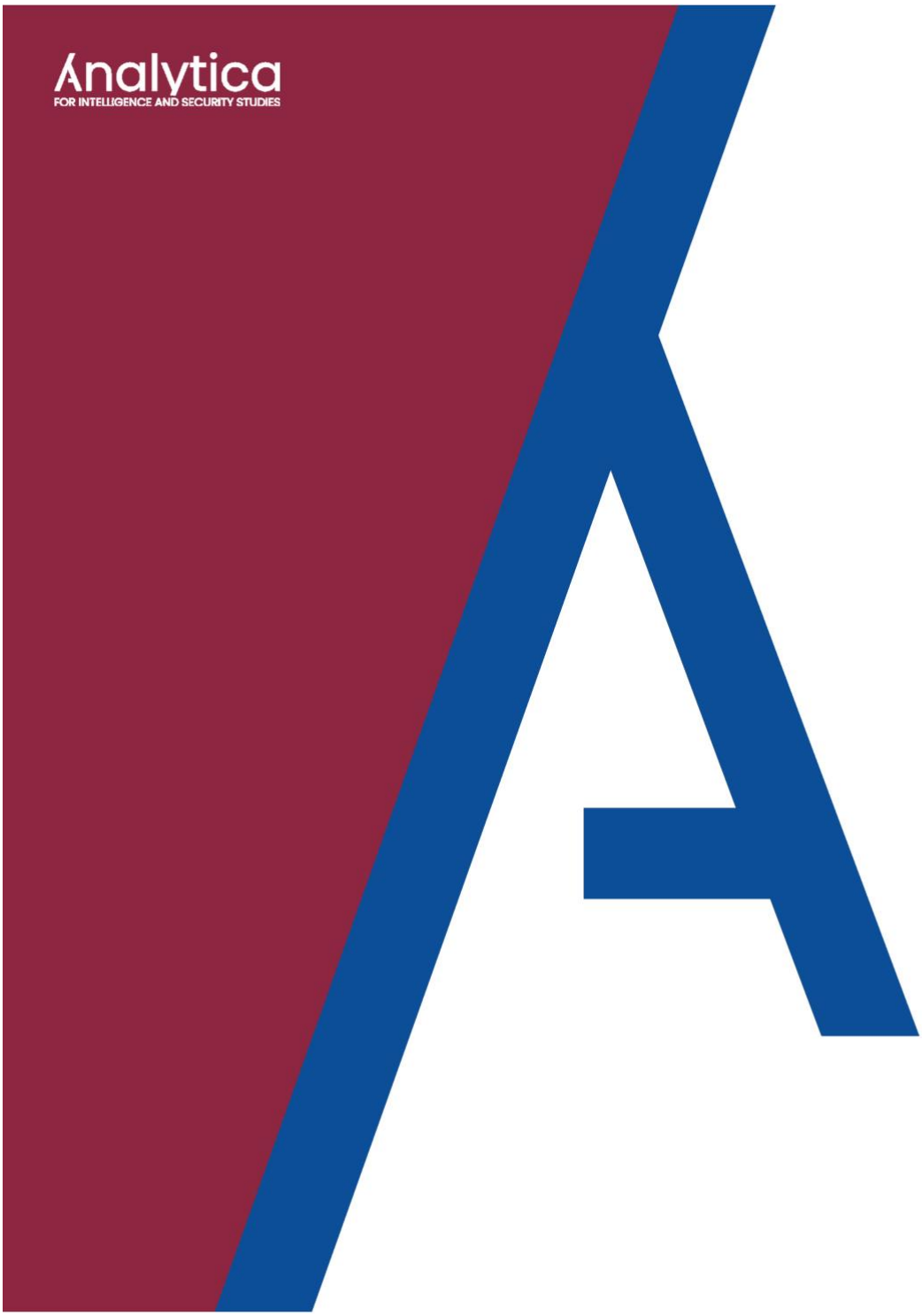

L’evoluzione dell’intelligence italiana tra vecchie e nuove minacce.

Iavarone Luca

Analytica for intelligence and security studies

Paper Intelligence
ISSN 2724-3796

L'evoluzione dell'intelligence italiana tra vecchie e nuove minacce.

Iavarone Luca
(Tirocinante Università di Bologna - International Relations – Crime Justice and Security)

Correzioni e revisioni a cura del Direttore del Dipartimento Intelligence Dott.

CONIO Giovanni.

Torino, maggio 2021

Introduzione

Con la legge n. 16761 del 20 marzo 1854 nacque, all'interno dello Stato Maggiore dell'Esercito Sabaudo, la sezione dei servizi segreti italiani. Sin da allora la sua organizzazione è stata soggetta a numerose evoluzioni, volte all'adattamento ai nuovi scenari mondiali, che ad oggi non si sono ancora fermate. Questa analisi è stata ispirata dalla consapevolezza che questi cambiamenti si rendono necessari per mantenere un alto livello di efficienza operativa e per non essere surclassati, né da un punto di vista tecnologico né da quello strategico. Si ritiene importante, quindi, individuare quali potrebbero essere le modificazioni organizzative che l'Intelligence italiana potrebbe adottare per far fronte alle nuove sfide globali, e contrastare in una maniera adeguata quelle che sono le nuove minacce e i nuovi attori con cui conviviamo.

Nella prima parte verrà analizzata la struttura del "Sistema di Informazione per la Sicurezza della Repubblica" (SISR) partendo, a premessa, dall'organizzazione dei "Servizi" delineata dalla legge n. 801 del 1977, che sarà poi comparata con l'organizzazione assunta con la legge n. 124 del 2007. Verranno quindi evidenziate le differenze tra le due leggi da un punto di vista "strutturale" e "operativo" per evidenziare come i servizi si siano adattati ad un nuovo contesto internazionale portatore di minacce per le quali la legge n.801, ratificata durante la guerra fredda, non era in grado di far fronte.

Una volta chiarito l'ambito organizzativo del Comparto d'intelligence, saranno successivamente esaminate le minacce, storiche e recenti, dalle quali lo Stato italiano deve tutelarsi. Verranno quindi elencate le sfide verso cui è rivolta l'attività informativa dell'Intelligence italiana sia a livello interno, che al di fuori del territorio nazionale. Questa parte si svilupperà a partire da un'analisi delle "Relazioni sulla politica dell'informazione per la sicurezza" del 2019 e del 2020 che vengono presentate annualmente al Parlamento dai Servizi. Col passare degli anni il quadro delle minacce esistenti non ha mai subito sostanziali variazioni, e ancora oggi lo stato convive con esse cercando il modo migliore per contrastarle e limitarne i danni. Il forte impatto dell'emergenza pandemica del 2020 non ha solo colpito le economie mondiali e le relazioni internazionali, ma ha avuto conseguenze rilevanti anche su tutte le minacce preesistenti, aggravandole o modificandone l'operatività. Proprio per questo motivo, la crisi sanitaria non sarà in questa analisi (così come avviene nelle due relazioni prese in riferimento) presa in esame come nuova minaccia, ma verrà piuttosto analizzata come "prospettiva" per verificare se e come le minacce sono evolute, aumentando così il loro grado di pericolosità.

