nelle ONG. Nella sua parte conclusiva lo studio evidenzia che esistono indubbiamente delle differenze tra gli stati baltici che, tuttavia, possono essere superate da una serie dalle seguenti raccomandazioni, tendenti a rafforzare la difesa nazionale di tutti quei paesi che si trovano al confine orientale con l'alleanza:

- sostenere gli sforzi nazionali per educare i propri cittadini sulle questioni di sicurezza nazionale, aumentando così la loro disponibilità e interesse a partecipare. Facilitare discussioni aperte sulla difesa nazionale che coinvolgano il settore governativo, le forze armate, il settore privato, le ONG e i membri della società aumenterà la consapevolezza della difesa e della sicurezza tra il pubblico in generale;
- aumentare gli sforzi nazionali per educare i propri cittadini su cosa fare in tempo di crisi o di guerra, fornendo supporto a pubblicazioni, programmi televisivi e radiofonici che diffondono tali informazioni;
- fornire consulenza agli Stati baltici sulle migliori pratiche in merito a come aumentare la cooperazione inter-agenzia tra i loro ministeri della difesa e

¹⁷² “Siil Exercise success ends fully professional army debate: Estonia Defence Minister”. The Baltic Times 14.05.2015, https://www.baltictimes.com/success_of_siil_exercise_ends_debate_about_fully_professional_army_estonia_defence_minister/

¹⁷³ “Lithuanian Armed Forces closing Lightning Strike 2017 exercise”, https://www.army.mil/article/189507/exercise_saber_strike_17_culminates_in_latvia

della cooperazione delle forze armate e i loro ministeri dell'interno, delle ONG e della società in generale;

- partecipare alla progettazione e all'esecuzione di esercitazioni multilivello di difesa e resilienza che includano la partecipazione della società civile.

Si tratta di raccomandazioni in perfetta sintonia con le strategie NATO e rispondenti ai programmi divulgati in ambito di resilienza, preparazione civile, prontezza civile-militare, discussi durante il vertice NATO svoltosi a Varsavia nel 2016¹⁷⁴

3.5.2 Resistance Operating Concept

Sulla base delle esperienze ricavate dalle situazioni dei paesi baltici e analizzando diversi studi, esercitazioni e seminari dedicati, la maggior parte dei quali sviluppati in ambito NATO, lo Special Operations Command Europe statunitense¹⁷⁵ ha approntato un concetto operativo che, ovviamente, diventa parte integrante e pertanto recepito nei concetti strategici dei vari paesi europei. Si tratta del “Concetto Operativo di Resistenza” o Resistance Operating Concept (ROC). Sviluppato inizialmente in collaborazione con i paesi baltici e scandinavi, fonda i suoi presupposti sulle politiche governative tendenti a promuovere delle capacità in una fase che precede la crisi vera e propria e quindi in una condizione di parziale vantaggio. Nella sua formulazione, alla base del Concetto Operativo di Resistenza si hanno due principi cardine costituiti dalla resistenza e dalla resilienza. Nel primo caso si tratta di attuare una risposta considerata naturale da parte di un paese sovrano e della sua popolazione di fronte alla minaccia esterna.¹⁷⁶ La resilienza nel caso di specie è considerata quale volontà da parte della popolazione locale di mantenere ciò che ha, ovvero la capacità di resistere a pressioni e influenze esterne e reagire dallo sviluppo di tali effetti. Quest'ultimo aspetto è considerato una base fondamentale su cui cementare l'intero processo poiché è nella preparazione della popolazione a reagire ad una potenziale crisi che si innescano i

¹⁷⁴ Shea J., “Resilience: a core element of collective defence! – NATO Review, 30 mar. 2016, <https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html>

¹⁷⁵ “SOCEUR is an inclusive community, dedicated to a culture where all voices are heard, respected, and valued”, official site, <https://www.socom.mil/soceur>

¹⁷⁶ Fiala O. C., Pettersson, U. “ROC(K) Solid Preparedness: Resistance Operations Concept in the Shadow of Russia”, National Defense University Press, PRISM Vol. 8, No. 4, 11 June 2020.

meccanismi decisivi per la veicolazione dell'azione "resistenza" da parte del decisore politico.¹⁷⁷ Di particolare importanza la prima fase, nella quale andranno identificate le principali minacce e, conseguentemente, andranno predisposte le misure militari e civili idonee a contrastarle, avendo cura di rappresentare tramite un'efficace comunicazione, i principali rischi, affinché la popolazione ne sia (almeno in parte) consapevole. Tuttavia per mettere in atto una efficace operazione di questo tipo, occorre disporre di una serie di elementi indispensabili e strutturalmente predisposti che possono essere così riepilogati¹⁷⁸:

- *Identità Nazionale*; è alla base della resistenza nazionale deve esserci una decisa e concreta coesione nazionale che rafforzi la resilienza. La si ottiene con un'educazione anche di profilo storico in linea con i valori culturali e identitari anche tramite l'inclusione delle minoranze nella vita civile e governativa della nazione.
- *Identificazione delle Potenziali Minacce Esterne*; per mitigare i rischi e prepararsi alla resistenza occorre riconoscere e definire le minacce. Parimenti importante è un'adeguata comunicazione rivolta alla popolazione previa valutazione di quegli elementi che sono vulnerabili alle attività e all'influenza del nemico. La comunicazione va rivolta anche ad alleati, partner ed avversari, ricorrendo anche alla contropropaganda.
- *Conoscenza delle Vulnerabilità*; il decisore politico deve identificare e mitigare vulnerabilità e debolezze che un avversario può sfruttare a suo vantaggio.
- *Riduzione delle Vulnerabilità*; essa richiede il coinvolgimento totale del decisore e dell'intera società. È possibile attuare varie misure come: contrastare la narrazione avversaria; diversificare l'economia; proteggere industrie ed infrastrutture critiche; proteggere gli standard di vita; promuovere l'unità nazionale; attuare misure di protezione informatica.
- *Preparazione Psicologica*; va condotta con ampio anticipo rispetto ad un potenziale conflitto. Si tratta di un processo delicato e importante che prosegue anche in caso di conflitto, dato che la resistenza dovrà mantenere

¹⁷⁷ Friberg J., "SOCEUR and Resistance Operating Concept (ROC)", SOF News, 19 July 2019. <https://sof.news/uw/resistance-operating-concept/>

¹⁷⁸ Fiala O. C., "Resistance Operating Concept (ROC), The JSOU Press, MacDill Air Force Base, Florida, 2020.

il sostegno popolare, mantenendone il sostegno con un'adeguata e calibrata narrazione.

Il sistema risente tuttavia di un'altra condizione imprescindibile, cioè la volontà da parte di alleati (o comunque di entità statali e supporter economici) di contribuire a creare quel substrato indispensabile (forniture di armi e materiale tecnologicamente all'avanguardia, reti satellitari, capacità cyber e logistiche, invio di personale specializzato) che crei il substrato indispensabile ad una configurazione tale che la ROC possa essere talmente efficace da costituire, essa stessa, un deterrente per l'avversario da controllare anche attraverso un'efficace comunicazione strategica. Nella fase successiva quando l'aggressore ha già attuato l'occupazione o comunque iniziato una serie di operazioni anche di guerra convenzionale, viene data attuazione a tutte le ramificazioni predisposte: unità speciali, intelligence, comunicazioni, sabotaggi, attraverso un coordinamento unico nelle principali sedi preposte alla Difesa, responsabili del reclutamento del personale, da impiegare nelle figure chiave, della pianificazione, dello sviluppo delle linee d'azione e della valutazione e verifica del piano di resistenza. Il reclutamento per un'organizzazione di resistenza dovrebbe essere selettivo, ed il personale selezionato in base alle sue abilità e alla sua capacità di conformarsi al comportamento necessario per le operazioni speciali. ¹⁷⁹

3.5.3 l'intelligence tra vecchi e nuovi schemi

Quale che sia il processo argomentativo in materia di intelligence europeo non è possibile scinderlo da quello statunitense per una serie di considerazioni storiche, organizzative e geopolitiche in senso più ampio. È inevitabile infatti che nel corso della storia sia siano verificati eventi più o meno importanti (alcuni definiti epocali) che hanno inciso nella postura dell'intelligence USA determinando, a cascata, implicazioni e adattamenti anche all'intelligence dei paesi UE che comunque si muovono, generalmente, di concerto con essa, pur con i dovuti distinguo in materia di sovranità più o meno accentuata ma alla fine comunque condizionata dalla posizione egemonica di gran lunga superiore dettata dagli Stati Uniti. Lo

