

# I Report dell'IsAG

*September 2016*

*Quale futuro per la cooperazione intelligence in materia antiterrorismo?*

*Author: Marlene Mauro*

89



## **Sommario**

---

*La presenza di minacce transnazionali e l'oggettiva difficoltà per ciascun servizio di intelligence di affrontare il rischio legato ai fenomeni terroristici di matrice islamica, sottolineano l'assoluta urgenza di affrontare finalmente il tema legato alla spinosa questione della cooperazione informativa tra i principali Paesi europei. Il report provvederà a riassumere i principali miglioramenti introdotti nel sistema di intelligence sharing europeo, accordando particolare attenzione alla minaccia terroristica e all'insieme di misure implementate per affrontarla. L'analisi esaminerà inoltre i punti di forza e debolezza dell'architettura intelligence europea con l'obiettivo di fornire riflessioni e linee guida potenzialmente utili nel prossimo futuro.*

## **Abstract**

---

*The increasing importance of transnational threats and the objective difficulty for each intelligence agency to address the terrorist risk, highlight the absolute urgency to finally address the issue related to the thorny question of intelligence sharing between the main EU countries. The report will provide to reassume all the major improvements introduced in UE Intelligence sharing system, giving particular attention to the jihadist threat and to the whole system of security measures improved to address it. The analysis will also examines the strengths and weakness of European Intelligence architecture with the aim of proposing reflections and a guidelines for future development.*

**Parole chiave: Intelligence Sharing, EU, Europol, Terrorismo**

**Keywords: Intelligence Sharing, EU, Europol, Terrorism**

**Lingua: Italiano**

**Language: Italian**

## ***L'Autore - About the author***

---

### **MARLENE MAURO**

Ricercatrice associata del programma "Antiterrorismo", IsAG, Roma  
Associate Researcher of the "Antiterrorism" Programme, IsAG, Rome  
Laurea Specialistica in Relazioni Internazionali, Università Roma Tre  
MA in International Relations, Roma Tre University  
Specializzazione in Intelligence e Sicurezza Nazionale, LinkCampus  
Postgraduate Specialization in Intelligence and National Security, LinkCampus



Le opinioni espresse in questo report sono esclusivamente dell'Autore e non rappresentano il punto di vista dell'IsAG.  
Any opinions or ideas expressed in this paper are those of the individual author and don't represent views of IsAG.

**ISSN: 2281-8553**

**© Istituto di Alti Studi in Geopolitica e Scienze Ausiliarie**

# Indice

---

1. Premessa - fattori ambientali e analisi di scenario .....	4
1.1 <i>I vantaggi della cooperazione e specializzazione informativa</i> .....	4
1.2 <i>Criticità normative e politiche</i> .....	5
2. Breve quadro riassuntivo degli attuali strumenti di cooperazione .....	7
2.1 <i>Cooperazione multilaterale</i> .....	7
2.2 <i>Cooperazione bilaterale</i> .....	10
2.3 <i>Club informali</i> .....	10
3. Cooperazione intelligence antiterrorismo .....	11
3.1 <i>Condivisione intelligence e contrasto convenzionale alla minaccia</i> .....	11
3.2 <i>Banche dati e sistemi IT di condivisione informativa</i> .....	13
3.3 <i>Cooperazione giudiziaria</i> .....	15
3.4 <i>Cooperazione in ambito Cyber e Communication</i> .....	15
3.5 <i>Cooperazione per il contrasto alle attività di finanziamento del terrorismo</i> .....	16
3.6 <i>Ulteriori misure di cooperazione informativa</i> .....	16
4. Una cooperazione intelligence è possibile? Modelli di <i>information sharing</i> e prospettive future .....	16

## 1. Premessa - fattori ambientali e analisi di scenario

Il complesso scenario di crisi e di mutamento multi-fattoriale che ha interessato il contesto internazionale ha consolidato la radicata percezione di un'insicurezza globale le cui caratteristiche, del tutto differenti rispetto al passato, pongono spesso problemi di analisi e reazione anche ai servizi di sicurezza nazionale.

Lo stato di crisi permanente, insicurezza e quotidiana conflittualità converge con caratteristiche ambientali in cui la comunicazione e la percezione dell'emergenza perpetua influenza ampiamente le agende e le modalità di *policy* governativa. Se ciò non bastasse, la congiuntura economica costringe a contingentare le risorse anche in quei settori di impiego fondamentali alla garanzia di sicurezza, evidenziando così le numerose criticità con cui la gestione e la mitigazione del rischio devono confrontarsi. Nel contesto appena definito, non sorprende quindi che la tematica dell'intelligence e l'opportunità di incrementare gli sforzi di cooperazione per garantire maggiore sicurezza, abbia acquisito nuovamente - e non a torto - un posto di primo piano all'interno del dibattito europeo e internazionale.

L'attualità del dibattito è stata di recente intensificata dalla manifesta debolezza dei frammentari servizi di intelligence europea che si trovano oggi a dover contrastare, con risorse ben inferiori a quelle probabilmente indispensabili, il complesso fenomeno del terrorismo internazionale promosso ed attuato da *Daesh*.

L'esistenza di cellule capaci di attivarsi autonomamente, la minaccia rappresentata dai lupi solitari e l'esistenza di un coordinamento centrale capace di segnalare l'opportunità di attentati su suolo europeo, lasciando però autonomia tattica circa le modalità e i tempi dell'esecuzione, rende il complesso compito del contrasto al fenomeno terroristico particolarmente difficoltoso.

La rete jihadista, sia essa pienamente organizzata o di spontanea affiliazione, attraversa in modo trasversale le società europee e ha le risorse - in termini di uomini e mezzi - per colpire lì dove, per ragioni differenziate di impatto mediatico, ideologia

anti-occidentale, o opportunità di reclutamento, può essere maggiore il vantaggio e risulta ridotto il rischio di fallimento (anche a causa della debolezza degli apparati di contrasto).

L'esistenza di minacce transnazionali e integrate nei tessuti societari delle stesse nazione europee; la carenza di risorse destinate all'ambito intelligence e l'oggettiva impossibilità per ciascun servizio di sicurezza di monitorare in modo totalitario e capillare qualunque soggetto potenzialmente rischioso, evidenzia - oggi in misura maggiore che in passato - l'assoluta urgenza, necessità e opportunità di affrontare definitivamente il problema relativo non solo alla più ampia integrazione europea di carattere politico, ma anche la spinosa questione relativa alla creazione di sistemi autentici di *information sharing* tra i principali paesi dell'Unione.

### 1.1 I vantaggi della cooperazione e specializzazione informativa

I vantaggi della cooperazione non possono sfuggire visti gli elementi che abbiamo già precedentemente accennato.

In uno scenario di crescenti vincoli di bilancio, scarse risorse economiche e minacce sistemiche e transnazionali, la condivisione informativa tra Paesi che convergono nel voler assicurare la riduzione della minaccia terroristica su proprio territorio, costituirebbe evidentemente un importante progresso in direzione delle garanzie di una maggiore sicurezza collettiva.

Ad oggi i rapporti di intelligence sono fondati sulla credibilità e sulla reputazione delle singole agenzie e dei singoli soggetti, individualità ben precise, che ne veicolano l'immagine e l'interazione. L'implementazione dei pur esistenti meccanismi di cooperazione intelligence europea continua a non essere sufficientemente perseguita per legittime preoccupazioni di carattere politico, e qualunque struttura organizzata esistente rischia di restare attualmente seconda a quel tipo di scambio informativo a carattere personalistico o informale che spesso, per la stessa natura del settore, condiziona la cooperazione su campo.

Dall'analisi dello scenario esistente si possono individuare alcuni importanti indicatori che evidenziano come manchi una precisa strategia di collaborazione e come, al contrario, permangano tipi di relazioni e scambi informativi generici, sporadici e strumentali. Tutti elementi che ben manifestano la diffidenza politica e la complessità di attuare dei reali meccanismi di cooperazione intelligence tra i Paesi del Vecchio Continente.