I temi fin qui trattati, saranno quindi ripresi e analizzati però dal punto di vista di un altro sistema statale: quello spagnolo. Verranno quindi descritti l'assetto organizzativo del Centro Nacional de

Inteligencia (CNI) e come esso risponde alle minacce individuate dal Governo spagnolo. Questo studio comparativo permetterà di mettere in risalto le differenze tra i due sistemi, quello italiano e quello iberico, da un punto di vista organizzativo e legislativo.

Le considerazioni finali ci porteranno a delineare le possibili modifiche o strategie che il Comparto intelligence nazionale dovrebbe o potrebbe implementare per adempiere efficacemente ai propri compiti istituzionali. Discutendo e comprovando il grado di necessità e l'efficacia di queste misure verranno infine individuate (se esistenti) le variazioni organizzative, ad esempio l'introduzione di nuovi reparti e assetti specialistici, o strategiche, come un maggiore impulso nella formazione sempre più orientata ai recenti sviluppi tecnologici.

1. Il sistema informativo nazionale – come si giunge alla struttura attuale

Il **Sistema di informazione per la sicurezza della Repubblica (SISR)**, istituito con la promulgazione dalla legge n. 124 del 2007 che ne delinea responsabilità e compiti, è costituito da *"l'insieme degli organi e delle autorità che, nel nostro Paese, hanno il compito di assicurare le attività informative allo scopo di salvaguardare la Repubblica dai pericoli e dalle minacce provenienti sia dall'interno sia dall'esterno"* (Chi siamo, 2021). Per meglio comprendere questo sistema, si ritiene opportuno partire dall'organizzazione che l'ha preceduta, e dopo un sintetico riepilogo degli organi istituiti dalle due leggi, sarà definito un confronto tra i due sistemi, sottolineandone le differenze organizzative e funzionali.

Inoltre, considerando che dalla data della sua promulgazione a oggi la legge n.124, è stata modificata in molteplici occasioni per ragioni sia politiche che strategiche, persiste l'esigenza di un riordinamento giuridico delle principali evoluzioni che hanno interessato la suddetta legge, con conseguenti modifiche nell'assetto organizzativo del sistema. Verranno quindi brevemente riportate le citate modifiche, seguendo non un ordine cronologico che risulterebbe di difficile fruizione, ma inserendo la loro descrizione nel paragrafo di confronto tra gli organi delle due leggi analizzate. Queste modifiche faranno esclusivamente riferimento al primo dei sei capi[1] della legge e agli attori che hanno visto maggiormente mutate le proprie competenze e autonomie, tralasciando quindi le modifiche ai successivi cinque per concentrare l'analisi sulla struttura odierna del SISR.

2.1. Legge 801/77 – I "Servizi" di informazione

[1] Capo 1: struttura del sistema d'informazione per la Repubblica; capo 2: disposizioni organizzative; capo 3: garanzie funzionali, stato giuridico del personale e norme di contabilità; capo 4: controllo parlamentare; capo 5: disciplina del segreto; capo 6: disposizioni transitorie e finali

Nel 1977 la Commissione speciale per la riforma dei servizi promulgò la legge n. 801 del 24 ottobre che istituì una nuova organizzazione e un nuovo funzionamento per la politica d'informazione e sicurezza (*Grafico 1*), la cui responsabilità e direzione vennero affidate al Presidente del Consiglio dei Ministri (da qui in avanti "Presidente"). Il Presidente inoltre presiedeva il **Comitato Interministeriale per le Informazioni e la Sicurezza (CIIS)**, organo istituito con funzioni propositive e di consulenza per coadiuvare il processo di definizione degli indirizzi e degli obiettivi da perseguire in materia di politica informativa e di sicurezza. Oltre al Presidente ne erano membri anche i ministri di Affari Esteri, Interni, Grazia e Giustizia, Difesa, Industria e Finanze, ai quali si potevano occasionalmente aggregare, se invitati dal Presidente, anche i Direttori dei Servizi (SISMI e SISDE, che vedremo in seguito).

Il **Comitato Esecutivo per i Servizi di Informazione e di Sicurezza (CESIS)**, fu invece l'organo di collegamento istituito come responsabile del passaggio di informazioni e analisi dai Servizi al Presidente. Ulteriore responsabilità affidata al CESIS erano i rapporti con i servizi di informazione e sicurezza degli altri stati, i cosiddetti "servizi collegati".

La legge 801 istituì, inoltre, due organi responsabili concretamente dello svolgimento delle operazioni:

- Il **Servizio per le Informazioni e la Sicurezza Militare (SISMI)**, incaricato della protezione dello Stato da ogni pericolo sul piano militare e dipendente dal Ministero della difesa che ne stabiliva l'ordinamento e ne curava le attività;
- Il **Servizio per le Informazioni e la Sicurezza Democratica (SISDE)**, incaricato dei *"compiti informativi e di sicurezza per la difesa dello Stato democratico e delle istituzioni poste dalla Costituzione a suo fondamento contro chiunque vi attenti e contro ogni forma di eversione"* (L. 801/1977). Come per il SISMI, anche il SISDE era dipendente da un ministero, che in questo caso era però quello dell'Interno.

Infine, il **"Comitato Parlamentare di Controllo sui Servizi Segreti" (COPACO)**, fu l'organo "democratico" incaricato di esercitare il controllo sui servizi segreti in merito all'applicazione dei principi stabiliti dalla legge n. 801.