¹⁷⁹ Stejskal J. "Bear Trap: Building a Pre-Conflict Underground Force to Resist the Future Enemy", Journal on Baltic Security, vol.1, oct 2022,

scioglimento dell'URSS e del blocco sovietico ha rappresentato certamente una svolta epocale e da quel momento gli sforzi dell'intelligence si sono diretti su altro. Tuttavia l'evento dell'11 settembre 2001 è comunemente ritenuto quale vero "spartiacque" tra due epoche diverse, evento che ha radicalmente cambiato dottrine, concetti operativi e assetti istituzionali, evidenziando come dei nemici non tradizionali siano in grado di arrecare danni incalcolabili al nostro modo di vivere.¹⁸⁰ Anche in questo caso la riconfigurazione dell'intelligence si è spostata su nuovi target ma la novità si è registrata soprattutto in un'accettazione della regola "non regola" di operare in qualsiasi parte del mondo su presupposti che andavano in deroga a norme e diritti consuetudinari. Si è così assistito a uno stanziamento di fondi incredibilmente più ampio rispetto al passato, al reindirizzamento delle capacità di intelligence per affrontare quella nuova minaccia (alla quale sono immediatamente seguite senza soluzione di continuità, nuove/diverse minacce che inducono i decisori politici a governare con sistemi di tipo "emergenziale").¹⁸¹ Tutta la comunità di intelligence ha subito un radicale cambiamento e lo stesso personale ha dovuto adattarsi a scenari anche operativi diversi rispetto al passato. I nuovi processi di globalizzazione, pur non essendo classificati come fatto/evento al pari dell'11 settembre 2001, rappresentano tuttavia un altro passaggio epocale determinante un cambiamento. La globalizzazione infatti produce delle sfide alla sicurezza nazionale. Basti pensare alle campagne di propaganda per plasmare i sentimenti e capacità cognitive delle persone, allo stesso modo diventano incidenti in questo processo, le campagne di disinformazione predisposte da attori statali e non statali che promuovono obiettivi imprevisti sfruttando i canali di comunicazione sia tradizionali ma soprattutto i social. Nel rimarcare il legame intrinseco tra difesa e intelligence, che caratterizza l'intera impostazione di questa ricerca, va riconosciuto che la maggior parte dei processi di sviluppo e di ricerca delle forze armate di qualsiasi paese, soprattutto fatti nell'ottica di superare quelli avversari, passa inevitabilmente attraverso il supporto qualificato dell'intelligence. È noto infatti che per raggiungere una capacità militare di livello

¹⁸⁰ Sims J. E., "Decision Advantage and the Nature of Intelligence Analysis," Chapter 24 in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York: Oxford University Press, 2010),

¹⁸¹ Marshall C. Belasco E., A. "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service *Report for Members and Committees of Congress*, September 18, 2013,

elevato e competitivo, occorre avere un'idea delle capacità dell'avversario e, per ottenere questo, è indispensabile disporre di una intelligence che sia in grado di anticipare la dottrina e le intenzioni del paese straniero o del competitor, prevenire interventi tattici e operativi che potrebbero sfruttare l'effetto sorpresa e garantire che le proprie capacità non vengano compromesse prima di un loro effettivo utilizzo. Recenti analisi hanno evidenziato che Cina e Russia dispongono delle più efficaci ed emergenti tecnologie, che consentono loro potenzialmente di minare gli interessi USA e quelli occidentali. Per ottenere questo continuano a finanziare importanti progetti, con investimenti significativi nei settori dell'artificial intelligence (AI) e del machine learning (MI) per l'elaborazione e l'analisi di grandi quantità di dati. La Cina in particolare ha da tempo destinato molte risorse ai sistemi denominati "dual use" che consentono alle autorità di rintracciare i propri cittadini, sistemi che tuttavia che in ambito intelligence, possono servire ad acquisire notizie e dati degli avversari. Nel corso di questi anni i portavoce governativi avevano più volte annunciato che la Cina avrebbe investito un ammontare di circa 1,4 trilioni di dollari fino al 2025, chiedendo alle aziende del settore, di creare reti wireless basate sul sistema 5G, di installare telecamere e sensori e di sviluppare software di intelligenza artificiale finalizzati alla gestione autonoma delle fabbriche e alla sorveglianza di massa¹⁸². Nonostante le riforme intraprese dalla comunità di intelligence USA e dalle intelligence europee molti aspetti sono suscettibili di miglioramento. Tra i provvedimenti auspicati c'è quello relativo a una migliore collaborazione tra le diverse agenzie di intelligence al fine di oltrepassare una resistente barriera ideologica che impedisce una piena condivisione delle informazioni. La tematica è sempre in discussione all'interno della comunità di intelligence USA e se le resistenze sono così forti all'interno di diverse agenzie dello stesso paese, è facilmente intuibile come la cosa assuma un aspetto ancor più controverso quando si pensa a una *intelligence sharing* tra diversi paesi. Maggiore sforzo dovrà essere fatto per acquisire e migliorare il livello tecnologico; questo elemento pone anche un problema di mentalità poiché proprio per i motivi più volte accennati è indispensabile che tutta l'intelligence sia disposta ad accogliere soluzioni tecnologiche all'avanguardia, siano esse anche

¹⁸² Bloomberg News, "China's Got a New Plan to Overtake the U.S. in Tech," updated May 21, 2020, <https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech>

commerciali, modificandole, se necessario per soddisfare i propri requisiti. Una mentalità adeguata da parte della leadership dell'intelligence dovrà inoltre determinare un più proficuo spostamento di risorse e capacità nei citati settori dell'AI e del ML in risposta all'aumento della concorrenza costituita dai paesi avversari. Un progetto di ricerca predisposto dalla Oracle Corporation nel 2019 ha evidenziato che l'efficienza aziendale è suscettibile di un aumento del 64% quando la tecnologia giusta viene implementata, all'interno di una organizzazione, stante la presenza dei seguenti sette fattori culturali chiave¹⁸³:

- Flessibilità e accettazione del cambiamento,
- Cultura dell'apprendimento,
- Processo decisionale basato sui dati,
- Comunicazione aperta e collaborazione,
- Visione digitale condivisa e leadership partecipativa,
- Cultura imprenditoriale
- Pensiero critico.

Secondo la ricerca, molte organizzazioni hanno investito nelle giuste tecnologie ma mancano della cultura, delle competenze o dei comportamenti necessari per trarne appieno i benefici. Lo studio ha rilevato che l'efficienza aziendale aumenta solo del 27% quando la tecnologia viene implementata senza i sette fattori identificati. Operando una traslazione dei dati e dei contenuti della ricerca menzionata nel settore insito alla presente ricerca si può facilmente dedurre che l'anello di congiunzione con l'intelligence è costituito proprio da tale capacità "mentale" di adeguarsi e di modificare un approccio che non sembra essere, in alcuni casi, al passo con i tempi. Sul versante delle minacce alla sicurezza poste da Cina e Russia le strutture e il personale dell'intelligence USA ha certamente focalizzato le sue attenzioni ma probabilmente gli sforzi fatti finora si sono concentrati unicamente su due delle sette aree sopra indicate: pensiero critico e cultura dell'apprendimento. Esistono ancora molte ritrosie a intraprendere processi decisionali basati su dati acquisiti a tutti i livelli possibili ed avere così una visione digitale condivisa alla stregua di una cultura di tipo imprenditoriale. Altro aspetto imprescindibile è costituito dalla condivisione delle informazioni. Gestire