Nell'attuale scenario è tenuto adeguatamente conto delle caratteristiche della congiuntura economica tutt'altro che favorevole, il sistema di *intelligence sharing*, se rafforzato, potrebbe permettere di massimizzare il risultato in termini di sicurezza dei singoli Stati europei, risparmiando al contempo risorse spesso non più disponibili. Il fenomeno terroristico rappresenta inoltre un ottimo punto di partenza per l'analisi delle attuali debolezze dei sistemi statali. Alcune delle principali caratteristiche del fenomeno *Daesh* sono infatti riconducibili alla sua natura di Stato-diffuso transnazionale; è dalla ramificazione, dalle reti costituite ed auto-costituite, dalla differenziazione degli strumenti di attacco, dalla pluralità di uomini e risorse e dalla contemporanea potenziale presenza offensiva su diversi territori che il Califfato trae i suoi principali vantaggi. Sarebbe di conseguenza utile analizzare il fenomeno della cooperazione informativa tenendo presente che solo una pluralità di strumenti e una convergenza transnazionale di interessi a contrasto della minaccia, possono raggiungere l'obiettivo di ridurre e prevenire efficacemente la possibilità di attentati su suolo europeo.

La presenza in Europa di Paesi che perseguono interessi plurimi e non sempre reciprocamente compatibili è certamente uno dei principali problemi sulla strada dell'efficace condivisione informativa. Tuttavia la differenziazione di politiche e interessi in ambito europeo potrebbe costituire un vantaggio non indifferente in ragione della potenziale integrazione di informazioni relative ad aree, soggetti, tematiche e priorità differenti che, se messe a sistema, possono

significativamente aumentare la chiarezza della visione d'insieme.

Se ciascun Paese riuscisse a definire una propria specializzazione informativa, elemento per altro spesso già presente, e a condividere il suo vantaggio competitivo nei singoli settori di pertinenza con gli altri *partner* europei, si riuscirebbe con ogni probabilità ad incrementare la capacità informativa generale, massimizzando i benefici, riducendo i costi e liberando risorse per il riorientamento e la specializzazione ulteriore delle funzioni di analisi e previsione. L'applicazione degli strumenti di analisi economica del vantaggio comparato derivante dalla specializzazione potrebbe aiutare, nel caso di specie, a comprendere le potenzialità di un modello di integrazione differenziale tra specializzazioni intelligence dei singoli Paesi europei<sup>1</sup>.

Tenendo presente che l'intelligence dovrebbe perseguire i propri risultati, non servendosi di strumenti grossolani e eccessivamente pervasivi (e quindi dispendiosi e non in linea con le priorità democratiche), ma sfruttando con razionalità, perspicacia e capacità strategica quelle opportunità suggerite dall'impiego di raffinate risorse intellettuali e tecnologiche, è auspicabile che venga rapidamente superata l'attuale incapacità di cogliere i benefici di un'accorta e ben strutturata cooperazione intelligence.

### ***1.2 Criticità normative e politiche***

I recenti attentati di Parigi e Bruxelles hanno intensificato il dibattito sull'opportunità di cooperazione intelligence in ambito UE, mostrando apparentemente una significativa convergenza di intenti in tale direzione. Sebbene sia convinzione di chi scrive che l'intensificarsi della minaccia e dell'impatto su territorio siano elementi storicamente favorevoli alla creazione di senso di comune

---

<sup>1</sup> *Intelligence Sharing. La collaborazione internazionale nell'intelligence come strumento per la sfida economico-finanziaria del nuovo decennio*, «Istituto Italiano di Studi Strategici», maggio 2012, <[http://www.strategicstudies.it/wp-content/uploads/2012/05/paper\\_16-05-2012INTELLIGENCE-SHARING.pdf](http://www.strategicstudies.it/wp-content/uploads/2012/05/paper_16-05-2012INTELLIGENCE-SHARING.pdf)>

appartenenza e all'implementazione dei meccanismi orientati alla maggiore integrazione politica, una reale convergenza sui meccanismi di *information sharing* sembra tutt'ora ostacolata da fattori di diversa natura:

➤ **La “disabitudine” all'integrazione informativa nazionale**, costituisce a riguardo uno dei principali problemi di carattere strutturale e organizzativo. È solo recente la comprensione e adozione in Italia di strumenti e strutture di condivisione tra le forze di sicurezza presenti sul territorio e i servizi di intelligence. Il rischio di duplicazione delle funzioni e la carenza di reale comprensione delle opportunità offerte dall'adozione del principio del *need to share*, hanno per lungo tempo costituito ostacoli rilevanti anche alla formazione di una cultura e di una politica della sicurezza integrata all'interno dei singoli contesti nazionali. Mancando ancora l'abitudine e la cultura della condivisione, si comprende agevolmente come la possibilità reale di estendere l'integrazione informativa al di fuori dei confini nazionali possa incrociare serie difficoltà generate dall'assenza, purtroppo ancora attuale, di una mentalità di sistema. Va segnalato come l'esperimento italiano rappresentato dal Comitato di Analisi Strategica Antiterrorismo (CASA)<sup>2</sup> istituito nel 2004, sia nel panorama di condivisione informativa, tutt'ora una novità e un modello virtuoso di cui non si può che caldeggiare l'estensione a livello comunitario. Il principale elemento che favorirebbe l'espansione del modello in ambito europeo è collegato alla natura estremamente specifica dei suoi compiti. Se una mentalità della condivisione sui temi della prioritaria sicurezza dello Stato è ancora parzialmente assente a livello nazionale e ampiamente osteggiata a livello internazionale per chiare ragioni che

ineriscono alla difesa degli interessi di ciascun Paese, più agevole e realizzabile sembra la creazione di una struttura in cui le opportunità di *information sharing* siano rigidamente circoscritte alla singola minaccia terroristica. Un simile schema non esporrebbe i *partner* europei al rischio di condividere reciprocamente informazioni capaci di fornire ai *competitor* elementi da cui trarre un vantaggio politico-economico nel raggiungimento di interessi contrastanti. Riprendendo il modello sulla cui base è strutturato il CASA, un'analogia cooperazione in ambito europeo legittimata da adeguati assetti normativi potrebbe di conseguenza concentrarsi (puntando sull'integrazione informativa dei dati disponibili e sulla raccolta Osint) su:

- attività di controllo coordinato a livello europeo e in contesti vicini all'estremismo islamico, nei confronti di cittadini stranieri contigui agli ambienti radicali;
- servizi di controllo straordinario e di carattere preventivo volti a ridurre la minaccia di attentati sui territori dei Paesi membri;
- approfondimenti svolti su soggetti, enti e associazioni per verificare adeguati flussi di finanziamento verso organizzazioni legate al terrorismo internazionale;
- costante monitoraggio (e auspicabile intervento diretto di repressione/infiltrazione) della rete internet con riferimento a siti e canali impiegati dai fondamentalisti.

Un modello capace di concentrare sforzi congiunti nei campi della prevenzione, repressione, monitoraggio e controllo dei finanziamenti al terrorismo, sarebbe di conseguenza un buon compromesso tra l'esigenza legittima e prioritaria degli Stati di difendere il proprio patrimonio informativo e la necessità di intensificare in termini di efficacia ed efficienza il contrasto alla minaccia terroristica.

➤ **La non uniformità delle legislazioni e delle modalità operative** dei Paesi membri, che potrebbe causare problemi di carattere

<sup>2</sup> Collaborazione istituzionale, Sistema di Informazione per la Sicurezza della Repubblica, <<https://www.sicurezza nazionale.gov.it/sisr.nsf/cosa-facciamo/collaborazione-istituzionale.html>>.

organizzativo, amministrativo e logistico anche in relazione ad elementi secondari come l'esistenza nei paesi UE di un linguaggio tecnico non omogeneo.

- **La forte frammentazione dell'Unione** e le già ampiamente dibattute difficoltà incontrate dai tentativi di cessione di sovranità in settori di storica competenza nazionale come la politica di sicurezza e difesa, certamente non facilitano le prospettive di genesi di un'intelligence europea. Un simile progetto è, a detta di molti, assolutamente irrealizzabile nella sua totalità. Gli elementi per concordare con tale visione sono molteplici e tutti fondamentalmente riconducibili all'esistenza di diversi "filoni" di confronto/scontro sommerso tra gli stessi Paesi europei.