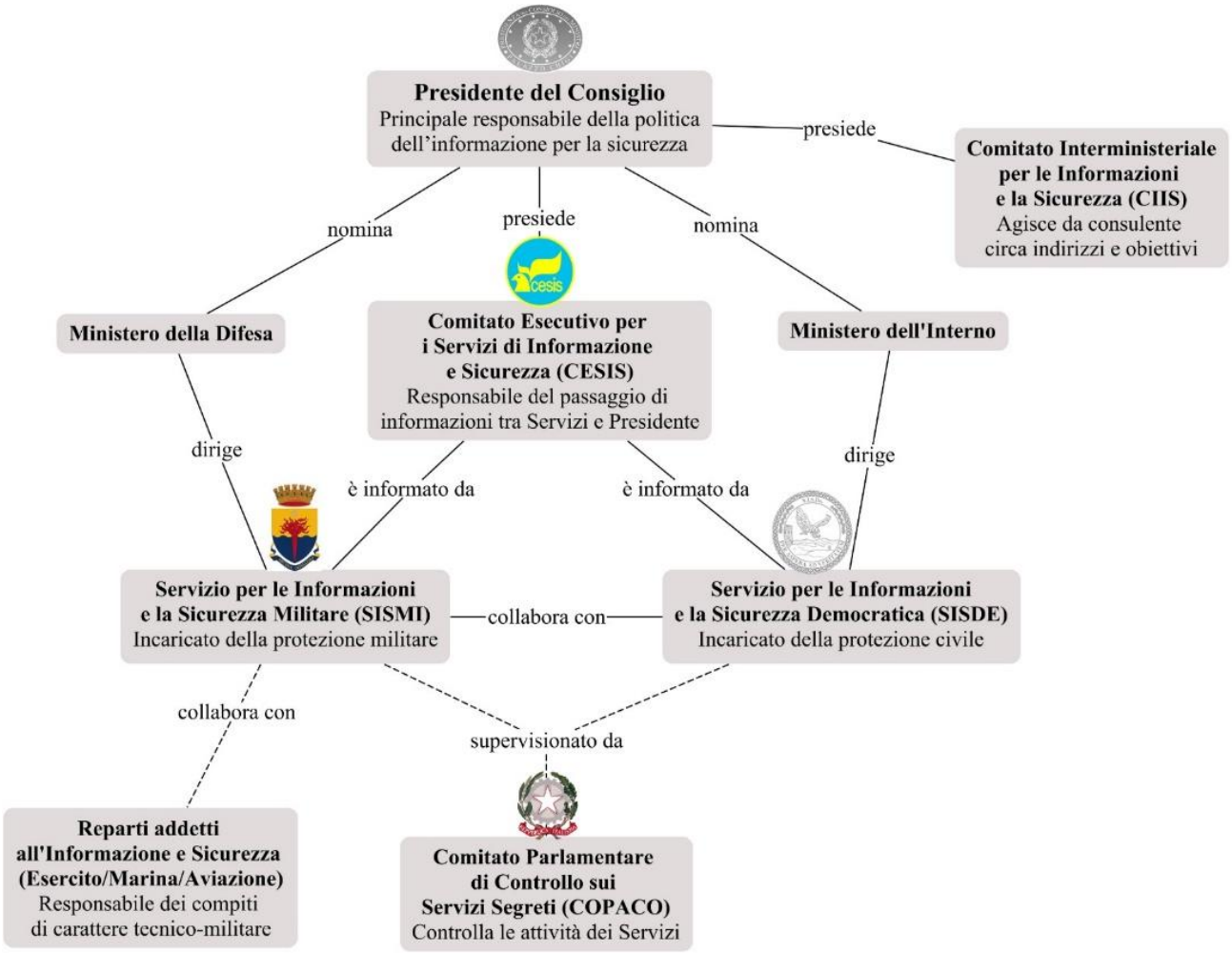

Grafico 1: Organizzazione della politica di informazione e sicurezza sancita dalla legge 801

2.2. Legge 124/07 – Il "Sistema" di informazione

Con la legge n° 124 del 3 agosto 2007, i Servizi Segreti italiani subirono una modifica nella struttura e nei compiti, giungendo così all'organizzazione odierna, secondo la quale il SISR si avvale della cooperazione di cinque attori principali (*Grafico 2)*.

In primo luogo, il Presidente è il principale responsabile della politica dell'informazione per la sicurezza, in particolar modo per ciò che concerne il suo coordinamento e la sua direzione. In virtù del ruolo istituzionale e delle responsabilità a cui esso è vincolato, concernenti la politica dell'informazione per la sicurezza e i lavori della compagine governativa, il Presidente gode della possibilità di nominare discrezionalmente una Autorità Delegata. Questa figura, individuata in un Sottosegretario di Stato o in un Ministro senza portafoglio, può assumere tutte le competenze del Presidente in materia di politica dell'informazione per la sicurezza, eccetto quelle di natura

esclusiva[2]. Questa divisione dei poteri, che agevola lo svolgimento dei lavori, è però subordinata ad un costante dialogo tra Autorità delegata e Presidente, in ragione del fatto che quest'ultimo può in qualunque momento ritirare la delega concessa al primo, in caso lo ritenga necessario. L'autorità delegata (se nominata) presiede il Collegio di vertice (formato dai direttori di DIS, AISE ed AISI, definiti in seguito) e fa parte del **Comitato Interministeriale per la Sicurezza della Repubblica (CISR)**, a sua volta presieduto dal Presidente.

Il CISR è l'organo responsabile di consulenza, proposta e delibera circa indirizzi e finalità della politica dell'informazione per la sicurezza. Oltre al Presidente e all'Autorità delegata, ne sono membri anche il Direttore del DIS in qualità di segretario, e i ministri di Affari Esteri, Interno, Difesa, Giustizia, Economia e Sviluppo economico.

Il **Dipartimento delle Informazioni per la Sicurezza (DIS)** è l'organo che si occupa di programmare la ricerca informativa, l'analisi e l'attività operativa delle Agenzie (AISI e AISE). Il DIS si compone dell'Ufficio Centrale Ispettivo (UCI), l'Ufficio Centrale degli Archivi (UCA), l'Ufficio Centrale per la Segretezza (UCSe) e la Scuola di Formazione.

Il **Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR)** è un organo bicamerale predisposto dalla legge n. 124 al controllo sistematico delle attività del SISR nel rispetto della Costituzione e delle leggi.

Dispone di poteri di controllo che gli permettono non solo l'accesso a documenti e informazioni provenienti sia dal SISR che da altri organi, ma detiene anche la possibilità di svolgere audizioni sia di membri del SISR (Presidente, Autorità delegata, ministri del CISR, direttori di DIS, AISE e AISI) che di persone esterne in grado di fornire informazioni utili. Al comitato sono attribuite inoltre funzioni consultive, ed il suo parere (obbligatorio ma non vincolante) viene richiesto in merito agli schemi dei regolamenti di attuazione della legge di riforma dei servizi di sicurezza.

Il COPASIR può richiedere al Presidente l'avvio di inchieste interne per verificare la legittimità delle condotte dei membri del sistema e in caso di violazioni delle norme sulle attività di informazione per la sicurezza, riferisce ai Presidenti delle Camere e al Presidente.

Ogni sei mesi il comitato riceve dal Presidente la relazione sulle attività dei servizi, recante un'analisi della situazione e dei pericoli per la sicurezza. Annualmente invece, è Il Comitato a dover presentare una relazione al Parlamento in merito alle attività svolte e per formulare proposte e

[2] Le competenze di natura esclusiva del Presidente sono tre: Tutela e conferma dell'opposizione del segreto di stato; Nomina dei direttori di DIS, AISE e AISI; Definizione delle risorse finanziarie necessarie al funzionamento dei tre enti sopraindicati.

presentare pareri.

L'**Agenzia Informazioni e Sicurezza Esterna (AISE)** è l'organo operativo preposto alla ricerca e all'elaborazione delle informazioni utili alla protezione da minacce di origine estera. Dato questo suo compito, le operazioni che conduce si svolgono esternamente ai confini nazionali, ad esempio per contrastare attività di spionaggio e di contro-proliferazione di materiali strategici volte a danneggiare gli interessi politici, militari, economici, scientifici e industriali dell'Italia.

L'**Agenzia informazioni e sicurezza interna (AISI)** è l'organo che opera da controparte dell'AISE, svolgendo gli stessi compiti all'interno del territorio statale. Ha quindi il dovere di ricercare ed elaborare tutte le informazioni utili per difendere la sicurezza e gli interessi statali da ogni minaccia di origine interna, sia essa un'attività eversiva, criminale, terroristica o di spionaggio.

Sia AISE che AISI rispondono al Presidente e sono incaricati di informare rapidamente e con continuità il Ministro dell'Interno, degli Affari Esteri e della Difesa, per le materie di rispettiva competenza.