¹⁸³ Oracle Cloud, "Adaptable Businesses and the Productivity Paradox", in *The Adaptable Business: Future Skills and Cultural Forces*, 2019, <https://www.oracle.com/a/ocom/docs/dc/the-adaptable-business.pdf?elqTrackId=28c5abc9c44d4a5d872b2e6cd1a92c68&elqaid=79966&elqat=2>

tale processo in maniera efficace in un mondo particolarmente riservato qual è quello di interesse, resta impegnativo e causa della necessità di proteggere segreti essenziali in un'ottica di equilibrio tra la "necessità di condividere" e la "necessità di proteggere".¹⁸⁴ Nello stesso ambito va valutato l'incremento esponenziale dei dati in possesso. Gli analisti di intelligence oggi sono inondati da dati che non sempre riescono a processare in modo efficace, dati che spesso non riescono a scambiare tra loro o tra analisti e operatori e mondo militare. Ne consegue una situazione di criticità che rischia di interrompere interi processi di valutazioni e, conseguentemente anche decisionali. Esistono basi solide per il mondo dell'intelligence USA e per quelli dell'Unione europea. Tuttavia una mutazione o meglio un processo di adattamento ai tempi è reso obbligatorio dalle criticità enunciate. Aumento esponenziale nelle competenze linguistiche, perfezionamento delle attività operative, intelligence sharing, uso delle tecnologie emergenti, analisi dei dati, capacità operative cyber, devono diventare la norma per il raggiungimento del successo in un settore di vitale importanza. Tutto questo richiederà una leadership adeguata ma soprattutto una volontà politica che concordi in tale processo di adeguamento ritenuto da più parti inevitabile.¹⁸⁵ La leadership tuttavia è espressione del potere un potere che si sta dirigendo oggi verso una posizione elitaria e di dominio assoluto; fase questa particolarmente delicata e che presenta dei rischi nel momento in cui l'uso della Difesa e dell'Intelligence non sia più come storicamente conosciuto ma possa mutarsi in qualcosa di diverso a uso di mire egemoniche.

¹⁸⁴ Van Puyvelde D., Coulthart S., Shahriar H. M., "Beyond the Buzzword: Big Data and National Security Decision-Making," *International Affairs*, Vol. 93, No. 6 (November 2017),

¹⁸⁵ Shedd D. R., "Intelligence and National Defense," in *2016 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2015)

LE MISSIONI MILITARI NELL'AMBITO DELLA POLITICA DI SICUREZZA E DIFESA DELL'UNIONE EUROPEA: SVILUPPI E PROSPETTIVE

Intervista al Generale di Divisione Massimo MINGIARDI

Capo di Stato Maggiore del Comando per la Formazione, Specializzazione e Dottrina dell'Esercito COMFORDOT (già Mission Commander missione EUTM Somalia 2014/2015).

06 gennaio 2022

Domanda: Generale Mingiardi, lei è stato Mission Commander dell'operazione EUTM in Somalia, missione avviata dall'Unione Europea a partire dal 2010, in recepimento degli accordi Berlin Plus e nel contesto di una Strategia Europea di stabilizzazione del Corno d'Africa; qual è stato il bilancio della missione in quegli anni?

Risposta: Una risposta molto semplice e diretta potrebbe essere: un successo! Ciò è vero se paragono le condizioni generali dell'inizio del mio periodo di comando della missione con quello che ho lasciato. Basti solo pensare che fino a qualche giorno prima della mia assunzione del comando avvenuta in Mogadiscio, la missione era schierata in Uganda, in quanto la Somalia in generale e soprattutto Mogadiscio erano considerati il posto più insicuro al mondo. E a ragione! In poche parole mi trovai ad aprire una missione partendo quasi da zero. Con una struttura di comando da amalgamare e formata da Ufficiali e Sottufficiali provenienti da diversi paesi di Europa che mai avevano operato insieme. Per dare una idea il mio vice Comandante era un Colonnello svedese (Paese non NATO) e il mio Capo dello Staff un colonnello spagnolo (Paese NATO). Quindi dovetti implementare procedure e modalità di lavoro oltretutto verificare le condizioni di sicurezza per l'addestramento del ricostituendo Esercito Somalo, la nostra missione. Il tutto chiusi in un'area protetta e senza controllo dell'ambiente esterno dagli attacchi di Al Shabab l'equivalente dell'ISIS in Somalia. Insomma nonostante tutto questo da 0 siamo riusciti ad addestrare in un anno più di 2500 soldati somali. Quindi un grande successo!

Domanda: le prospettive strategiche dell'UE e della NATO devono necessariamente trovare dei punti in comune per una programmazione coerente e adeguata ai tempi; le missioni militari a guida UE potranno ancora rappresentare un ambito operativo esclusivo o pensa sia inevitabile un coinvolgimento dell'Alleanza Atlantica?

Risposta: La recente crisi in Ucraina, ma soprattutto il disastroso, affrettato e poco onorevole ritiro dall'Afghanistan hanno dimostrato la necessità di un credibile

strumento militare europeo integrato. Le dichiarazioni della Von der Leyen del 21 settembre scorso che preannunciavano la nascita di un esercito europeo di circa 6000 uomini in grado di poter operare in piena autonomia dalla NATO farebbero ben sperare. Però la mia esperienza di Comandante di Missione sotto egida europea che rispondeva direttamente al COPS non mi fa essere così ottimista. Ho sperimentato sulla mia pelle le rivalità, le divisioni e la necessità della unanimità per le più importanti decisioni che di fatto paralizzano la operatività di una missione europea. Questa incapacità di agire subito e tempestivamente a causa di anche piccolissime nazioni che bloccano l'operatività militare (a me ad esempio è capitato con Cipro), devono essere necessariamente superate se si vuole veramente agire nel mondo con la bandiera europea contro chi mette a repentaglio la sicurezza internazionale.

Domanda: la tecnologia ha già cambiato le prospettive e le modalità di combattimento tanto che si parla sempre più con insistenza di un approccio multi-dominio. Quali prospettive vede in tale ambito e in che modo dovrà essere strutturata una adeguata formazione?

Risposta: Le minacce attuali al nostro Paese sono sicuramente quelle dirette alla sicurezza cibernetica. Ne è riprova il fatto che anche in Italia, pur con ritardo, sono state realizzate strutture in grado di gestire il multi-dominio. Però io continuo a pensare che tale approccio non può prescindere dalla formazione basica e classica all'uso dei soli strumenti in grado di difenderci dalle minacce ibride che oggi sono le più attuali e concrete. Il recente passato ci ha dimostrato che un camion, mezzo che circola in centinaia di migliaia sulle nostre autostrade trasportando i beni primari e consentendo l'ordinata vita del nostro Paese, si può trasformare in maniera inaspettata in uno strumento di morte. O un uomo con in mano un coltello da cucina presente in tutte le nostre case, si può trasformare in un assassino spinto da ideologie religioso-estremiste. E allora? Va bene sviluppare strutture in grado di gestire le minacce provenienti dalla quarta dimensione, però mai dimenticare che l'uomo addestrato, ben equipaggiato e soprattutto motivato sarà sempre la migliore e più efficace difesa contro qualsiasi minaccia.

DIFESA E INTELLIGENCE NELL'UNIONE EUROPEA

**Intervista al S. E. Amb. Dott. Giampiero Massolo
già Direttore del Dipartimento delle Informazioni per la Sicurezza.**

13 settembre 2021

Domanda: Eccellenza, l'Unione Europea non ha una sua intelligence (così come tradizionalmente può essere intesa) ma dispone di tante e diverse piattaforme e centri settoriali. É ipotizzabile una struttura unica, organicamente predisposta? Oppure ritiene prevarranno le esigenze di sovranità dei paesi membri e, molto più pragmaticamente, ci si dovrà accontentare dell'architettura attuale.

Risposta: Se per intelligence europea intendiamo una struttura unica nel suo complesso e che risponda alle esigenze di tutti i Paesi membri penso che occorrerà aspettare ancora a lungo, se mai ci si arriverà. La ricerca attuale di intelligence è inestricabilmente legata alle rispettive esigenze nazionali. L'Europa, almeno per il momento, sembra aver perso di vista il progetto unitario prospettato in origine. Non può sfuggire, ad una attenta visione critica, che attualmente ci troviamo di fronte ad un assetto più compatibile con quello di una Confederazione, rispetto a una Europa unica, sotto il profilo delle varie politiche e soprattutto sotto quello culturale. In tale senso è possibile affermare che un "interesse europeo" al momento è un concetto molto vago. Se invece intendiamo un approccio comune su tematiche comuni e mi riferisco al "data sharing" (nell'accezione più ampia del termine) allora va sottolineato che molti progressi sono stati fatti in questo campo. Gli esempi più evidenti sono gli scambi di dati relativi alle tematiche sul terrorismo di matrice jihadista; si tratta di un intento condiviso, sviluppato su comuni accordi e con risultati positivi ma che certamente è suscettibile di implementazione.