Sul piano squisitamente politico le principali sfide poste alla cooperazione possono riassumersi come segue:

- **Preferenze divergenti:** ciascuna nazione è portata allo scambio informativo e a stabilire funzioni di intelligence condivisa se ritiene che tali attività favoriscano i suoi interessi. L'esistenza di meccanismi di economia di scala e la necessità di supportare obiettivi politici comuni rappresentano certamente forti incentivi alla cooperazione. Nonostante ciò si riscontrano forti resistenze correlate ai rischi derivanti dalla condivisione di fonti e metodi operativi. Non va sottovalutato inoltre il ruolo di "merce di scambio" che le informazioni spesso acquisiscono, né la loro natura di strumento spendibile per guadagnare vantaggi politici o commerciali. In un contesto di perdurante contrasto e divergenza politico-economica tra i Paesi membri dell'Unione, non sorprende che il timore di veder diminuire i vantaggi derivanti dai propri prodotti intelligence costituisca un blocco razionale e oggettivo alla piena integrazione informativa.
- **Asimmetrie:** in aggiunta alle preferenze divergenti, i Paesi membri dell'Unione sono caratterizzati da un'ampia

disomogeneità, da diverse capacità di raccolta informativa e da ampie differenze in termini di influenza politico-economica. Ciò conduce inevitabilmente ad una "selezione" gerarchica che rischia di generare meccanismi di cooperazione intelligence caratterizzati da trattamenti differenziali in ragione del maggior potere di ciascuno Stato.

- **Mancanza di infrastrutture:** la cooperazione intelligence è inoltre generalmente dipendente dall'esistenza di un'adeguata condivisione delle infrastrutture e degli *asset*. Perché ciò avvenga sono necessari tuttavia alti livelli di fiducia e credibilità reciproca tutt'ora assenti.

## 2. Breve quadro riassuntivo degli attuali strumenti di cooperazione

Nel paragrafo che segue esamineremo i diversi strumenti di cooperazione intelligence esistenti a livello multilaterale, bilaterale e informale.

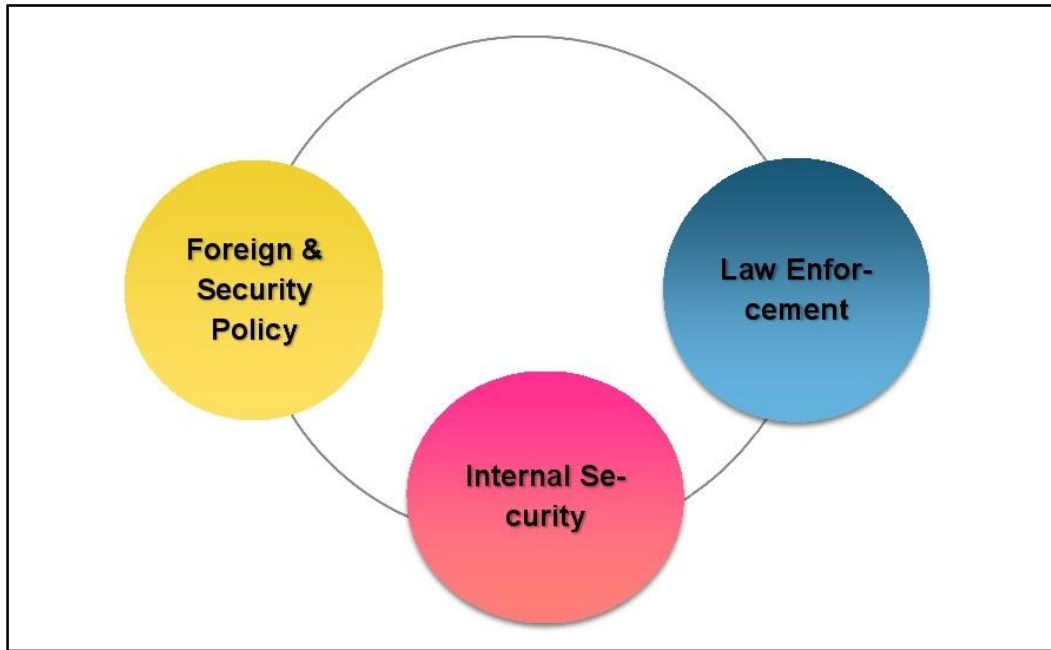
### 2.1 Cooperazione multilaterale

Il dibattito sulla condivisione intelligence europea ha conosciuto più volte, e sempre in prossimità di eventi terroristici su territorio comunitario, momenti di celebrità in genere coronati da misure e adeguamenti legislativi validi, ma spesso non pienamente realizzati.

A differenza di quanto potrebbe suggerire la sola percezione mediatica del problema, gli strumenti di *information sharing* già presenti in ambito europeo sono numerosi e appaiono, se implementati, sufficienti a garantire un adeguato livello di condivisione in vista di eventuali interventi futuri più incisivi.

L'Unione ha svolto, nel corso degli ultimi quindici anni, un importante lavoro di progressiva integrazione e condivisione informativa, sviluppato intorno all'implementazione di tre funzioni fondamentali:

1. *Foreign and security policy*
2. *Internal Security*
3. *Law enforcement*



Tenendo presente che il contrasto al terrorismo, per la sua natura ibrida e multifattoriale, richiede di fatto l'implementazione di ciascuna delle funzioni elencate, si riporta di seguito un breve schema riassuntivo degli assetti esistenti che permetterà di procedere in seguito con un'analisi più approfondita.

#### ***Int Cooperation - Foreign and Security Policy***

La cooperazione intelligence orientata al supporto della politica estera e di sicurezza costituisce probabilmente l'ambito in cui l'azione europea ha raggiunto maggiori risultati in termini di efficienza e integrazione. L'*information sharing* si svolge prevalentemente in ambito istituzionale e all'interno delle strutture dell'EEAS, articolandosi nelle seguenti strutture intelligence e di condivisione informativa:

- ***L'UE Intelligence and Situation Centre (INTCEN)***<sup>8</sup> costituisce l'*hub* principale della raccolta ed elaborazione informativa in ambito europeo e focalizza la sua attenzione su scenari esteri di particolare rilevanza per il supporto alla politica estera dell'Unione. La creazione dell'INTCEN, derivante dalla precedente struttura del

SITCEN, è strettamente connessa alla Politica di Difesa e Sicurezza Comune dell'Unione e alla creazione della figura dell'Alto Rappresentante per gli affari esteri. Il SITCEN venne creato nel 2002 all'interno del Segretariato Generale per essere direttamente collegato con l'ufficio dell'allora Alto Rappresentante Javier Solana. Nel 2005 esso venne rafforzato inserendo al suo interno un team di esperti in antiterrorismo provenienti dai servizi di sicurezza dei Paesi membri. La successiva collaborazione con l'*UE Military Staff Intelligence Directorate* (INTDIR) ha ulteriormente rafforzato le funzioni e capacità di analisi dell'agenzia europea. Oggi l'INTECEN è alle dirette dipendenze del Servizio Europeo di Azione Esterna e riceve il contributo informativo delle Agenzie di sicurezza nazionali dei Paesi membri. L'agenzia svolge funzioni di intelligence civili e coadiuva tramite le sue analisi i rappresentanti degli organismi esecutivi di Bruxelles<sup>4</sup>. Lo scambio informativo all'interno dell'INTCEN avviene tramite i servizi di sicurezza degli Stati membri e attraverso il canale informale del *Counter Terrorism Group*

<sup>8</sup> *EUINTCEN. Intelligence Analysis Centre*, 5 February, 2015, <[https://eeas.europa.eu/factsheets/docs/20150206\\_factsheet\\_eu\\_intcen\\_en.pdf](https://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf)>.

<sup>4</sup> Lo strumento giuridico su cui si fondano le basi legali di EUINTCEN è rappresentato dalla Decisione del Consiglio dell'Unione del luglio 2012.



costituito dopo gli attacchi dell'11 settembre all'interno del Club di Berna.

- **L'Intelligence Directorate (INTDIR)**<sup>5</sup> dipendente dall'*UE Military Staff*, il cui focus è concentrato su questioni di stretto interesse militare.
- **EU Satellite Centre (SATCEN)**<sup>6</sup>. L'azione Esterna dell'Unione è infine rafforzata grazie al supporto **IMINT** (*Imagery intelligence*) fornito dall'*EU Satellite Centre*.

### ***INT Cooperation - Law Enforcement***

Per ciò che riguarda le attività di *Law Enforcement* la cooperazione si svolge prevalentemente per tramite dell'**Europol**<sup>7</sup> che ospita al suo interno diverse strutture e database di condivisione informativa la cui implementazione ha costituito oggetto di recenti misure legislative.