Pur non facendo propriamente parte del SISR, la legge n. 124 fa riferimento al rapporto tra il Sistema e il **Reparto Informazioni e Sicurezza (RIS)** dello Stato Maggiore della Difesa**.** L'art. 8 disciplina, infatti, l'esclusività delle funzioni attribuite al DIS, all'AISE e all'AISI, rimarcando come il RIS sia un organo di intelligence di carattere tecnico-militare. Sono parte delle sue mansioni la definizione delle linee di indirizzo e degli obiettivi relativi allo sviluppo della ricerca informativa nel settore tecnico-militare, per le attività di sicurezza e di polizia militare in ambito Forze Armate. Opera principalmente nei teatri operativi o nelle zone a rischio dove sono impiegati militari italiani.

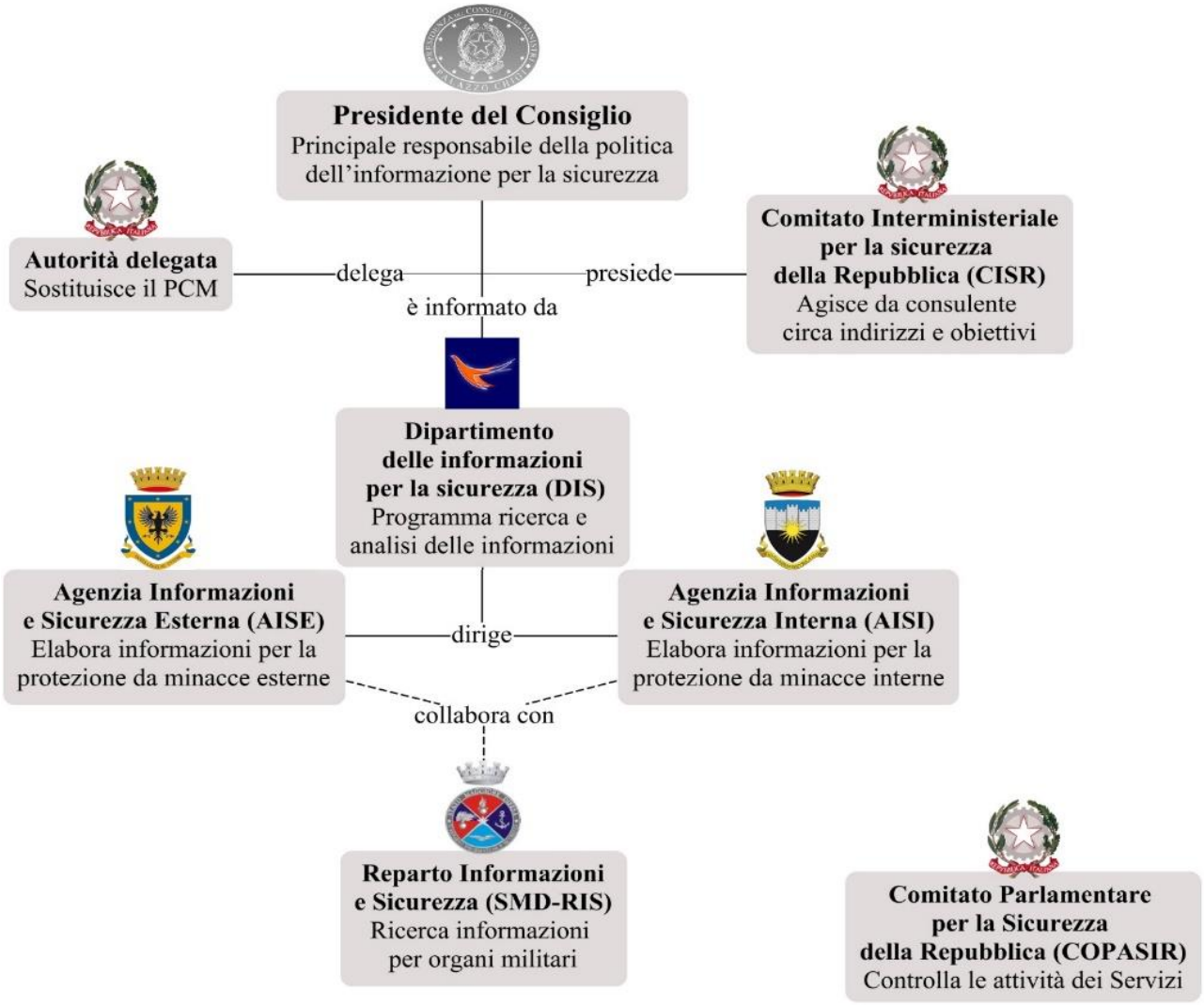

Grafico 2: Organizzazione della politica di informazione e sicurezza sancita dalla legge 124

2.3. 801 vs 124. Due leggi a confronto

Per quanto riguarda la figura del Presidente, ad esso è sempre stata conferita la responsabilità di direzione della politica dell'informazione per la sicurezza e dell'apposizione, la tutela e la conferma dell'opposizione del segreto di stato (Il segreto di Stato, 2021). Con la legge n. 124 gli sono state però anche attribuite nuove competenze di natura esclusiva che accentuano maggiormente l'importanza della sua carica. Egli è infatti oggigiorno responsabile anche della nomina dei direttori di DIS, AISE e AISI, e della definizione delle risorse finanziarie necessarie al funzionamento dei tre enti sopraindicati.

La prima legge ad apportare delle modifiche rilevanti al sistema istituito dalla legge n.124 è stata la legge n. 133 del 7 agosto 2012. All'art. 1 essa accorda al Presidente la possibilità, sentito il CISR, di impartire a DIS, AISE e AISI direttive volte a *"rafforzare le attività di informazione per la*

protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali" (L. 133/2012).

Anche l'ultima legge in materia di intelligence, la n. 198 dell'11 dicembre 2015 art. 7-bis, ha riportato al suo interno quattro disposizioni che hanno, in parte, incrementato le competenze del Presidente:

- Il comma 1 permette al Presidente di emanare, acquisito il parere del COPASIR, *"disposizioni per l'adozione di misure di intelligence di contrasto, in situazioni di crisi o di emergenza all'estero che coinvolgano aspetti di sicurezza nazionale o per la protezione di cittadini italiani all'estero, con la cooperazione di forze speciali della Difesa con i conseguenti assetti di supporto della Difesa stessa"* (L. 198/2015).
- Il comma 2 dispone che il Presidente del Consiglio debba informare Comitato parlamentare per la sicurezza di tutte le misure di intelligence a cui ci si riferisce nel comma 1.
- Il comma 3 disciplina le disposizioni che si applicano al personale delle Forze armate impiegato nell'attuazione delle attività di cui al comma 1 del presente articolo.
- Il comma 4 definisce invece i crimini per i quali il comma 3 non trova applicazione.

Oltre alle modifiche alle competenze del Presidente, la legge del 2007 istituì a suo supporto, la figura dell'Autorità Delegata, assente nel precedente ordinamento. Originariamente la legge 124 all'art. 3 comma 2 prevedeva l'impossibilità per l'Autorità Delegata di *"esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei Ministri a norma della presente legge"* (L. 198/2015). Con la legge n. 121 del 14 luglio 2008 art.1 comma 21 il suddetto comma venne però momentaneamente abrogato, riconducendone la motivazione alla *"relazione al vincolo quantitativo per il numero dei componenti del Governo, e all'esigenza di assicurare in ogni caso l'efficienza della struttura del Governo"* (A.C. 5284). In questo modo era potenzialmente permesso all'Autorità Delegata di esercitare maggiori poteri o di ricoprire ulteriori incarichi di Governo. Tuttavia, l'art. 2 comma 1 della legge n. 133 del 2012 reinserisce il comma precedentemente abrogato, ristabilendo la norma iniziale.