Domanda: É indubbio che "le intelligence nazionali", quando anche riescano ad operare in un ambito per così dire comunitario, continuino comunque a mantenere ben presenti i propri interessi di parte anche a discapito dei cd partner; fino a che punto i Paesi con più peso e prospettive strategiche hanno l'interesse a porsi sullo stesso piano di altri la cui rilevanza strategica è minima, condividendo prodotti di intelligence?

Risposta: La collaborazione tra le intelligence dei vari Paesi esiste e, nella sua complessità, non si può dire che proceda "de plano", non tanto per il diverso peso del singolo o della sua prospettiva strategica. Vi è alla base uno dei tanti criteri che contraddistinguono il rapporto tra le intelligence, che è quello legato al principio del "do ut des". Più nello specifico si tratta della qualità e della quantità di

intelligence che si può offrire in un determinato momento e in determinato ambito (o anche relativamente a una determinata area geografica). L'abilità sta soprattutto nel poter offrire dei prodotti di intelligence in un momento in cui c'è urgente richiesta, meglio ancora se quei prodotti possono essere offerti con caratteristiche di esclusiva. Tornando alla domanda occorre tenere presente le numerose difficoltà che ci sono tra i Paesi membri derivanti da differenze nella tradizione, nella cultura, nella legittimazione degli apparati di intelligence, ma anche delle differenze tra procedure standardizzate, individuazione dei fabbisogni, accettazione di minacce condivise e cultura della sicurezza, aspetto quest'ultimo sul quale è assolutamente indispensabile procedere attraverso una adeguata comunicazione, elemento chiave che può davvero contribuire a superare molti degli ostacoli appena evidenziati.

Domanda: oggi si parla, con eccessivo slancio, di autonomia strategica dell'UE e si tende a dimenticare oggettive risultanze storiche in virtù delle quali, questa UE, esiste perché così decisero gli Stati Uniti, all'indomani della seconda guerra mondiale stabilendo, per il vecchio continente, anche l'attuale architettura di politica e di difesa. Lei ritiene che questi presupposti siano sufficienti ad accantonare idee quali esercito europeo, ambizioni strategiche europee e intelligence europea?

Risposta: Se per autonomia strategica pensiamo a una Unione Europea che possa fare da sola senza poter contare sull'appoggio degli Stati Uniti è evidente che la risposta non può che essere negativa. Questa impossibilità è legata a una mancanza di identità europea, una mancanza di politica estera comune e a diversi e importanti fattori. Quello che è possibile ipotizzare, in quanto più praticabile è invece un aumento delle capacità militari e tecnologiche che consentano all'Europa di agire con più forza in limitati spazi e ambiti, con maggiore autorità. Il legame con l'Alleanza Atlantica e con gli USA è chiaramente indissolubile e difficilmente si può fare a meno di esso. Tuttavia i fattori appena citati, ovvero quelli dello sviluppo e implementazione di capacità militari e tecnologiche, consentirebbero all'Unione di porsi con maggiore forza sulla ribalta internazionale e laddove possibile con una autonomia maggiore, rispetto al passato, seppur relativa.

Domanda: pluralità delle minacce, economie globali, caos multipolari. Lei ritiene che oggi l'intelligence sia ancora in grado di riconoscere con facilità "il nemico" e quale potrebbe essere l'approccio più idoneo per affrontare il futuro che in realtà è già adesso?

Risposta: l'11 settembre 2001 ha plasticamente dimostrato la mutazione del concetto di "nemico" e dei canoni tradizionali a cui tutti eravamo abituati. Oggi ci troviamo di fronte a una profusione di minacce, siano esse asimmetriche o afferenti il dominio cyber; spesso c'è una sostanziale difficoltà ad attribuire la paternità di una azione ostile e altrettanto difficile può essere individuarne la provenienza. Se a questi fattori includiamo le possibilità che tali azioni possano

avvenire sfruttando tecnologie emergenti, e mi riferisco all’A.I. o a uno dei suoi sottoinsiemi costituito dal “machine learning”, allora è evidente che le difficoltà aumentano in maniera esponenziale. L’intelligence oggi si adegua alle minacce emergenti. Deve quindi evolversi al pari di esse e sviluppare idonee capacità di discernimento in tutti i settori di interesse specifico e, quindi, verso il dominio cyber ma anche verso lo sviluppo delle nuove tecnologie e, non ultimo, verso una dimensione economico-finanziaria la cui strategicità è spesso sottovalutata. In tal senso l’intelligence ha in sé due vantaggi: il primo è legato al fatto che riesce a muoversi entro perimetri giuridici caratterizzati da una intrinseca flessibilità pur restando legata a essi; il secondo è quello generato dalla possibilità di far coagulare al meglio l’analisi di fonti aperte e di quelle chiuse. É inevitabile che in questa fase occorra puntare al reclutamento di nuove professionalità che siano ampiamente inserite nel contesto di rinnovamento sociale e tecnologico appena descritto ma che, parallelamente, sappiano dare ancora valenza al fattore umano, importantissimo e imprescindibile in ogni processo di valutazione senza il quale la pur ampia valenza delle più moderne tecnologie risulterebbe non completa. Vale la pena ricordare infatti che “l’intuito non è rimpiazzabile”.

**POLITICHE DI SICUREZZA E DIFESA COMUNI E RELAZIONI INTERNAZIONALI:
QUALI PROSPETTIVE**

Intervista al Prof. Cesare La Mantia

Professore associato presso l'Università degli Studi di Trieste; docente Storia dell'Europa orientale nel corso di Scienze Internazionali e Diplomatiche (SP01) e Storia della politica estera russa contemporanea nel corso magistrale di Diplomazia e Cooperazione Internazionale (SP54).

25 ottobre 2022

Domanda: Professor La Mantia, L'Unione Europea sembra essere indirizzata verso una Politica di Sicurezza e Difesa Comune, caratterizzata da maggiore impegno, soprattutto economico, inclusione di nuovi partner e proiezioni esterne non immaginabili fino a qualche anno fa. Ritiene lei che tale scelta sia frutto di una ponderata riflessione interna tendente a una crescita e a una consapevole rimodulazione della PSDC?

Risposta: Il dibattito è in corso ormai da diverso tempo ed è fortemente condizionato da due attori esterni all'Unione le cui azioni sembrerebbero spingere verso la creazione di un modello di politica di sicurezza e difesa comune. È l'esistenza della pressione statunitense e dell'aggressione russa all'Ucraina che stanno determinando pur tra numerose difficoltà una risposta quasi unitaria che potrebbe favorire la nascita del modello prima indicato. Nascita che comporterebbe necessariamente una ulteriore riduzione di sovranità per gli stati membri ai quali non solo gli stati c.d. sovranisti non sembrano essere propensi. Gli Stati Uniti sono molto favorevoli all'assunzione di maggior oneri per la propria difesa da parte degli stati europei e con questa volontà l'Unione dovrà fare i conti; così come dovrà valutare come non sempre gli interessi europei collimino con quelli statunitensi.

Domanda: Il rapporto tra NATO e UE prosegue con sempre maggiore incisività, specie negli ultimi tempi seppure le scelte strategiche, l'autonomia e la capacità gestionali e decisionali siano prioritariamente dettate dall'Alleanza Atlantica. Quali pensa possano essere i margini per l'Europa, di avere un ruolo quale attore credibile nel panorama internazionale?

Risposta: I margini sono molto ristretti e allargarli è faccenda molto delicata, poiché l'allargamento di essi potrebbe comportare l'erosione del rapporto con gli Stati Uniti. Non dimentichiamo, inoltre, che i membri dell'Unione a volte si muovono in ordine sparso nelle relazioni con Washington.