**L'Europol** costituisce il principale *hub* per lo scambio di informazioni e analisi inerenti al contrasto dei fenomeni criminali e di stretta competenza delle forze di polizia nazionali.

Il principale riferimento normativo della cooperazione in ambito di *Law Enforcement* è contenuto nella **decisione quadro 2006/960/GAI**<sup>8</sup> relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione e recepita nell'ordinamento italiano con il **Decreto Legislativo n. 54 del 23 aprile 2015**<sup>9</sup>.

La semplificazione attuata in materia interessa le autorità nazionali competenti incaricate all'applicazione della legge, escludendo esplicitamente gli organismi

informativi disciplinati nel nostro ordinamento dalle disposizioni della legge n. 124/2007. Lo scambio può essere effettuato dietro esplicita richiesta o su iniziativa delle autorità nazionali competenti nel caso in cui sussistano le ragioni per ritenere che le informazioni possano contribuire all'individuazione, prevenzione o alle indagini riguardanti i reati di cui all'articolo 2 paragrafo 2 della decisione 2002/584/GAI<sup>10</sup> del Consiglio relativa al mandato d'arresto europeo.

Sebbene la normativa esposta possa apparire debole o incompleta per l'esplicita esclusione delle Agenzie Intelligence nazionali dai meccanismi di scambio disciplinati, essa in realtà costituisce un ottimo strumento di cooperazione il cui profilo di ambiguità e debolezza può essere superato ove si consideri che l'attività di contrasto alla criminalità non dovrebbe rientrare nei compiti dei sistemi nazionali di raccolta informativa, configurandosi piuttosto come dominio di competenza delle forze dell'ordine. In tale ottica e nell'auspicabile condizione di una buona cooperazione tra forze di informazione e sicurezza interna ai singoli Stati, i profili di debolezza della normativa risultano di conseguenza totalmente superati e possono costituire un importante tassello per affrontare parte delle incombenze necessarie alle attività di contrasto al terrorismo internazionale.

### ***Int Cooperation - Internal Security***

Per ciò che concerne la cooperazione in tema di supporto e garanzia della sicurezza interna ai singoli Stati, va sottolineato come tale ambito di cooperazione - per quanto fondamentale - rappresenti ad oggi probabilmente il meno sviluppato all'interno delle strutture formali dell'Unione.

In tema di sicurezza interna va segnalata l'importanza preminente del **Club de Berne**, club informale di scambio e cooperazione intelligence tra i Paesi europei, Svizzera e

<sup>5</sup> European Union. External Action, <[http://eeas.europa.eu/csdp/structures-instruments-agencies/eu-military-staff/organization/index\\_en.htm](http://eeas.europa.eu/csdp/structures-instruments-agencies/eu-military-staff/organization/index_en.htm)>.

<sup>6</sup> European Union. Satellite Centre, <<https://www.satcen.europa.eu>>.

<sup>7</sup> Europol, <<https://www.europol.europa.eu>>.

<sup>8</sup> Decisione quadro 2006/960/GAI DEL CONSIGLIO, 18 dicembre, 2006, <<http://www.csm.it/Eurojust/CD/27.pdf>>.

<sup>9</sup> Decreto Legislativo 23 aprile 2015, n. 54, <[http://www.gazzettaufficiale.it/atto/serie\\_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2015-05-09&atto.codiceRedazionale=15G00068&elenco30giorni=false](http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2015-05-09&atto.codiceRedazionale=15G00068&elenco30giorni=false)>.

<sup>10</sup> Decisione quadro del Consiglio, 13 giugno 2002, <[http://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0008.02/DOC\\_1&format=PDF](http://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0008.02/DOC_1&format=PDF)>.

Norvegia, esistente fin dal 1970. Il Club non trova fondamento in nessun accordo formale, opera al di fuori delle strutture dell'Unione e rappresenta tuttora il principale punto d'incontro dei vertici delle agenzie intelligence europee.

Il Club di Berna ingloba al suo interno il **Gruppo Antiterrorismo**<sup>11</sup> (*Counter Terrorism Group* - **CTG**) le cui azioni e attività specifiche vengono coordinate tramite l'interazione formale con l'INTCEN. Il CTG garantisce la cooperazione in tema antiterrorismo sulla base di memorandi di intesa informali. La cooperazione del CTG con le strutture dell'Unione venne avviata a partire dal 2004 quando si decise di implementare gli aspetti intelligence collegati alla Dichiarazione sulla lotta al terrorismo del Consiglio Europeo. Il CTG è presente con i suoi rappresentanti all'interno dell'INTCEN, tuttavia - trattandosi di cooperazione su base volontaria - è bene sottolineare che l'invio di informazioni riservate ha carattere totalmente volontario e non formalmente strutturato. Di conseguenza il livello di efficienza ed efficacia di questo meccanismo di *information sharing* rimane strettamente legato alle singole volontà e opportunità identificate dai governi nazionali.

## 2.2 Cooperazione bilaterale

L'analisi degli strumenti di cooperazione bilaterale si limiterà in questa sede alla sola ricognizione degli accordi generali stipulati in materia di scambio informativo dal Governo Italiano. Gli accordi generali di sicurezza costituiscono uno strumento per gestire lo scambio di informazioni classificate con altri Paesi e organizzazioni internazionali.

Gli accordi vengono stipulati dal DIS e sono attualmente attivi nei confronti di ventisette Paesi, di cui sedici membri dell'Unione<sup>12</sup>, più l'EEAS e OCCAR.

Attraverso gli stessi le parti si impegnano ad applicare misure e procedure di sicurezza adeguate a garantire la protezione delle informazioni classificate. Con gli accordi di sicurezza si garantiscono<sup>13</sup>:

- l'Identificazione delle autorità di sicurezza nazionale dei Paesi firmatari e l'attivazione di canali ufficiali di comunicazione delle informazioni;
- il mutuo riconoscimento delle abilitazioni di sicurezza di persone fisiche ed operatori economici;
- la reciproca protezione delle informazioni scambiate;
- l'attivazione di procedure di sicurezza comuni per le visite ed i trasporti classificati.

L'attenzione accordata alla complessa questione della protezione delle fonti, alla non ulteriore diffusione delle notizie a Paesi terzi e all'equiparazione dei livelli di classificazione, dimostra la complessità delle tematiche trattate e evidenzia i problemi presenti anche in ambito europeo circa le garanzie di adeguata protezione e la necessità di omologare differenti sistemi di organizzazione interna alle agenzie.

## 2.3 Club informali

Il principale sistema di condivisione informativa fin qui impiegato dalle agenzie intelligence nazionali fa riferimento a club informali di natura pubblica ma riservata e di appartenenza selezionata. Si citano a riguardo i due casi noti del Club di Berna e del Medi Club, che veicolano lo scambio volontario di informazioni utili al coordinamento delle attività di contrasto alla minaccia.

Le informazioni così scambiate sono soggette alle ordinarie clausole che generalmente investono anche gli accordi bilaterali, non possono essere cedute su

<sup>11</sup> Counter Terrorist Group (CTG), <<http://pilac.law.harvard.edu/europe-region-efforts/counter-terrorist-group-ctg>>.

<sup>12</sup> Bulgaria, Estonia, Finlandia, Francia, Germania, Lettonia, Lituania, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Romania, Slovacchia, Slovenia,

Spagna, Ungheria. Vedi Sistema di Informazione per la Sicurezza della Repubblica, <[www.sicurezza nazionale.gov.it](http://www.sicurezza nazionale.gov.it)>.

<sup>13</sup> Accordi generali di sicurezza, Sistema di Informazione per la Sicurezza della Repubblica, <<http://www.sicurezza nazionale.gov.it/sisr.nsf/documentazione/accordi-general-di-sicurezza.html>>.

richiesta di terzi né usate per fini diversi da quelli stabiliti. È evidente che in un simile contesto il ruolo dei singoli soggetti a cui viene affidata la responsabilità della condivisione informativa acquista importanza predominante e permette spesso di ottenere informazioni rese disponibili, non tanto e non prevalentemente da sistemi regolamentati di scambio informativo, quanto dall'esistenza di rapporti personali di fiducia e reciproca stima che consentono di veicolare le informazioni al di fuori di strutture di condivisione formali. Il problema dei club è, come già accennato, relativo alla natura totalmente volontaristica, generale e non definita delle informazioni in essi veicolate; questa caratteristica impedisce di fatto di considerare lo strumento di cooperazione informale ai fini della valutazione di efficienza delle strategie coordinate in ambito europeo.