Nel passaggio tra la legge n. 801 alla 124, il CIIS venne riformato nel CISR, mantenendo le sue funzioni di definizione degli obiettivi della politica dell'informazione per la sicurezza, alle quali però vennero aggiunte la ripartizione delle risorse finanziarie di DIS, AISE e AISI e il compito di individuare il fabbisogno informativo necessario a ciascun Ministero. La sua composizione rimase pressoché invariata con il solo inserimento permanente del direttore del DIS.

Il CESIS fu invece sostituito nel 2007 dal DIS che, dotato di maggiori competenze e responsabilità rispetto al suo predecessore, permise di agevolare i lavori di AISI e AISE migliorandone

l'operatività. Infatti, grazie alla sua nuova organizzazione interna in uffici, oltre al ruolo di collegamento tra servizi e Presidente al DIS vennero attribuiti numerosi compiti, tra i quali:

- tutela amministrativa del segreto di Stato;
- gestione dei dati in possesso alle Agenzie;
- controllo giuridico sulle operazioni di AISE e AISI;
- addestramento del personale del DIS e delle Agenzie;
- promozione della cultura della sicurezza;
- trasmissione al Presidente del Consiglio dei Ministri delle analisi prodotte dal Sistema in base alle operazioni di AISE e AISI.

L'art. 3 della legge n. 133 del 7 agosto 2012 dispose inoltre che il DIS:

- è responsabile del coordinamento delle attività di ricerca informativa al fine di rafforzare la protezione cibernetica e la sicurezza informatica nazionali;
- Approva annualmente il piano annuale delle attività dell'ufficio ispettivo previo parere del Comitato Parlamentare;
- gestisce unitariamente gli approvvigionamenti e i servizi logistici comuni del SISR.

Il primo comma di quest'articolo si è rivelato essere solo il primo di una lunga serie di interventi volti a rafforzare le capacità statali nel campo della protezione cibernetica ed informatica. Ad esso sono seguiti il DPCM del 27 gennaio 2014 con il quale è stato adottato il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", una Direttiva del 1° agosto 2015 sullo stesso tema e il DPCM del 31 marzo 2017 che ha aggiornato il Quadro strategico precedentemente approvato.

Il COPACO è stato invece sostituito dal COPASIR che nel corso degli anni ha visto incrementare esponenzialmente i suoi compiti, trasformandosi da organo consultivo di rilevanza quasi formale, ad un sostanziale organo di controllo. Questa "facoltà" di controllo di cui disponeva il COPACO è stata rafforzata, permettendo non solo l'accesso a documenti e informazioni provenienti sia dal SISR che da altri organi, ma anche di svolgere audizioni sia di membri del SISR (Presidente, Autorità delegata, ministri del CISR, direttori di DIS, AISE e AISI) che di persone esterne al Sistema in grado di fornire informazioni utili. Al nuovo comitato sono state inoltre attribuite funzioni consultive, ed il suo parere (obbligatorio ma non vincolante) viene richiesto in merito agli "*schemi dei regolamenti di attuazione della legge di riforma, su quelli di modifica e su ogni altro schema di decreto concernente l'organizzazione e lo stato del contingente speciale di DIS, AISE e AISI"* (Il controllo parlamentare, 2021).

Tra i nuovi compiti del COPASIR l'art. 5 della legge n. 133 del 2012 dispose l'inserimento della responsabilità di accertamento dell'esclusività delle funzioni attribuite al DIS, all'AISI e all'AISE, ossia verificare che organismi non appartenenti al SISR, operino nel rispetto della legge, affinché non si determinino sovrapposizioni o interferenze con le attività svolte dai Servizi di intelligence. I successivi articoli della stessa legge avevano tutti come obiettivo il rafforzamento dei poteri di controllo del COPASIR. Essi prevedono ad esempio:

- una maggioranza dei due terzi per la deliberazione dello svolgimento di indagini sulla rispondenza dei comportamenti di appartenenti ai Servizi ai compiti istituzionali previsti dalla legge;
- l'introduzione dell'obbligo di parere del COPASIR sulle delibere assunte dal Comitato Interministeriale per la Sicurezza della Repubblica sulla ripartizione delle risorse finanziarie tra DIS, AISE e AISI e sui relativi bilanci preventivi e consuntivi, nonché sul piano ispettivo annuale;
- la possibilità di richiedere al Presidente del Consiglio di disporre lo svolgimento di inchieste interne volte ad accertare la correttezza di condotte poste in essere da appartenenti o ex appartenenti agli organismi di informazione;
- l'obbligo di fornire al COPASIR, in caso di conferma dell'opposizione del segreto di Stato, non solo delle ragioni essenziali ma anche l'intero quadro informativo in possesso del Governo.

Radicalmente diversa dalla ripartizione di competenze tra SISMI e SISDE è l'organizzazione dei nuovi organi nati per sostituirli che si dividono tra sicurezza interna, **Agenzia Informazioni e Sicurezza Interna (AISI)**, ed esterna, **Agenzia Informazioni e Sicurezza Esterna (AISE)**. Tale suddivisione di compiti e responsabilità fa assumere al Sistema un assetto più vicino a quello delle principali Agenzie europee, improntato su una divisione basata sulle competenze e non più su una distinzione tra servizi civili e militari[3]. Il SISMI, incaricato della protezione dalla minaccia militare, è stato quindi sostituito dall'AISE proposto per il contrasto a minacce di origine esterna; il SISDE, delegato alla sicurezza civile, è stato rimpiazzato dall'AISI, preposto alla sicurezza interna. Questa modifica è stata ritenuta necessaria per trovare una soluzione alla sovrapposizione che spesso si verificava tra le operazioni di SISMI e SISDE che agivano entrambi sia all'estero che all'interno dei confini nazionali.

[3] Inghilterra: MI5 (Military Intelligence, sezione 5) - interno; MI6 (Military Intelligence, sezione 6) - esterno;
Germania: Ufficio Federale per la Protezione della Costituzione – interno; Servizio Federale d'Informazioni – esterno;
Francia: Direction centrale du renseignement intérieur – interno; Direction générale de la sécurité extérieure – esterno;

A differenza degli organi che li hanno preceduti, che erano dipendenti dal Ministero della Difesa (SISMI) e da quello dell'Interno (SISDE), sia AISE che AISI non sono direttamente dipendenti da specifici ministeri bensì rispondono al Presidente, anche se incaricati di informare rapidamente e con continuità il Ministro dell'Interno, degli Affari Esteri e della Difesa, per le materie di rispettiva competenza.