Domanda: Minacce ibride e guerra cognitiva sono alcune tra le recenti forme di conflitto che si intersecano con i fenomeni più tradizionali. La soglia della “grey zone” tra periodo di pace e periodo di guerra tende ad assottigliarsi sempre più. In alcuni casi, i conflitti sono persistenti seppure con diverse intensità. Questi scenari attuali si protrarranno senza una fine o possono essere suscettibili di uno stop dettato dalla consapevolezza di una direzione estremamente pericolosa

Risposta: Uno storico non fa previsioni, meno che mai se riguardano l’assunzione di consapevolezza di appartenenti al genere umano. Durante la “guerra fredda” l’equilibrio del terrore mantenne lo scontro tra le due super potenze e i rispettivi alleati lontano dall’Europa e dal confronto diretto; ma non lo eliminò, lo esportò in altre parti del mondo mantenendolo a un livello inferiore rispetto al conflitto diretto e probabilmente definitivo. Le nuove tipologie di guerra più che rafforzare il muro di separazione da una guerra totale tendono ad eroderlo. Entrambe le guerre mondiali diedero vita a nuovi ordini internazionali. Perché quella in corso dovrebbe essere diversa?

Domanda: Parliamo di futuro: come pensa si evolveranno le relazioni internazionali? Quale potrebbe essere il focus delle stesse per adattarsi a un mondo proiettato a una realtà finora inimmaginabile?

Risposta: Non so come si evolveranno, so che utopisticamente sarebbe necessaria una condivisione delle risorse, una profonda riforma dell’ONU e una o più dottrine o ideologie che andassero in tal direzione.

CONCLUSIONI

I contenuti della presente ricerca presentano un dato incontrovertibile: la Difesa Comune è auspicata dalla maggior parte dei paesi membri. Emerge nelle dichiarazioni ufficiali, nel corso di incontri bilaterali o multilaterali, nei progetti e negli studi commissionati e infine dall'impellente richiesta a margine di situazioni di crisi, sempre più frequenti. È pur vero che a volte si parla di Difesa Comune, altre volte di esercito comune, altre ancora di asset comuni propedeutici. Queste differenze tecniche, di non poco valore, introducono alcune delle tante divergenze esistenti. L'evoluzione delle politiche di Difesa ha certamente contribuito a stratificare almeno "concettualmente" questo ambito ma resta da fare tanto e soprattutto occorre superare le perplessità e le divergenze ideologiche in tale settore. Germania, Francia e Italia potrebbero costituire un nucleo certamente in linea con la maggior parte dei dossier che riguardano la tematica esposta, seppure sussistono forti divergenze su obiettivi di politica estera e di economia, tali che in certe situazioni i citati partner assumono il ruolo di competitor con "azioni" ai limiti della diplomazia. Se spostiamo la prospettiva a Polonia, Romania e Repubblica Ceca ad esempio, è possibile notare un atteggiamento diverso, stante le prospettive, le diverse ragioni storiche e, non ultimo, le decisioni prese nei loro confronti dagli USA che, con l'installazione di basi missilistiche e interi asset di Difesa, ne condizionano le decisioni. Altra visione avranno i paesi baltici. Il loro ingresso in entrambe le strutture di partenariato (NATO prima e Unione Europea dopo) ha determinato una diversificata analisi delle loro richieste e delle esigenze di difesa e, ovviamente, la propensione per lo scudo difensivo dell'Alleanza Atlantica ha prevalso per una serie ovvia di ragioni: interesse primario USA a una presenza più avanzata e migliori garanzie di difesa a fronte di budget e investimenti minimi da parte dei tre paesi. Attualmente ognuno questi ultimi dispone di un centro di eccellenza NATO; nel 2008 è stato creato in Estonia il Centro di eccellenza per la difesa informatica (CCD NATO CoE), nel 2012 il Centro di eccellenza per la sicurezza energetica in Lituania (NATO ENSEC CoE), mentre in Lettonia è stato istituito il Centro di eccellenza per le comunicazioni strategiche (NATO Stracom CoE) nel 2014. Nel 2017, infine, in risposta alle operazioni russe in Crimea e nel Donbass, la NATO ha creato una presenza costante (Enhanced

Forward Presence, eFP) che comprende quattro battaglioni tattici multinazionali che ruotano tra Estonia, Lettonia, Lituania e Polonia, a presidiare il cosiddetto fianco orientale dell'Alleanza, quello che corre dal Mar Baltico al Mar Nero e che si trova dunque più esposto ad eventuali attacchi. Tutte e tre le repubbliche baltiche spendono oggi per il bilancio della difesa tra il 2,1% e il 2,3% del proprio Pil, eccedendo dunque l'obiettivo NATO del 2%. Svezia e Finlandia rappresentano anche loro un "unicum" dal momento che pur appartenendo all'Unione europea, al momento non fanno parte della NATO ma rientrano nelle ipotesi di allargamento per evidenti interessi strategici. La loro tradizione di neutralità è stata superata da contesti geopolitici in evoluzioni e l'interesse occidentale nei loro confronti è risultato evidente dal momento che entrambi fanno parte del circuito PARP (PfP Planning and Review Process), un programma NATO che li assiste nella transizione militare e nella modernizzazione del settore della difesa, pur essendo ufficialmente fuori dall'Alleanza. La Difesa Comune è un'ideale, a volte vicino a concretizzarsi, altre volte sempre più distante. L'adozione dello "Strategic Compass" può essere funzionale alla definizione di nuovi rapporti tra UE e NATO, atteso che da qualche anno ci si sta muovendo in tal senso, ovvero nell'identificazione della NATO quale struttura unitaria e convergente della Difesa, mettendo a disposizione di essa: battlegroup, forze di intervento, forze di proiezione o qualsiasi denominazione vorrà essere data a un esercito eterogeneo e multiforme. Tuttavia, ad oggi, le possibilità di dare vita a una struttura militare autonoma europea, possono essere racchiuse in tre ipotesi. La prima potrebbe essere la trasformazione permanente degli attuali assetti militari (in termini di risorse umane, economiche e strutturali) impegnati nelle diverse missioni civili e militari in vari teatri esteri; impegno non certo facile poiché anche sotto il profilo giuridico, oltre che politico, ognuna di esse nasce e si sviluppa in un contesto di esigenza/emergenza ben individuato e con regola di ingaggio diverse da teatro a teatro, con coinvolgimento, mission e durata variabile. La seconda ipotesi potrebbe basarsi su una vecchia proposta tedesca ovvero di costituire un primo nucleo di esercito europeo in aggiunta ai singoli eserciti nazionali. La terza ipotesi che appare, solo in parte, più realistica, prevede una trasformazione dell'attuale "Eurocorps", quale 28° esercito dell'Unione. Si tratta di una struttura già esistente nata a margine di un accordo del 1992 tra cinque paesi (Belgio, Francia, Germania,

Lussemburgo e Spagna) e dal 2002, ristrutturata a livello di Corpo d'Armata di "reazione rapida" a seguito di decisione e raccordo con il SACEUR NATO e, in quanto tale subordinata al Comando Supremo delle Potenze Alleate in Europa. Si tratta tuttavia di un Corpo d'Armata che vede un nucleo di paesi che ne fanno parte attiva e altri in qualità di osservatori e/o membri associati, con partecipazione di ufficiali di collegamento di paesi terzi quali Grecia, Turchia, Polonia e Canada, poi allargatisi anche a Gran Bretagna, Paesi Bassi, Austria e Finlandia. Anche in questo caso, perplessità di parte (la Francia ad esempio ostacola il rafforzamento del *Military Planning and Conduct Capability*, una sorta di Stato maggiore europeo in embrione legato al potenziamento del citato Eurocorps), rendono difficile qualsiasi azione definitiva. Fino a qualche anno fa ci si nascondeva dietro una storica ritrosia a creare un esercito comune operata principalmente dalla Gran Bretagna, peraltro uno dei maggiori contribuenti alle spese della Difesa UE; adesso emergono (o sarebbe opportuno dire riemergono) incertezze e diffidenze francesi e tedesche. Spostando l'obiettivo sull'idea di costruire un'intelligence comune la ricerca evidenzia le perenni difficoltà riscontrate forse in maniera più marcata rispetto alla Difesa. Sono ancora troppi gli ostacoli da superare in prospettiva. L'attuale IntCen è espressione diretta dell'Alto Rappresentante per la politica estera e di sicurezza ma non opera alla stregua di un servizio di intelligence tradizionale, dove per "intelligence" si intende per l'appunto, la struttura di per sé più specificamente nazionale, dove si intersecano controllo, elaborazione strategica e informazioni riservate, intimamente legate alla sicurezza del proprio paese, ivi comprese le attività di monitoraggio (e non solo) nei confronti degli stessi paesi alleati. Storicamente, anche nei momenti più critici in occasioni di conflitti tradizionali o asimmetrici, sono state riscontrate alleanze o partenariati tra intelligence, funzionali al raggiungimento di uno o più obiettivi. Non vi è traccia invece di coesione tra due o più intelligence sia essa strutturale e/o funzionale. Le varie strutture esaminate, siano esse prettamente nazionali o quelle internazionali alla stregua del Club di Berna o dei Five Eyes, fondano la loro attività su un fitto scambio di informazioni pur mantenendo assoluta autonomia nella composizione e mission delle proprie strutture di intelligence. I motivi ostativi sono davvero tanti. Superare diffidenze non solo di indirizzo politico ma anche essenzialmente di tipo organizzativo. A ciò