### 3. Cooperazione intelligence antiterrorismo

Il cambiamento nella natura e delle sfide poste ai sistemi di sicurezza nazionali è strettamente legato alla natura delle nuove minacce emergenti e manifesta le sue importanti ripercussioni anche in ambito europeo ove si consideri la maggiore complessità che un'adeguata cooperazione intelligence transnazionale può comportare. Le numerose strutture europee di prevenzione e contrasto al terrorismo hanno generato una complessa sfera transnazionale di contrasto al fenomeno che risponde certamente, almeno in linea di principio, alla necessità di confronto con minacce transnazionali di natura ibrida, ma pone non poche complessità circa l'efficienza e l'efficacia di un simile sistema di coordinamento.

Accennando brevemente al processo di genesi dei primi meccanismi di cooperazione in materia non può essere tralasciata la spinta decisiva derivante dagli attacchi condotti su territorio europeo a partire dal 2004 e di poco successivi all'attentato terroristico dell'11 settembre. Il collegamento sempre più stretto tra dimensione interna ed estera della sicurezza si manifestò qui con tutta la sua intensità, spingendo allora Alto

Rappresentante Solana all'adozione di misure e proposte di fondamentale importanza per la costituzione di strumenti europei di prevenzione.

#### 3.1 *Condivisione intelligence e contrasto convenzionale alla minaccia*

L'impegno strategico europeo<sup>14</sup> nel contrasto al terrorismo si basa sui quattro pilastri di:

- **Prevenzione**
- **Protezione**
- **Perseguimento**
- **Risposta a situazioni di emergenza**

L'attuale assetto di *information sharing* dell'Unione può contare su numerose strutture e strumenti di condivisione informativa articolati secondo i diversi ambiti di competenza. L'esigenza di contrastare un fenomeno complesso impone di porre attenzione agli aspetti integrati di *Law Enforcement*, Sicurezza e Difesa estera e Sicurezza interna, e suggerisce contestualmente una maggiore cooperazione informativa anche in ambito giuridico e investigativo. Il fenomeno *Daesh* esplica gran parte della sua pericolosità su suolo europeo in relazione alla sua grande attrattività e alla capacità di dotarsi di numerosi strumenti di comunicazione e di radicalizzazione che sfruttano la dimensione del *cyber-space*.

L'azione europea si è di conseguenza concentrata anche su quest'ultimo settore, avviando azioni finalizzate a coordinare gli sforzi dei Paesi membri contro il rischio di radicalizzazione in ambiente *cyber*.

Fondamentale ai fini di una corretta strategia di prevenzione è infine lo strumento delle banche dati che, come vedremo di seguito, può contare su numerosi database che risultano però non ancora perfettamente integrati tra loro e non pienamente implementati dai singoli governi nazionali.

Tentando una schematizzazione che segua, per quanto possibile, le linee guida delle attività di contrasto stabilite in seno all'Unione

---

<sup>14</sup> Consiglio dell'Unione Europea, 30 novembre 2005, <<http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=it>>.

si evidenzia come, per ciò che riguarda le attività di prevenzione e protezione la cooperazione intelligence può servirsi dei seguenti organismi.

- **L'Europol** che, come già detto, costituisce il principale *hub* per lo scambio di informazioni e analisi inerenti al contrasto dei fenomeni criminali. Sebbene la sua competenza sia più vasta e vada oltre le sole attività di contrasto al terrorismo, Europol rimane la principale struttura di condivisione informativa finalizzata alla garanzia della *Law Enforcement* e di una maggiore cooperazione in tema di sicurezza interna tra gli Stati membri. A conferma di ciò si descriveranno più avanti le numerose banche dati interne ad Europol e il loro ruolo fondamentale nelle attività di *information sharing* europea. Il Parlamento Europeo ha inoltre di recente approvato nuove regole di *governance* volte a intensificare i poteri e le attività Europol in materia di contrasto al terrorismo internazionale. Il regolamento<sup>15</sup> potenzia le attività di contrasto ai crimini transfrontalieri e alle minacce terroristiche, e permetterà la costituzione di unità specializzate di risposta alle minacce emergenti. L'agenzia europea potrà agire in contrasto alla propaganda terroristica online attivando accordi anche con quei soggetti privati capaci di coadiuvare le operazioni. Viene inoltre imposto agli Stati un maggiore onere di condivisione informativa al fine di ridurre le lacune esistenti e di colmare le attuali inefficienze da molti considerate co-responsabili dei recenti attentati terroristici realizzati su territorio europeo. Dell'Europol fa inoltre parte il **Centro Europeo Antiterrorismo (ECTC)**<sup>16</sup> di recente creazione di cui si dirà in seguito.
- **INTCEN e INTDIR** di cui si è già detto.

- **Il Coordinatore antiterrorismo dell'UE**<sup>17</sup>, figura istituita in seno al Consiglio dell'Unione dopo gli attentati di Madrid del 2004. Attualmente l'incarico è ricoperto dal belga Giles de Kerchove, cui spetta la supervisione degli strumenti esistenti in ambito europeo, il coordinamento con il Consiglio e la condivisione con Paesi terzi.
- **Frontex**, rilevante ai fini della cooperazione antiterrorismo per il suo ruolo nella gestione dei confini esterni dell'Unione e per la rilevanza potenziale della banca dati che fa capo all'agenzia.
- **Il Club di Berna e il Counter Terrorism Group (CTG)** di cui si è già detto in precedenza. Si segnala qui la creazione recente in seno al CTG (01/07/2016) di una piattaforma finalizzata a migliorare le attività di *information sharing* e dedicata alle sole attività di contrasto al terrorismo transnazionale.

**European Counter Terrorism Centre (ECTC)**. La struttura in realtà fa parte a pieno titolo di Europol, ma viene descritta separatamente in quanto rappresenta un'innovazione significativa capace di dimostrare la reale volontà europea, dopo i tragici attentati di Parigi e Bruxelles, di attuare un serio coordinamento comunitario finalizzato alla riduzione della minaccia. L'ECTC è composto da esperti del settore incaricati alla raccolta informativa e all'analisi delle informazioni disponibili ed è strutturato in modo tale da garantire la formazione di un *network* di analisi e risposta al fenomeno all'interno delle strutture dell'Unione. Esso può contare su una banca dati separata costituita all'interno del *Secure Information Exchange Network Application* (SIENA) e sull'*Europol Analysis System* (EAS). È inoltre previsto il coordinamento con l'*Eu Internet Referral Unit* (EU IRU), l'*Europol Information System* (EIS) e le unità di intelligence finanziaria.

<sup>15</sup> EUR-Lex, <<http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0794>>.

<sup>16</sup> Europol, ECTC Infographic, <<https://www.europol.europa.eu/content/ectc-european-counter-terrorism-centre-infographic>>.

<sup>17</sup> Consiglio europeo, Il coordinatore antiterrorismo, <<http://www.consilium.europa.eu/it/policies/fight-against-terrorism/counter-terrorism-coordinator/>>.



Data la recente istituzione del Centro europeo Antiterrorismo non si può per il momento fornirne alcuna valutazione esaustiva; ci sembra però di poter concludere che gli strumenti normativi e istituzionali per progredire lungo la strada dell'*information sharing* europea siano ormai numerosi ed ampiamente presenti. La capacità di implementare adeguate strategie di reazione verrà quindi decisa dalla disposizione dei singoli governi nazionali all'uso delle piattaforme esistenti ed alla reale cooperazione a livello comunitario. La principale criticità riscontrabile nell'analisi degli strumenti di condivisione descritti riguarda infatti l'atteggiamento ancora cauto e scarsamente cooperativo che caratterizza i Governi.

I compiti di raccolta informativa sono inoltre, nella stragrande maggioranza, demandati alle intelligence nazionali che per loro natura condividono le informazioni con la consueta e legittima diffidenza che caratterizza il settore. Tuttavia tali problematiche potrebbero essere superate adeguatamente dall'introduzione dei recenti strumenti di coordinamento che, circoscrivendo l'*information sharing* allo specifico campo dell'antiterrorismo (considerato settore a sé stante e separato dagli altri), potranno in futuro favorire la condivisione riducendo le resistenze che si presenterebbero nel caso di scambi informativi non circoscritti a specifici obiettivi e ambiti di applicazione.