Le competenze dell'AISE sono state incrementate dalla legge n. 43 del 17 aprile 2015 (art. 8 comma 2-bis), che ha disposto l'ampliamento della portata dei mezzi funzionali alla ricerca di informazioni permettendo così l'utilizzo di assetti di ricerca elettronica, seppur esclusivamente verso l'estero. In questo modo viene autorizzato l'utilizzo da parte dell'AISE di una serie di installazioni presenti sul territorio nazionale, utilizzabili per intercettazioni di segnali e comunicazioni provenienti dall'estero. Viene però anche stabilito che *"Il Presidente del Consiglio dei Ministri informa il Comitato Parlamentare per la Sicurezza della Repubblica con cadenza mensile circa le attività di ricerca elettronica"* (L. 43/2015).
Anche le collaborazioni del SISR con gli ambienti militari sono cambiate molto nel corso degli anni. La legge n. 801 stabiliva che ciascuna Forza Armata avesse propri Reparti e i propri Uffici addetti all'attività informativa per la sicurezza, con compiti di carattere esclusivamente tecnico-militare e che, ciascuno di questi, collaborasse in stretto collegamento col SISMI. La legge n. 124 stabilì invece che, il neonato **Reparto Informazioni e Sicurezza (RIS)**[4], pur non facendo parte del SISR, agisse in stretto collegamento con l'AISE. Seppur brevemente, il sopracitato articolo è stato oggetto di una delle prime variazioni alla legge n. 124. Il D.Lgs. 15 marzo 2010, n. 66 all'art. 2268, comma 1, numero 1064 ne aveva infatti disposto l'abrogazione. Tuttavia, in seguito al Comunicato 30 settembre 2010, il citato numero 1064 è stato espunto dal precedente decreto-legge, ristabilendo formalmente l'art. 8.

3. Esame delle minacce - Definizione e confronto

Per poter efficientemente valutare se la struttura e l'organizzazione adottate dai nostri servizi siano idonee al contrasto delle minacce, sia "classiche" che "emergenti", è innanzitutto importante cercare di definire alcuni concetti centrali in questa analisi.

Per primo, il "Glossario intelligence – Il linguaggio degli Organismi informativi" edito dal SISR

[4]Nascono nel 1997 in seguito alla promulgazione della Legge n. 25 del 18 febbraio sulla ristrutturazione dei Vertici Militari con la quale vengono sciolti i Servizi Informazioni Operative e Situazione (SIOS) di ciascuna Forza Armata.

definisce la minaccia come "*Fenomeno, situazione e/o condotta potenzialmente lesivi della sicurezza nazionale. Può essere rappresentata dalle attività di stati, di organizzazioni non statuali o di singoli individui. A seconda delle forme di estrinsecazione, degli agenti, del bene aggredito e del contesto viene definita come minaccia criminale, minaccia terroristica, minaccia economica, minaccia transnazionale, etc.*".

Secondo aspetto da prendere in considerazione è definire cosa si intende per "interesse nazionale" e "sicurezza nazionale".

Lo stesso SISR definisce la Sicurezza Nazionale come "*condizione in cui ad un paese risultino garantite piene possibilità di sviluppo pacifico attraverso la salvaguardia dell'intangibilità delle sue componenti costitutive, dei suoi valori e della sua capacità di perseguire i propri interessi fondamentali a cospetto di fenomeni, condotte ed eventi lesivi o potenzialmente tali*.".

Per "interesse nazionale" si intende invece un concetto che risale alla nascita degli Stati, e che ne rappresenta l'identità. Ma se nei secoli passati tale interesse coincideva con quello del sovrano o dell'élite al potere, con l'avvento della Democrazia questo si trasforma in una nozione ben più complessa, che si riferisce agli aspetti economici, politici e culturali dell'intera società. Il Governo non ha solo la "gestione" dell'interesse del Paese, il suo compito è quello di "coordinare e rendere coerenti le azioni dei diversi settori coinvolti".

Nel merito, Giampiero Massolo (già Direttore del DIS) indica "*L'interesse nazionale è ciò che uno Stato non può evitare di perseguire senza creare un danno alla collettività. Spetta ai governi definirne il contenuto. Questi sono responsabili del loro operato di fronte ai Parlamenti e, in ultima analisi, ai cittadini. La definizione in negativo di interesse nazionale si presenta come quella in assoluto più ampia. Consente di ricomprendervi una gamma illimitata di azioni e inazioni delle Autorità di governo, definita solo in base alla loro dannosità rispetto alla condizione pre-esistente. Una definizione in positivo presuppone, invece, delle scelte a monte che portano a restringerne l'ambito, escludendo a priori talune determinazioni governative rispetto ad altre a seconda dei criteri di valutazione assunti. Scegliere ciò che non danneggia significa, nell'attività pratica dei governi, prevenire le minacce e cogliere le opportunità, sulla base delle componenti permanenti e contingenti che definiscono l'interesse nazionale. Tra i fattori immodificabili e costanti nel tempo sono la collocazione geografica di un Paese, la sua storia, la cultura e la tradizione nazionale, la sua articolazione territoriale, le etnie che lo popolano, i livelli diversificati di sviluppo sociale ed economico. Essi coesistono e interagiscono con una pluralità di fattori contingenti, rappresentati da minacce e opportunità*"(L'interesse nazionale, 2021).

Una attenta riflessione circa le condotte che possono, quindi, ledere gli interessi politici, militari, economici, scientifici ed industriali del Paese, consente di determinare un elenco delle minacce da prendere in considerazione. Tra queste possono essere individuate:

- minacce “classiche”, a cui storicamente i reparti di intelligence devono far fronte e che restano attuali grazie alle loro continue evoluzioni;
- minacce “emergenti”, consolidatesi in tempi più recenti spesso a causa della globalizzazione, del progresso tecnologico e di una accentuata mobilità.

Tra le minacce classiche possiamo annoverare:

- **Acquisizione di informazioni**, che può avvenire mediante:
  - raccolta aperta (*overt collection*), che prevede il reperimento di informazioni attraverso lo sfruttamento di fonti aperte (*open sources*).
  - raccolta coperta *(covert collection)*, con la quale le informazioni sensibili, debitamente protette, sono reperite attraverso attacchi intenzionali condotti da assetti altamente specializzati.
- **Sovversione**, effettuata attraverso:
  - diffusione di informazioni devianti;
  - manipolazione segreta di particolari organizzazioni;
  - infiltrazione in organizzazioni locali;
  - arruolamento di persone eversive in qualità di agenti.
- **Sabotaggio**, ovvero distruzione o danneggiamento di infrastrutture o materiale vitale.
- **Terrorismo**, cioè azioni violente di grande impatto psicologico diretto e indiretto.
- **Crimine organizzato**, protratto da organizzazioni strutturate per eseguire attività in grande scala come traffici illeciti che possono destabilizzare l'economia e l’ordine sociale.
- **Operazioni Informative** (INFO OPS), cioè azioni intraprese per influenzare i *decision makers* attraverso un’azione diretta nei confronti delle notizie, dei processi informativi, dei sistemi di Comando e Controllo (C2) e *Communications Information System* (CIS) dell’avversario garantendo, al contempo, lo sfruttamento e la protezione dei propri sistemi informativi e delle proprie notizie.

In questa casistica vanno inoltre considerate le Aeree di crisi, aree di interesse e proiezioni di influenza, nonché la proliferazione di armi di distruzione di massa, tra cui rientrano anche le armi biologiche, minaccia resa attuale dalla recente pandemia di COVID-19 e i relativi sospetti sulla provenienza del virus.