vanno aggiunte le differenze storiche; ogni agenzia ha una sua storia e ha ripartito compiti e organizzazione secondo profili diversi da paese a paese, con incidenze in aree geografiche di interesse variabili. Non si può certamente nascondere che spesso alla presunta cooperazione si opta per la competizione tra agenzie di paesi anche alleati e, storicamente, gli scontri non sono mai stati facili da gestire. Appare invece molto più realistico lavorare in maniera decisa al fine di stabilire delle sfere di interesse comuni, nei settori e relativamente ai dossier critici più impellenti e indirizzare i propri sforzi, attraverso la definizione di protocolli di intesa, vertici e spazi di confronti che tengano conto delle esigenze di tutti e non solo dei Paesi costituenti il nocciolo duro dell'Unione. Nel momento in cui la presente ricerca volge al termine (quantunque, in astratto una ricerca non è mai destinata a concludersi ma al contrario a essere rivista, integrata e indagata in nuovi e diversi aspetti), dei fatti epocali stanno riscrivendo i rapporti di forza internazionali. Dopo ogni conflitto mondiale (e questo in atto, per diversi aspetti lo è, non fosse altro per la moltitudine di attori statali e non, che partecipano attivamente con forniture di armi, equipaggiamento, forze armate, contractor, tecnologie spaziali e satellitari, expertise nei settori cyber e della guerra cognitiva, tecnologia IA e ML) sono sorti nuovi e diversi ordini internazionali. È verosimile che lo stesso accada al termine di questo conflitto che parte da lontano e che da lontano ha visto muoversi esigenze (spinte endogene ed esogene) per ristabilire un ordine, da una situazione di caos non solo organizzativo, ma anche concettuale (da molti definito disordine mondiale). Ma i paragoni col passato si rendono superflui con lo sviluppo recente delle relazioni internazionali. Qualcosa di più complesso e non facilmente catalogabile con gli schemi tradizionali è in corso e, come affermato in premessa, la decrittazione del presente potrà avvenire in un futuro, magari a breve termine, purché vi sia ancora (e la cosa non deve mai essere data per scontato), la possibilità di esercitare quello spirito critico indispensabile per vivere in un mondo libero. Un'eventuale assenza di tale possibilità, costituirà una condizione esiziale di non facile risoluzione.

Bibliografia

AA.VV.: *“Historikerkommission zur Erforschung der Geschichte des Bundesnachrichtendienstes 1945–1968”*, Band 9. 1. Auflage. Ch. Links Verlag, Berlin 2018, ISBN 978-3-96289-022-3

AA.VV.: *“Lithuanian Armed Forces closing Lightning Strike 2017 exercise”*, https://www.army.mil/article/189507/exercise_saber_strike_17_culminates_in_latvia

AA.VV.: *“Ministère des Affaires étrangères (1732-1998). Ministère des Affaires étrangères – Traités et Conventions. Traité entre la Belgique, la France, le Luxembourg, les Pays-bas et le Royaume Uni de Grande-Bretagne et d’Irlande du Nord”*, Bruxelles, AE TC 365

AA.VV.: *“Siil Exercise success ends fully professional army debate: Estonia Defence Minister”*. The Baltic Times 14 may 2015, https://www.baltictimes.com/success_of_siil_exercise_ends_debate_about_full_y_professional_army__estonia_defence_minister

AA.VV.: *“The EU Strategic Compass: A Blueprint for a European Defensive and Securitization Policy”*, IAI, Istituto Affari Internazionali, joint papers, <https://www.iai.it/en/pubblicazioni/eu-strategic-compass-blueprint-european-defensive-and-securitisation-policy>

AA.VV.: *“Unione de l’Europe occidentale (06.10.2000)”*. <http://www.weu.int/index.html>. Archives nationales du Luxembourg, Luxembourg. <http://anlux.lu/>.

Breccia G.: *“Corea, la guerra dimenticata”* – Il Mulino – 2019 ISBN-13: 978-8815280145

Bloomberg News, *“China’s Got a New Plan to Overtake the U.S. in Tech,”* updated 21 may, 2020, <https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech>

Canali L. *“L’interesse cinese a connettere Pakistan, Africa orientale e Europa”*. 14 agosto 2019, Limes, <https://www.limesonline.com/carta-cavi-sottomarini-internet-come-armi-il-progetto-peace-di-hauwei/114005>

Council of Europe: *“Information Disorder. Toward an interdisciplinary framework for research and policy making”*. Report, 2017, <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>

Council of Europe: *“Headline Goal 2010, Council of the European Union”*, november 2007, http://www.consilium.europa.eu/uedocs/cmsUpload/MilitaryCapabilitiesFC06backgroundNov06_en.pdf

Darnis J.P.: *"The European Union between strategic autonomy and technological sovereignty: impasses and opportunities"*, in Recherches & Documents - Fondation pour la recherche stratégique - N°10/2021 - April 2021

Darnis J.P.: *"Il Trattato del Quirinale può rilanciare l'Italia in Europa"* – LUISS School of Government – Policy Brief 39/2021

De Gasperi A.: *"Scritti e discorsi di politica internazionale e Antologia degli scritti"* su "L'illustrazione Vaticana" (1933-1938) e di discorsi all'estero (1945-1954). http://www.cvce.eu/obj/discorso_di_alcide_de_gasperi_strasburgo_10_dicembre_1951-it-7dbeb557-c313-4703-a237-d909f35a2c25.html

De Gennaro P.: *"The Gray Zone and Intelligence Preparation of the Battle Space"*, august 2016, <https://smallwarsjournal.com/jrnl/art/the-gray-zone-and-intelligence-preparation-of-the-battle-space>

Department of States – Office of Historian: *"Foreign Relations of the United States – 1981–1988"*, volume IV – Soviet Union, January 1983 – March 1985. <https://history.state.gov/historicaldocuments/frus1981-88v04>

European Parliament Report On The Role Of Nato In The Security Architecture Of The Eu 2008/2197, INI, 28 January 2009

Extract from the Declaration of the Helsinki European Council <https://publications.parliament.uk/pa/cm199900/cmselect/cmdfence/264/26425.htm>

Fägersten B.: *"Sharing Secrets: Explaining International Intelligence Cooperation"*, Lund Political Studies, 2010

Fiala O. C., Pettersson, U. *"Resistance Operations Concept in the Shadow of Russia"*, National Defense University Press, PRISM Vol. 8, No. 4, 11 June 2020

Fiala O. C., *"Resistance Operating Concept (ROC)"*, The JSOU Press, MacDill Air Force Base, Florida, 2020

Friberg J., *"SOCEUR and Resistance Operating Concept (ROC)"*, SOF News, 19 July 2019. <https://sof.news/uw/resistance-operating-concept/>

Gaub F. *"Enhancing early warning and preparedness" in Crisis Rooms: Towards a global network?*, eds. Patryk Pawlak and Andrea Ricci, Paris: European Union Institute for Security Studies, 2014

Girven R., Beaghley S., Weinbaum C., *"A New Paradigm for Secrecy"*, *US News & World Report*, 13 ottobre 2015, www.usnews.com/opinion/blogs/world-report/2015/10/13/definire-un-nuovo-paradigma-per-il-segreto-di-governo

Greenemeier L.: *"AI versus AI: Self-Taught AlphaGo Zero Vanquishes Its Predecessor"*, *Scientific American*, 18 ottobre 2017, www.scientificamerican.com/article/ai-versus-ai-self-taught-alphago-zero-vince-il-suo-predecessore/