### 3.2 Banche dati e sistemi IT di condivisione informativa

Le banche dati costituiscono inevitabilmente la principale fonte di cooperazione informativa tanto in relazione all'elevato numero di dati immediatamente disponibili, quanto per la possibilità di condividere tali dati senza che ciò pregiudichi gli interessi economico-politici dei Paesi coinvolti.

Le banche dati attualmente attive sono le seguenti:

- **Europol Information System (EIS)**<sup>18</sup> - si configura come sistema di riferimento per l'immissione dei dati relativi ai reati commessi nei Paesi membri ed alle informazioni ad essi correlate. Le informazioni vengono inserite e condivise mediante sistema automatico di caricamento dati. L'evoluzione che ha investito l'approccio alla raccolta dati ha favorito lo sviluppo del database in direzione della maggiore efficienza ed accuratezza informativa grazie alle procedure di raccolta e incrocio di dati differenti inerenti a singoli soggetti. L'apertura dei Paesi membri all'uso della piattaforma e la possibilità di incrociare le informazioni presenti nei database nazionali con i dati registrati all'interno

<sup>18</sup> Europol, Europol Information System, <<https://www.europol.europa.eu/content/page/europol-information-system-eis-1850>>.

dell'EIS, rappresenta un rilevante passo in avanti per garantire l'*information sharing* e l'utilità dei sistemi di raccolta.

- Il ***Secure Information Exchange Network Application (SIENA)***<sup>19</sup> permette a ciascun paese di scambiare informazioni utili alla *Law enforcement* tra Paesi membri, Europol e parti terze che hanno siglato accordi di cooperazione. Il database è progettato per garantire un alto livello di interoperabilità con altri sistemi analoghi presenti in Europol e con i sistemi di raccolta dati in uso ai singoli Paesi membri.
- Lo ***Schengen information System (SIS II)***<sup>20</sup> costituisce un ampio bacino informativo progettato per coadiuvare le operazioni di controllo delle frontiere esterne e la cooperazione in materia di *Law enforcement* tra i Paesi dell'area Schenghen.
- L'***European Criminal Records Information System (ECRIS)***<sup>21</sup> garantisce lo scambio informativo sulle condanne penali all'interno dei Paesi membri e può rilevarsi un valido strumento per il contrasto al terrorismo e in relazione allo specifico fenomeno della radicalizzazione nelle carceri.
- Il ***Visa Information System***<sup>22</sup> è lo strumento impiegato per favorire lo scambio informativo sui visti di ingresso tra i Paesi dell'area Schengen. Ciascuno dei Paesi membri può disporre di un sistema di controllo e registrazione dati sul proprio territorio nazionale direttamente connesso con il sistema di controllo centrale. Le

informazioni inserite da ciascun Paese dell'area Schengen vengono rese immediatamente disponibili agli altri Stati coinvolti. Il sistema può disporre di tecnologia che consente il confronto dei dati biometrici per favorire l'identificazione dei soggetti attenzionati.

Sebbene non risulti possibile reperire informazioni precise sull'esatto funzionamento e l'attuale stato di efficienza dei sistemi di raccolta sopra indicati, esistono alcune rilevanti indicazioni che portano a concludere che la politica di integrazione e il reale impiego degli strumenti disponibili sia ancora ampiamente carente. La Nota<sup>23</sup> sullo stato di attuazione della dichiarazione del Consiglio Europeo sulla lotta al terrorismo del febbraio 2015, evidenzia a riguardo come soltanto quattordici stati membri degli attuali ventisette hanno ad oggi collegato le proprie Autorità antiterrorismo alla *Secure Information Exchange Network Application (SIENA)* di Europol. Lo scambio registrato sulla piattaforma viene definito assai esiguo rispetto alla segnalazione dei reati di stampo terroristico. I dati sono ancor meno incoraggianti se si tiene presente che nell'ottobre 2015 è stata creata all'interno del SIENA un'area apertamente riservata alle autorità antiterrorismo nazionali che risulta ancora poco sfruttata. L'analisi conoscitiva sullo stato di attuazione sottolinea inoltre come sia poco diffusa la prassi d'uso relativa alle segnalazioni dei *foreign fighters* europei all'interno del SIS II e come risulti di conseguenza ridotto il livello di completezza dei casi raccolti.

I principali problemi relativi all'uso e all'impiego delle piattaforme di registrazione e condivisione dati possono essere sintetizzati come segue.

- **Risulta assente da parte degli Stati membri una prassi di adeguato impiego degli strumenti di condivisione informativa disponibili.** Il problema, considerata l'assoluta discrezionalità di cui ciascun

<sup>19</sup> Europol, SIENA, <<https://www.europol.europa.eu/content/page/siena-1849>>.

<sup>20</sup> Schengen Information System, <[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm)>.

<sup>21</sup> ECRIS (European Criminal Records Information System), <[http://ec.europa.eu/justice/criminal/european-justice/ecris/index\\_en.htm](http://ec.europa.eu/justice/criminal/european-justice/ecris/index_en.htm)>.

<sup>22</sup> Visa Information System (VIS), <[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm)>.

<sup>23</sup> Consiglio dell'Unione Europea, 30 novembre 2015, <<http://data.consilium.europa.eu/doc/document/ST-14734-2015-INIT/it/pdf>>.

sistema di sicurezza nazionale può disporre nel decidere quali informazioni registrare e condividere all'interno delle banche dati, potrebbe essere superato non tanto con un'imposizione normativa i cui capisaldi possibili non appaiono chiari, quanto piuttosto con la progressiva genesi di una cultura della sicurezza che accolga al suo interno il principio del *need to share*. Come già sottolineato, la condivisione informativa mediante lo strumento delle banche dati non può costituire pregiudizio agli interessi nazionali ove essa sia limitata a specifici settori di intervento come il contrasto al terrorismo.

- **Si evidenzia inoltre l'assenza di strumenti idonei a garantire un adeguato controllo incrociato delle informazioni anche tra banche dati interne agli organismi dell'Unione.** Preoccupa in particolare modo l'impossibilità attuale di effettuare controlli incrociati automatici tra il sistema SIS II e le banche dati Europol. L'implementazione di adeguati sistemi di confronto e integrazione dei database interni è un punto fondamentale e di semplice realizzazione che certamente ha un profilo molto meno problematico rispetto al ben più rilevante problema delle diffidenze dei Paesi membri. Non riuscire a garantire integrazione interna agli organismi informativi dell'Unione significa abbandonare di fatto ogni possibilità di realizzare un'adeguata cooperazione informativa per mancanza anche delle sole condizioni essenziali di base.

### 3.3 Cooperazione giudiziaria

La cooperazione sul piano giuridico rappresenta certamente un altro dei punti fondamentali della strategia di contrasto al terrorismo internazionale e ciò in ragione all'esigenza di garantire capacità europea di omogeneo perseguimento penale del fenomeno. Premessa l'assoluta rilevanza in tema di inquadramento e definizione delle politiche di cooperazione giuridica del GAI (Giustizia e Affari Interni), ci limitiamo qui a segnalare due organismi europei i cui compiti

in tema di lotta al terrorismo sono stati definiti dalla Comunicazione della Commissione Europea al Consiglio e al Parlamento dell'ottobre 2007:

- **L'European Judicial Network** il cui compito è la facilitazione delle attività di cooperazione giudiziaria tra gli Stati membri.
- **L'Eurojust**, istituito nel 2002 per stimolare e migliorare il coordinamento delle indagini e azioni penali tra le autorità giudiziarie competenti degli Stati membri dell'Unione europea nella lotta alle forme gravi di criminalità organizzata e transfrontaliera, ha il compito di cooperare con le autorità nazionali anche in materia anti-terrorismo.