Maggiore attenzione deve essere però riservata a quelle "emergenti", che rischiano di rendere obsoleti i servizi d'intelligence statali se non riformati o aggiornati in tempo. Sono esempi di minacce emergenti:

- **Minaccia cibernetica** (con attacchi principalmente rivolti verso soggetti pubblici)
- **Minaccia alle infrastrutture critiche e assetti strategici**
- **Minaccia ibrida** (campagne disinformative e *fake news* a scopo manipolatore e d'influenza)
- **Immigrazione clandestina**
- **Minaccia approvvigionamento energetico**

Tutte queste forme di minaccia, sia classiche che recenti, possono essere ricondotte a:

- servizi d'intelligence stranieri;
- assetti di sorveglianza, riconoscimento e raccolta di immagini e monitoraggio dello spettro elettromagnetico;
- organizzazioni o gruppi sovversivi e anarchici;
- organizzazioni o gruppi terroristici;
- organizzazioni e gruppi criminali;
- unità militari altamente specializzate come le Forze Speciali (SF).

3.1. Stato delle minacce in Italia

Per un'attenta analisi delle principali minacce contro cui i servizi segreti italiani sono tenuti a far fronte, è importante distinguere tra le minacce classiche, che ancora oggi continuano ad affermarsi come gravi pericoli per la nazione, e le minacce emergenti contro cui si cerca d'implementare rapide soluzioni.

La prima minaccia classica che va ricordata è quella che secondo la Realpolitik è il più grande pericolo per la sicurezza di uno stato: gli altri stati. L'esame delle Relazioni al Parlamento sulla politica dell'informazione per la sicurezza, relative agli anni 2019 e 2020 pubblicate dal Comparto intelligence, ha infatti evidenziato come uno degli sforzi maggiori dei servizi segreti sia infatti comportato dall'attività informativa, rivolta verso tutti quei **paesi, aree di crisi e di interesse** in grado di rappresentare una minaccia, anche solo potenziale, alla sicurezza statale. I servizi segreti italiani si sono infatti impegnati nel salvaguardare gli interessi nazionali in diverse aree del globo, contrastando l'immigrazione clandestina, la minaccia terroristica, e garantendo all'Italia i necessari rifornimenti energetici.

Un'altra delle minacce storiche dell'economia italiana è quella rappresentata dalle **criminalità organizzata**, da sempre oggetto delle indagini dei servizi. Nonostante non possa essere definito un pericolo emergente, deve essere tenuta in considerazione la capacità delle mafie, sia nazionali che estere, di evolversi e adattarsi ai tempi. Alle storiche attività illecite della criminalità organizzata, quali riciclaggio di denaro, contrabbando internazionale ed estorsioni di massa, si devono quindi affiancare al giorno d'oggi quelle azioni rese possibili dalle innovazioni tecnologiche. Esse, infatti, rendono disponibili per i network criminali nuove materie e nuovi spazi attraverso cui ampliare i propri traffici illeciti, come ad esempio la sopracitata tecno-finanza. L'inizio dell'emergenza pandemica ha inoltre comportato per le economie illegali un'occasione per trarre profitto dai piani di rilancio di matrice nazionale ed europea, intercettando questi flussi di denaro. Tutte le organizzazioni criminali si sono infatti dimostrate pienamente capaci di invadere gli spazi dell'economia legale reinvestendo il denaro frutto di attività illecite e inquinando le amministrazioni instaurando ampie reti collusive.

Per quanto il terrorismo sia un fenomeno ricorrente nella storia dell'Italia, più recente è la **minaccia terroristica di matrice jihadista**, oggetto di continuo monitoraggio da parte di AISI e AISE. La gravità di questa sfida è dovuta alla varietà di fattori che la compongono e che influiscono sui metodi e le azioni adottati per combatterla. I servizi, infatti, non hanno solo il dovere di sventare, in collaborazione con le forze di polizia, eventuali attacchi terroristici, ma devono anche cercare di impedire il processo di radicalizzazione caratteristico della matrice jihadista, che assume dimensioni preoccupanti all'interno delle carceri e sugli spazi digitali, e ostacolare il finanziamento delle organizzazioni terroristiche, recentemente dotatosi di strumenti digitali e di tecnofinanza per l'occultamento delle proprie finanze.

L'emergere di **movimenti eversivi** rappresenta una problematica di origine interna, che recentemente è stata interessata dagli effetti della pandemia, che ne ha limitato le potenzialità mobilitative costringendoli a focalizzarsi su propagande online volte a strumentalizzare la crisi sanitaria per guadagnare consensi tra le categorie sociali più in difficoltà tramite campagne di disinformazione e teorie cospirative. Tra i movimenti eversivi la componente più pericolosa è però quella della destra radicale, responsabile di molteplici attentati e mobilitazioni violente originatesi da odio razziale e intolleranza religiosa in risposta ad una presunta islamizzazione dilagante nel paese, anche a causa degli attentati terroristici di matrice jihadista. Secondo il monitoraggio del Comparto d'intelligence la diffusione e la riaffermazione di queste idee sono strettamente collegate all'utilizzo sempre più diffuso dei social network e delle piattaforme digitali che consento a chiunque di attuare una propaganda online in poco tempo e a basso costo.

Tra i pericoli emergenti uno dei più incombenti è rappresentato dalle **minacce all'economia nazionale,** di cui maggiore componente è una sempre più agguerrita competizione interstatale che assume le forme di investimenti esteri, acquisizioni e imposizioni unilaterali di dazi. Ad aggravare il quadro della minaccia economica, gli effetti "secondari" della pandemia da COVID-19, che ha comportato una diminuzione della domanda (sia interna che estera) e inevitabili tensioni sociali, oltre che l'incremento del rischio di manovre ostili nei confronti degli *asset* strategici italiani, tra le quali campagne denigratorie e acquisizioni indebite con conseguente perdita di know how a danno delle imprese nazionali, e trasloco dei centri decisionali e produttivi all'esterno dei confini italiani.

Anche **l'immigrazione clandestina** è oggetto di un attento e continuo monitoraggio da parte del Comparto Intelligence che ne indaga le criticità socioeconomiche e le connessioni con le organizzazioni criminali che la favoriscono. Questi network delinquenziali sono caratterizzati da un elevata capacità di adattamento ai diversi contesti che incontrano, che li rende abili a sfruttare conflitti ed emergenze umanitarie a beneficio dei propri interessi economici, che si rivelano per questo motivo estremamente difficili da contrastare. A questo pericolo si è recentemente aggiunto anche il rischio sanitario legato all'entrata illecita sul territorio nazionale di migranti positivi al Covid-19. In questo contesto, inoltre, i servizi hanno rivelato l'esistenza sui social network di molteplici gruppi e annunci pubblicitari, volti a promuovere questi traffici illegali, sponsorizzando le proprie tratte, diffondendo notizie false in merito ai permessi di soggiorno dei paesi di arrivo.

La **minaccia cibernetica** resta però uno dei pericoli più importanti per il paese, in quanto attraverso i mezzi digitali è possibile attuare operazioni a danno di obiettivi strategici sia pubblici che privati. L'affermarsi della crisi sanitaria ha aggravato ulteriormente questo pericolo esortando il Comparto intelligence a focalizzare le proprie energie nel contrasto di attività illecite, volte a sfruttare il maggiore ricorso al lavoro agile per fini criminali, come il furto di dati sensibili da centri di ricerca e ospedali impegnati nella ricerca di vaccini e terapie contro il Covid-19.