Grossman, D. : *“Keeping Up with the Policymakers: The Unclassified Tearline,” War on the Rocks* , 28 luglio 2016, <https://warontherocks.com/2016/07/keeping-up-with-the-policymakers-la-linea-di-lacrima-non-classificata>

Hicks K.: *“By Other Means Part I: Campaigning in the Gray Zone”*, Washington DC, July 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf;

Hoffmann F.G.: *“Conflict in 21st Century: The Rise of Hybrid Wars”*, Potomac Institute for Policy Studies, Aarlington, Virginia, December 2007

Holst A., *“Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025,”* Statista, June 2021, <https://www.statista.com/statistics/871513/worldwide-datacreated/>

Horowitz M.: *Keeping Score: A New Approach to Geopolitical Forecasting*, University of Pennsylvania, February 2021, <https://global.upenn.edu/sites/default/files/perry-world-house/Keeping%20Score%20Forecasting%20White%20Paper.pdf>

Kania E. B., *“Artificial Intelligence and Chinese Power,”* Foreign Affairs, 5 december 2017, www.foreignaffairs.com/articles/china/2017-12-05/artificial-intelligence-and-chinese-power

Katz B., *“The Analytica Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis,”* CSIS, *CSIS Briefs*, October 2020, <https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologiestransform-intelligence-analysis>

Kepe M., Osburg J.: *“Total Defense – How the Baltic States are Integrating Citinzery into their National Security Strategies”*, Rand Corporation, Small War Journals, sept. 2017

Knoll D., *“Story Telling and Strategy: How Narrative is Central to Gray Zone Warfare,”* Modern War Institute at West Point, August 24, 2021, <https://mwi.usma.edu/story-telling-and-strategy-hownarrative-is-central-to-gray-zone-warfare/>

Korskich F. W.: *NATO Gets better Intelligence New Challenges Require New Answers to Satisfy Intelligence Needs for Headquarters and Deployed/Employed Forces* - Institut für Außen- und Sicherheitspolitik - Center for Foreign and Defense Policy – Vienna, April 2010.

Jervis R.: *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* , Ithaca, NY: Cornell University Press, February 2010

Jordan J.: *“International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,”* Journal of Strategic Security 14, no. 1, November 2020, doi:10.5038/1944-0472.14.1.1836.

Lamberth M., Rasser M.: *“A Solid Plan to Compete with China in Artificial Intelligence”*, in *Defense One*, 1 mar. 2021,

<https://www.defenseone.com/ideas/2021/03/solid-plan-compete-china-artificial-intelligence/172360>

Lesti S.: *"Totalförsvaret: la Difesa Svedese tra Minaccia Russa ed Adesione alla NATO"*, Mondo Internazionale, 23 feb. 2022, <https://mondointernazionale.org/focus-allegati/totalf%C3%B6rsvaret-la-difesa-svedese-tra-minaccia-russa-ed-adesione-alla-nato>

Liulevicius V. : *The World Before the Treaty of Westphalia*, *The Great Courses Daily*, University of Tennessee, Knoxville July, 12, 2020, <https://www.thegreatcoursesdaily.com/the-world-before-the-treaty-of-westphalia/>

Lledo-Ferrer Y., Dietrich J.H.: *"Building a European Intelligence Community"* International Journal of Intelligence and Counterintelligence 33, no. 3, 2020: 440-451

Lucania P.: *"Guerra cognitiva e dominio umano"*, in Brainfactor, 2022, <https://www.brainfactor.it/guerra-cognitiva-e-dominio-umano/>

Lucania P.: *"La sicurezza nella cyber dimension"*, con M. Farina, codice ISBN 978-88-6959-546-2, Key Editore, luglio 2016

Lucania P.: *"Le prospettive strategiche e le piattaforme per la condivisione dell'Intelligence in Europa"*, in Brainfactor, 2020, <https://www.brainfactor.it/le-prospettive-strategiche-e-le-piattaforme-per-la-condivisione-dellintelligence-in-europa/>

Lucania P.: *"Le neurotecnologie nel futuro del settore della Difesa"*, in Brainfactor, 2020, <https://www.brainfactor.it/le-neurotecnologie-nel-futuro-del-settore-difesa/>

Lucania P.: *"L'attualità della Political Warfare"* in Brainfactor, 2021, <https://www.brainfactor.it/lattualita-della-political-warfare/>

Lucania P.: *"Minacce ibride: il ruolo dell'Europa e della NATO"*, in Brainfactor, 2020, <https://www.brainfactor.it/minacce-ibride-il-ruolo-delleuropa-e-della-nato/>

Lucania P.: *"PsyOp: operazioni psicologiche, evoluzione e prospettive"* in Brainfactor, 2021, <https://www.brainfactor.it/psyop-operazioni-psicologiche-evoluzioni-e-prospettive/>

Lucania P.: *"The Use of Artificial Intelligence to Combating Disinformation"*, in Beyond Fake News – Governments, Press and Disinformation through International History, Franco Angeli Editore, EAN-9788835121794 ISBN-8835121795, pagg. 145-162 – dicembre 2021)

Marshall C., Belasco E., *"Intelligence Spending and Appropriations: Issues for Congress,"* Congressional Research Service Report for Members and Committees of Congress, September 18, 2013

Massolo G. *“Italia-Francia: un messaggio per Bruxelles”*, ISPI online, novembre 2021 <https://www.ispionline.it/it/pubblicazione/italia-francia-un-messaggio-bruxelles-32470>

Mazarr M.: *Mastering the Grey Zone: Understanding a Changing Era of Conflict* (Carlisle Barracks, PA: United States Army War College Press, December 2015), 39, <https://publications.armywarcollege.edu/pubs/2372.pdf#page=39>

McHenry, J.: *“Three IARPA forecasting efforts: ICPM, HFC, and the Geopolitical Forecasting Challenge,”* presentation, Federal Foresight Community of Interest 18th Quarterly Meeting, January 26, 2018, https://www.ffcoi.org/wp-content/uploads/2019/03/Three-IARPA-Forecasting-Efforts-ICPM-HFC-and-the-Geopolitical-Forecasting-Challenge_Jan-2018.pdf

National Archives: *“Records of International Conferences, Record Group 43, Jessup-Malik Agreement, May 1943, box 304, Jessup-Malik Conversations”*, March, April, May 1949 <https://nsarchive.gwu.edu/document/17547-document-02-henry-byroade-acting-deputy-director>.

National Archives: *“RG 59, Conference Files, box 56, CF 359 Secretary's Trip to Bonn-London”*, Sept. 15-18, 1954, also published in *Foreign Relations of the United States 1952-1954 Volume 5 Part II Western European* Washington, D.C., 1983

National Archives: *“RG 59, Conference Files, box 56, CF 359 Secretary's Trip to Bonn-London”*, Sept. 15-18, 1954 <https://nsarchive.gwu.edu/document/17552-document-07-nine-power-meeting-september-28-29>

National Archives: *“RG 59, INR, Reports Coordination and Review Staff”*, Intelligence Reports, 1965-1966, box 155, REU-4-RM

National Commission: *“The 9/11 Commission Report*, Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004, www.9-11commission.gov/

National Intelligence: *“Artificial Intelligence Ethics Framework for the Intelligence Community,”* Office of the Director of National Intelligence, June 2020, <https://www.intelligence.gov/artificial-intelligence-ethicsframework-for-the-intelligence-community>

National Intelligence: *“ICD 204 - National Intelligence Priorities Framework,”* Office of the Director of National Intelligence, January 7, 2021, https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf

National Security Commission on Artificial Intelligence, *“Final Report”*. Washington, DC: March 2021, <https://www.nsc.ai.gov/2021-final-report/>

NATO publication: *“NATO and National CNRS, Analysis”*, file:///C:/Users/255793cz/Downloads/20150311055641_NATO_And_National_C_RMS_EN_Report_v6_4.pdf

NATO publication: “Sixth Progress Report, 2021”,
https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

NATO publication: Speech by the Secretary General at the Symposium on the Political Relevance of the 1648 Peace of Westphalia, Minster, Thursday, 12th November 1998 <https://www.nato.int/docu/speech/1998/s981112a.htm>

OECD, Organization for Economic Co-operation and Development, “*Framework for policy Coherence for sustainable development*”, building policy coherence, draft for discussion, 2015,
<https://www.oecd.org/gov/pcsd/TOOLKIT%20FRAMEWORK%20FOR%20PCSD.pdf>

European Union: “*Satcen annual report 2020*”, ISBN 978-92-95034-19-8 doi 10.2820/940883
<https://www.satcen.europa.eu/keydocuments/SatCen%20Annual%20Report%202020.pdf>

Paragano D.: “*Le basi militari degli Stati Uniti in Europa: posizionamento strategico, percorso localizzativo e impatto territoriale*”. Università degli Studi di Trieste – AA – 2007/2008.