### 3.4 Cooperazione in ambito Cyber e Communication

Per ciò che riguarda l'ambito *cyber* e considerata la sua particolare rilevanza nei fenomeni di proselitismo e coordinamento *Daesh*, si segnala la presenza dei seguenti strumenti:

- **L'Europol Internet Referral Unit (EU IRU)**<sup>24</sup>, istituita il 1° luglio 2015 in seno all'Europol con il compito di combattere la propaganda jihadista e le attività ad essa affini perpetrate sul web. L'IRU favorisce la realizzazione di un approccio preventivo coordinato tra i vari Paesi dell'Unione, permettendo la segnalazione dei contenuti di natura estremista presenti sul web.
- Il **Syria strategic communication Advisory Team**<sup>25</sup>, nato per prevenire il fenomeno dei *foreign fighters*, ha il compito di stabilire un *network* tra gli Stati membri volto a disincentivare la partenza di cittadini europei desiderosi di unirsi come combattenti al conflitto siriano.

<sup>24</sup> Europol, <<https://www.europol.europa.eu/content/europol's-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda>>.

<sup>25</sup> Parliamentary Questions, <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-000505&language=EN>>.

- Il *Radicalization Awareness Network (RAN)*<sup>26</sup>, nato per studiare e prevenire i fenomeni di radicalizzazione, si avvale della partecipazione di team altamente specializzati e fornisce supporto agli organi decisionali dell'Unione ed a ciascun Paese membro che ne faccia richiesta.
- L'*UE Internet Forum*, progetto avviato nel 2015 per favorire la cooperazione tra Istituzioni europee ed enti privati nelle attività di monitoraggio e rimozione dei contenuti terroristici presenti in rete (con riguardo alla propaganda condotta da *Daesh* sul web).

### 3.5 Cooperazione per il contrasto alle attività di finanziamento del terrorismo

Il contrasto alle attività di finanziamento del terrorismo rappresenta un settore non secondario. A riguardo si segnala la comunicazione della Commissione Europea del febbraio 2016 nella quale viene proposta la creazione dell'*EU Terrorist Finance Tracking System* (EU TFTS) finalizzato a segnalare le transazioni sospette eseguite all'interno dell'area SEPA e denominata in Euro. Le attività di contrasto finanziario potrebbero inoltre prevedere nel prossimo futuro la più stretta cooperazione tra le Unità di intelligence finanziaria dei singoli Stati membri. L'esistenza dei già numerosi meccanismi di segnalazione di operazioni sospette e contrasto al finanziamento al terrorismo e alla criminalità organizzata, se integrato maggiormente a livello europeo, potrà certamente garantire un migliore e più efficace scambio informativo in materia.

### 3.6 Ulteriori misure di cooperazione informativa

Secondo le indicazioni dell'*European Agenda on Security*<sup>27</sup>, l'intensificazione della

politica di contrasto al terrorismo non può inoltre prescindere dall'intensificazione dei contatti con i Paesi dell'Area MENA e in particolare con Libano, Giordania, Turchia, Iraq, Algeria, Marocco e regione balcanica.

### 4. Una cooperazione intelligence è possibile? Modelli di *information sharing* prospettive future

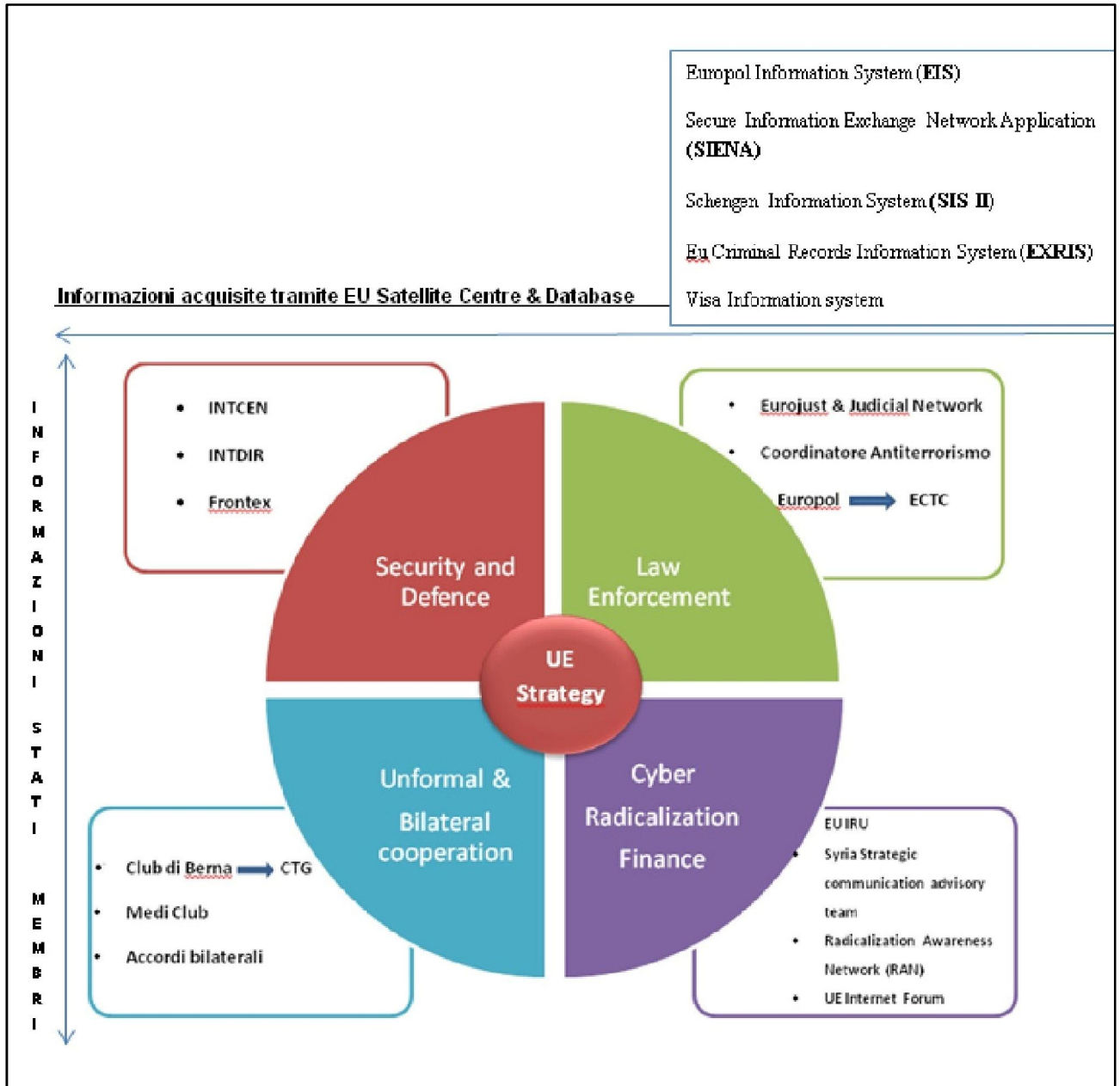
L'analisi appena effettuata mostra chiaramente l'esistenza di strutture già idonee a garantire un'efficace cooperazione intelligence europea e induce a spostare l'attenzione dai proclami politici di creazione di un "servizio unico europeo" alle strategie necessarie per rendere efficienti gli strumenti già esistenti.

Circoscrivere la cooperazione intelligence in ambito antiterrorismo, garantendo a questo specifico dominio un'importanza e un'autonomia organizzativa peculiare, è certamente - come abbiamo già avuto modo di segnalare - una scelta vincente per il superamento delle diffidenze che affliggono la cooperazione europea. Nel complesso la valutazione sulle politiche in tema di cooperazione informativa antiterrorismo non può che essere positiva, specialmente tenendo conto delle recenti ulteriori evoluzioni e dell'incisività degli ultimi strumenti approvati dagli organi decisionali dell'Unione. Per verificare il corretto funzionamento delle nuove strutture bisognerà ancora attendere e monitorare attentamente il grado di disponibilità alla cooperazione dimostrato dai governi. Il dibattito sulla creazione di un servizio intelligence europeo e sull'opportunità di garantire maggiore integrazione è tuttavia ancora aperto e investe direttamente la delicata e decennale questione relativa all'opportunità di una maggiore integrazione politica tra i Paesi del Vecchio Continente. Sebbene questa non sia la sede per approfondire gli sviluppi del dibattito sull'Unione politica, non possiamo non sottolineare lo stretto legame esistente tra un simile sviluppo e la possibilità di giungere realmente ad un sistema intelligence integrato.

<sup>26</sup> Radicalisation Awareness Network (RAN), <[http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation\\_awareness\\_network/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm)>.

<sup>27</sup> European Commission, Fact Sheet, <[http://europa.eu/rapid/press-release\\_MEMO-16-2118\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-2118_en.htm)>.





L'intelligence e le informazioni da essa veicolate rappresentano il vero *core business* del potere, il suo nucleo indispensabile, la cui cessione non può essere prevista senza che si incorra nel rischio oggettivo (e insostenibile) di mettere a rischio il supremo interesse nazionale di ciascuno Stato coinvolto. Lasciano di conseguenza il tempo che trovano i richiami non contestualizzati ad un'integrazione piena, che risulta, allo stato attuale, evidentemente non realizzabile e ampiamente osteggiata in seno alla comunità intelligence.

Il "grande disegno" di costituire in seno al Vecchio Continente un'agenzia che riproduca la struttura organizzativa delle grandi agenzie statunitensi (CIA, FBI, NSA) risulta al momento una chimera scarsamente impiegabile anche per scopi politici personalistici. Una simile struttura non potrebbe vedere la luce in assenza di integrazione politica, e il prestigio e la valutazione di fattibilità del progetto non potrà certo ricevere accoglienza positiva finché saranno solo gli Stati con capacità di

intelligence evidentemente limitate a chiederne l'attenzione.

In secondo luogo non è ancora sufficientemente chiaro quali problemi un'eventuale agenzia intelligence europea dovrebbe fronteggiare. In mancanza di unità di intenti politici la definizione del fabbisogno informativo subirebbe inevitabilmente il rischio di ampia inefficienza e inefficacia legato all'impossibilità di definire con chiarezza il focus su cui centrare le attività. Appare inoltre assai poco plausibile che i Paesi europei, già ampiamente restii a condividere informazioni con *partner* decennali, decidano di cooperare pienamente con una nuova struttura di cui sarebbero, per altro, da definire gli indirizzi e le posizioni di preminenza politica. La creazione di strutture di sicurezza nazionale rimane tutt'ora campo di competenza esclusiva dei singoli Stati membri, di conseguenza un progetto di agenzia unica europea non potrebbe prescindere da un preventivo sconvolgimento normativo europeo capace di realizzare la piena integrazione politica.

Ciò non significa che ulteriori progressi in campo di integrazione intelligence non siano realizzabili. Essi sono al contrario ampiamente auspicati da più parti e potrebbero certamente essere realizzati adottando modelli diversi dall'Agenzia Unica che siano più compatibili con le caratteristiche intrinseche dell'Unione.

A riguardo va in primo luogo considerato come il sistema intelligence europeo (e i suoi eventuali sviluppi) non possa essere paragonato a un servizio intelligence nazionale. Esso si configura al contrario come attore atipico la cui necessità di raccogliere informazioni per i propri decisori a Bruxelles viene affiancata dal compito di supportare le politiche di sicurezza degli Stati membri. Una base informativa comune e utile a ciascuno dei decisori nazionali e gli eventuali benefici economici che l'integrazione potrebbe in futuro comportare, rappresenterebbero in tal senso un forte incentivo per ridurre le resistenze dei singoli Stati ad una maggiore integrazione.

Ulteriore elemento che potrebbe facilitare il progresso di interazione riguarda l'ampia

esistenza, in seno a ciascuna intelligence nazionale, di accordi di cooperazione bilaterali e la già piena comprensione dei benefici che - con qualche accortezza - essi possono garantire. Se si riuscissero a identificare interessi comuni, il perseguimento di tali interessi in piccoli gruppi omogenei per finalità potrebbe ampiamente favorire l'*information sharing* e garantire - qualora ce ne sia la possibilità - una successiva condivisione parziale dei risultati raggiunti all'interno dei forum europei multilaterali.

Si segnala infine come il grande numero di informazioni già presenti e raccolte all'interno dell'UE da ciascuno Stato membro potrebbe, al pari di quanto avviene nei sistemi intelligence nazionali più efficienti, essere impiegato in modo più efficiente per portare alla creazione di un approccio sistemico capace di sfruttare dati già disponibili (e non dispendiosi in termini di restrizione delle libertà politiche o di risorse economiche da spendere) per ottenere ampi benefici in termini di contrasto alla minaccia e garanzia della sicurezza.

L'Unione Europea dovrebbe di conseguenza sfruttare la sua peculiarità di sistema ibrido nazionale/transnazionale ed espandere la sua capacità di raccolta ed elaborazione dei numerosi dati già disponibili e provenienti tanto dai singoli Stati membri, quanto dalla raccolta informativa su fonte aperta.

Se un modello di agenzia unica che ricalchi quello statunitense è, come già detto, assolutamente irrealizzabile dato l'attuale stato di integrazione politica europea, un giudizio di maggiore fattibilità potrebbe al contrario riguardare la possibilità di replicare in campo europeo il modello anglosassone dei *Five Eyes*<sup>28</sup>. Dall'accordo UKUSA del 1946 desecretato nel 2010 è possibile individuare alcune linee guida del modello segnalato. L'accordo regola «la raccolta, la produzione e la disseminazione delle informazioni derivanti dalle comunicazioni di altre nazioni» e prevede

---

<sup>28</sup> La nascita del sistema dei *Five Eyes* si riconduce generalmente al patto UKUSA siglato nel 1946.

lo scambio dei risultati derivanti da attività di raccolta e analisi del traffico di comunicazione; acquisizione di documenti ed equipaggiamenti per le comunicazioni; criptoanalisi; acquisizione di informazioni su organizzazioni, pratiche e procedure. Si prevede inoltre che lo scambio avvenga senza restrizioni eccetto quelle ritenute assolutamente necessarie; si sottolinea inoltre l'auspicio che tali eccezioni vengano ristrette il più possibile.

Il modello *Five Eyes* presenta profili di interesse anche rispetto alla precisa divisione delle competenze tra i Paesi coinvolti; tale divisione, stando a quanto si legge nei documenti desecretati, era effettuata per aree geografiche e prevedeva che ciascun Paese monitorasse in modo prioritario determinate aree del pianeta per poi avviare la condivisione con i *partner*. Una divisione simile permetterebbe di ottenere quei vantaggi competitivi di cui abbiamo già accennato, e potrebbe costituire un ottimo strumento di cooperazione anche in ambito europeo. È evidente che il principale problema che potrebbe presentarsi (problema che per altro non ha mancato di manifestarsi anche all'interno dei *Five Eyes*) riguarderebbe il rischio di sovrapposizione di interessi strategici, di carattere prevalentemente economico, riguardanti la medesima area geografica. Alcune recenti vicende hanno ampiamente evidenziato il grado di conflittualità politico-economica che può presentarsi anche tra alleati europei e un'integrazione su modello anglosassone dovrebbe necessariamente tenere conto di questo elemento e sviluppare adeguati strumenti e accortezze per "contenere" o ridurre per quanto possibile il problema.

Si segnala per altro come la recente decisione britannica di lasciare l'UE potrebbe avere come conseguenza un maggiore rafforzamento dell'intesa politica tra i ventisette Paesi che permangono nell'Unione. La Gran Bretagna, tanto in tema di cooperazione intelligence, quanto rispetto alle sue future prospettive politiche globali, sembra destinata ad avvicinarsi nuovamente - e in modo più strutturato - all'alleato statunitense. L'Europa

contestualmente potrebbe sfruttare l'occasione del Brexit per ridurre i propri attriti interni e per calmierare gli elementi di sovrapposizione e contrasto strategico che in passato sono dipesi ampiamente anche dalle scelte politiche britanniche.

Quale che sia l'evoluzione dell'*information sharing* e della cooperazione intelligence europea, ciò che è ormai evidente è l'importanza e il vantaggio che ciascun Paese potrebbe ottenere da un approccio sistemico capace di sfruttare le risorse e le informazioni esistenti, le strutture dell'Unione, le specializzazioni dei Paesi membri e i partenariati con le diverse aziende private di grande dimensione che sono già a vario titolo incluse nella sfera di influenza europea.

Un approccio simile può non richiedere necessariamente nell'immediato ulteriori sforzi legislativi e potrebbe consentire, a partire dagli elementi già presenti e senza sacrificare l'interesse nazionale degli Stati coinvolti, una migliore elaborazione delle informazioni disponibili e una più efficiente strategia di reazione alla minaccia tanto sui singoli territori nazionali, quanto a livello comunitario.