Petroni F., “*Il Baltico è un mare caldo*”, LIMES, 27/04/2018,
<https://www.limesonline.com/cartaceo/il-baltico-e-un-mare-caldo>

Picchiarelli A.: “*Per un’intelligenza artificiale a misura d’uomo: una possibile regolamentazione valoriale?*”, in *IAI Papers*, n. 20|47 dicembre 2020,
<https://www.iai.it/it/node/12578>

Quille G., Gasparini G., Menotti R., Pirozzi N., “*Developing EU Civil Military Coordination: the role of the new Civilian Military Cell*”, Joint Report by ISIS Europe and Ce.Mi.SS, giugno 2006, Bruxelles

Quiquet F.: “*Qu’est-ce que le grand Commandement De l’Espace (CDE) créé par la France pour la défense de l’espace*”, jun 2020, Space and Cyber Security,
<https://www.spacesecurity.info/quest-ce-que-le-grand-commandement-de-lespace-cde-cree-par-la-france-pour-la-defense-de-lespace/>

Schelling T., *The Strategy of Conflict*, Cambridge, MA. Harvard University Press, May 1981); Robert Jervis, “Deterrence Theory Revisited.” *World Politics* 31, no. 2 (January 1979), doi:10.2307/2009945

Schelling T.: “*Arms and Influence*”, New Haven, CT: Yale University Press, november 2008

Senate Select Committee on Intelligence: “*Hearing to examine worldwide threats*,” Hearing before the U.S., 117th Cong., 2nd sess., April 14, 2021,
<https://www.intelligence.senate.gov/hearings/openhearing-worldwide-threats-1>

Sheppard L., Conklin M.: “*Warning for the Gray Zone*,” in Hicks et al., *By Other Means Part II*, <https://www.csis.org/analysis/warning-gray-zone>

- Shea J.: *“Resilience: a core element of collective defence!”* – NATO Review, 30 mar. 2016, <https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html>
- Shedd D. R.: *“Intelligence and National Defense,”* in 2016 Index of U.S. Military Strength, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2015)
- Sims J. E.: *“Decision Advantage and the Nature of Intelligence Analysis,”* Chapter 24 in The Oxford Handbook of National Security Intelligence, ed. Loch K. Johnson, New York: Oxford University Press, 2010
- Stejskal J. *“Bear Trap: Building a Pre-Conflict Underground Force to Resist the Future Enemy,”* Journal on Baltic Security, vol.1, october 2022
- Stojanović B.: *“Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications,”* Sensors 21, no. 5, February 2021, doi:10.3390/s21051594
- Taini D.: *“Il boom dei satelliti: affari e geopolitica,”* aprile 2022, https://www.corriere.it/opinioni/22_aprile_20/boom-satelliti-affari-geopolitica-c4d14ef4-c0d6-11ec-a9eb-2524bc1194db.shtml
- Terzi di Sant’Agata G., *La Cooperazione Internazionale nel campo della sicurezza: l’Italia nelle principali organizzazioni multilaterali*, in La Comunità Internazionale, Fasc 1/2008, Editoriale Scientifica, Napoli
- Thomas M.A. *“Time for a Counter AI Strategy”* in Strategic Studies Quarterly – Policy Forum, spring 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Thomas.pdf
- Tossini J.V. *“The Five Eyes. The intelligence Alliance of the Anglosphere”*, april 2020, <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>
- Van Puyvelde D., *“European Intelligence Agendas and the Way Forward,”* International Journal of Intelligence and Counterintelligence 33, no. 3 (2020): 508
- Van Puyvelde D., Coulthart S., Shahriar Hossain M., *“Beyond the Buzzword: Big Data and National Security Decision-Making,”* International Affairs, Vol. 93, No. 6, november 2017
- Wither J.K., *“Back to the Future ? – Nordic total defence concept”*, jan 2020, Defence Studies series, vol. 20, iussue 1, <https://doi.org/10.1080/14702436.2020.1718498>
- Wolf T.: *“Die Entstehung des BND. Aufbau, Finanzierung, Kontrolle,”* Ch. Links Verlag; 1., Auflage 2018, 4 Oct. 2018, ISBN-10 396289022X
- Zanini A.: *Armi antisatellite: la nuova corsa agli armamenti spaziali*, Aspenia online, 31 gennaio 2022, <https://aspeniaonline.it/armi-antisatellite-la-nuova-corsa-agli-armamenti-spaziali/>

Sitografia

<https://atlantic-cable.com/CableCos/AngloAmerican/>

<https://atlantic-cable.com/stamps/Cablesips/indexstc.htm>

<https://carnegieendowment.org/programs/npp/hypersonic/>

<https://dispes.units.it/it/dipartimento/persona/personale-docente?q=it/node/1232>

https://ethw.org/Transatlantic_Optical_Cable

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008M042>

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/euspa_it

<https://history.state.gov/departmenthistory/people/by-name>

<https://history.state.gov/historicaldocuments/frus1948v02/d529>

https://knowledge4policy.ec.europa.eu/publication/eu-conflict-early-warning-system-objectives-process-guidance-implementation_en

<https://members.parliament.uk/member/1688/career>

<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1566262/intelligence-in-a-data-driven-age/>

<https://shape.nato.int/about/leadership-staff/command-group>

<https://sofrep.com/news/special-forces-detachment-a-an-elite-cold-war-unit/>

<https://www.academyofdiplomacy.org/member/thomas-l-hughe>

<https://www.aeronautica.difesa.it/organizzazione/loStatoMaggiore/organigramma/Pagine/UGS.aspx>

<https://www.asi.it/scienze-della-terra/cosmo-skymed/>

<https://www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/das-weltraumkommando-der-bundeswehr-5443406>

<https://www.consilium.europa.eu/it/council-eu/preparatory-bodies/coreper-ii/>

<https://www.cybersecitalia.it/tanel-sepp-la-nascita-eu-cybrid-serve-aumentare-la-consapevolezza-dei-leader-europei/3707/>

<https://www.difesa.it/Content/Manifestazioni/FORUMPA/2004/SistemaSICRAL/Pagine/default.aspx>

https://www.difesa.it/SMD_/Avvenimenti/giornata_nazionale_spazio/Pagine/Comando_Operazioni_Spaziali.aspx

<https://www.eastwestcenter.org/publications/will-the-partnership-global-infrastructure-and-investment-be-game-changer-in-the-indo>

https://www.eeas.europa.eu/node/32969_en

<https://www.eisenhowerlibrary.gov/sites/default/files/finding-aids/pdf/byroade-henry-papers.pdf>

https://www.europarl.europa.eu/doceo/document/E-7-2012-006027_EN.html?redirect

https://www.europarl.europa.eu/doceo/document/E-7-2012-006027-ASW_EN.html

<https://www.fpri.org/contributor/frank-hoffman/>

<https://www.hybridcoe.fi/who-what-and-how/>

https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=1782&lid=785

<https://www.intelligence-college-europe.org/>

<https://www.intelligence-college-europe.org/declaration-of-mrs-beth-sizeland-on-the-occasion-of-the-british-presidency-of-the-college/>

https://www.nato.int/cps/en/natohq/news_127836.htm

https://www.nato.int/cps/en/natohq/news_196144.htm

https://www.nato.int/cps/en/natohq/topics_156338.htm

https://www.nato.int/cps/en/natohq/topics_49202.htm

https://www.nato.int/cps/fr/natohq/topics_64557.htm?selectedLocale=pl

<https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html>

<https://www.nec.belvoir.army.mil/902dNCRFO/history.asp>

<https://www.oecd.org/about/secretary-general/selection-process/Cecilia-Malmstrom-Sweden-Bio.pdf>

<https://www.politico.com/news/2021/04/26/spychiefs-information-war-russia-china-484723>

<https://www.satcen.europa.eu/page/copernicus>

<https://www.spaceforce.mil/About-Us/About-Space-Force/>