Secondo le rilevazioni del Comparto intelligence la maggior parte di queste azioni non sono di matrice terrorista, ma sono perpetrate da hacktivisti. Questi attori hanno infatti recentemente limitato gli attacchi per fini propagandistici in modo da concentrare i propri sforzi su penetrazioni digitali miranti a screditare imprese private e istituti sanitari a loro dichiaratamente ostili. Questi strumenti vengono però allo stesso modo utilizzati da soggetti di matrice statale per attuare campagne di spionaggio digitale il cui è obiettivo è sabotare la stabilità dei sistemi democratici occidentali, e che recentemente si sono concentrati su attacchi informatici miranti a sottrarre informazioni relative alle terapie e ricerche contro il Covid-19.

La **minaccia ibrida**, che veniva solo accennata nella relazione del 2019, acquista una posizione di maggiore rilevanza in quella del 2020, affermandosi come nuova sfida separata dalle altre. Questo pericolo è caratterizzato dall'utilizzo di attacchi cibernetici per campagne di disinformazione veicolate attraverso canali sia cyber che convenzionali, volte a indebolire i sistemi democratici. Durante la crisi pandemica, ad esempio, la produzione di fake news dai toni allarmistici ha causato un infodemia volta a sfruttare l'insofferenza della popolazione non più in grado di distinguere le notizie false da quelle vere.

4. Il sistema d'informazione spagnolo

L'Italia non è stata l'unica a dover andare incontro ad una radicale trasformazione dell'assetto organizzativo dei suoi servizi segreti in modo da renderli più moderni ed efficaci. Le nuove minacce che rendono questi cambiamenti necessari hanno infatti portata globale, minacciando così gli interessi della quasi totalità delle entità statali. Anche la Spagna, con la riforma del proprio Comparto intelligence, implementata dalla legge n. 11 del 2002, è entrata a far parte di questi paesi. Questa legge ha avuto inoltre la funzione di sopperire alla mancanza di una regolamentazione unitaria dei Servizi di intelligence, che aveva in precedenza caratterizzato il **Centro Superiore di Informazione della Difesa (CESID)**, e senza la quale risultava infatti più problematico il processo di evoluzione e adattamento dei servizi da un punto di vista organizzativo.

La legge n.11 del 2002 ha quindi suddiviso l'attività informativa dei servizi in cinque agenzie *(Grafico 3)*. Con questa organizzazione la Spagna ha mantenuto la sua divisione dei compiti atipica rispetto a quella tradizionale dei Servizi occidentali. Con la creazione del CESID prima, e del **Centro Nazionale di Intelligence (CNI)** poi, lo stato spagnolo aveva optato per un solo servizio informativo principale invece che due Servizi, responsabili uno per l'attività informativa interna e uno per quella esterna.

Il CNI si afferma quindi come un organismo pubblico speciale dotato di autonomia funzionale, in ambito sia organizzativo che finanziario, necessaria al perseguimento dei propri obiettivi, che vengono stabiliti con cadenza annuale dal governo tramite una Direttiva di Intelligence classificata come segreta.

Il principale obiettivo del CNI è la raccolta informativa volta ad un efficiente analisi e neutralizzazione delle molteplici minacce agli interessi nazionali. Quest'organo ha però anche la responsabilità di garantire il necessario coordinamento e collaborazione con i Servizi di intelligence

esteri e con gli Organismi internazionali.
Seppur autonomo funzionalmente, il CNI è istituito all'interno del Ministero della difesa, ed è formato da una Direzione, una Segreteria generale e altre unità definite tramite regolamenti interni.

La Direzione del Servizio è affidata al Segretario di Stato Direttore del CNI, nominato sotto proposta del Ministro delle Difesa con un mandato di cinque anni. Il direttore è responsabile principalmente della promozione e del coordinamento delle attività del Centro, ma deve anche approvare la proposta del preventivo di bilancio del CNI, mantenere le relazioni con i servizi di informazione delle Forze e dei Corpi di Sicurezza dello Stato e gli organi dell'Amministrazione Civile e Militare, e dirigere il Centro Cryptologico Nazionale.

In situazioni di assenza emergenziale, il Direttore viene sostituito dal Segretario Generale del CNI che, anch'egli nominato su proposta del Ministro della Difesa, regge la Segreteria Generale del Servizio. Tra le sue funzioni oltre all'assistenza del Direttore rientrano anche la rappresentanza del CNI la definizione dei meccanismi e dei sistemi di organizzazione del Centro.

Oltre al passaggio da CESID a CNI, anche i Servizi informativi militari col tempo hanno subito una modifica della propria organizzazione. Mentre inizialmente ogni forza armata (esercito, marina, aereonautica) aveva i propri servizi di intelligence, con la Direttiva Interna 20/2000 venne istituito per unificarli il **Centro di Intelligence delle Forze Armate (CIFAS)**, sottoposto allo Stato Maggiore della Difesa. Al CIFAS venne affidata la responsabilità dell'attività di intelligence in ambito militare e la supervisione di possibili situazioni di interesse militare provenienti dall'esterno.

Per quanto riguarda invece il **Commissariato Generale di Informazione (CGI)** e il **Servizio Informativo della Guardia Civile (SIGC)**, in quanto Servizi informativi dei corpi di polizia e guardia civile sono responsabili dell'attività informativa atta al supporto delle operazioni dei rispettivi organi. In maniera similare, al **Centro di Intelligence contro il Terrorismo e il Crimine Organizzato (CITCO)** nato nel 2014 dall'unione del **Centro Nazionale di Coordinamento Antiterrorista (CNCA)** e del **Centro di Intelligence contro il Crimine Organizzato (CICO),** è affidata l'attività di analisi informativa in materia di antiterrorismo e lotta alla criminalità organizzata.

Il Servizio informativo spagnolo è periodicamente oggetto di tre tipi di controllo: governativo, parlamentare e giudiziario.

Il controllo governativo è affidato alla Commissione Delegata del Governo per gli Affari di Intelligence dello Stato *"presieduta dal Vicepresidente del Governo, che ne designa il Presidente, e composta dal Ministro degli Affari Esteri, il Ministro della Difesa, il Ministro dell'Interno, il*

Ministro dell'Economia, il Segretario Generale della Presidenza, il Segretario di Stato per la Sicurezza ed il Segretario di Stato Direttore del Centro Nazionale di Intelligence" (Rivista 22, 2021). È infatti davanti a questa commissione che viene presentata dal Direttore del CNI la relazione relativa alle attività di intelligence e alle minacce contro la Spagna. La ha inoltre la funzione di preservare lo stretto coordinamento tra il CNI e i Corpi e le Forze di Sicurezza dello Stato e degli organi dell'Amministrazione civile e militare.

Per ciò che concerne il controllo parlamentare sulle attività del CNI, esso viene effettuato dalla Commissione responsabile dei fondi destinati a spese riservate, data la sua conoscenza degli obiettivi di intelligence stabiliti a livello statale e del loro grado di attuazione.

Il controllo giudiziario preventivo viene invece eseguito ogni tal volta che l'operato dei Servizi viola *"i diritti protetti dagli artt. 18.2 e 18.3 della Costituzione spagnola, che, protetti da una riserva di giurisdizione, possano cioè essere violati o limitati solo con un'autorizzazione giudiziaria*" (Rivista 22, 2021).

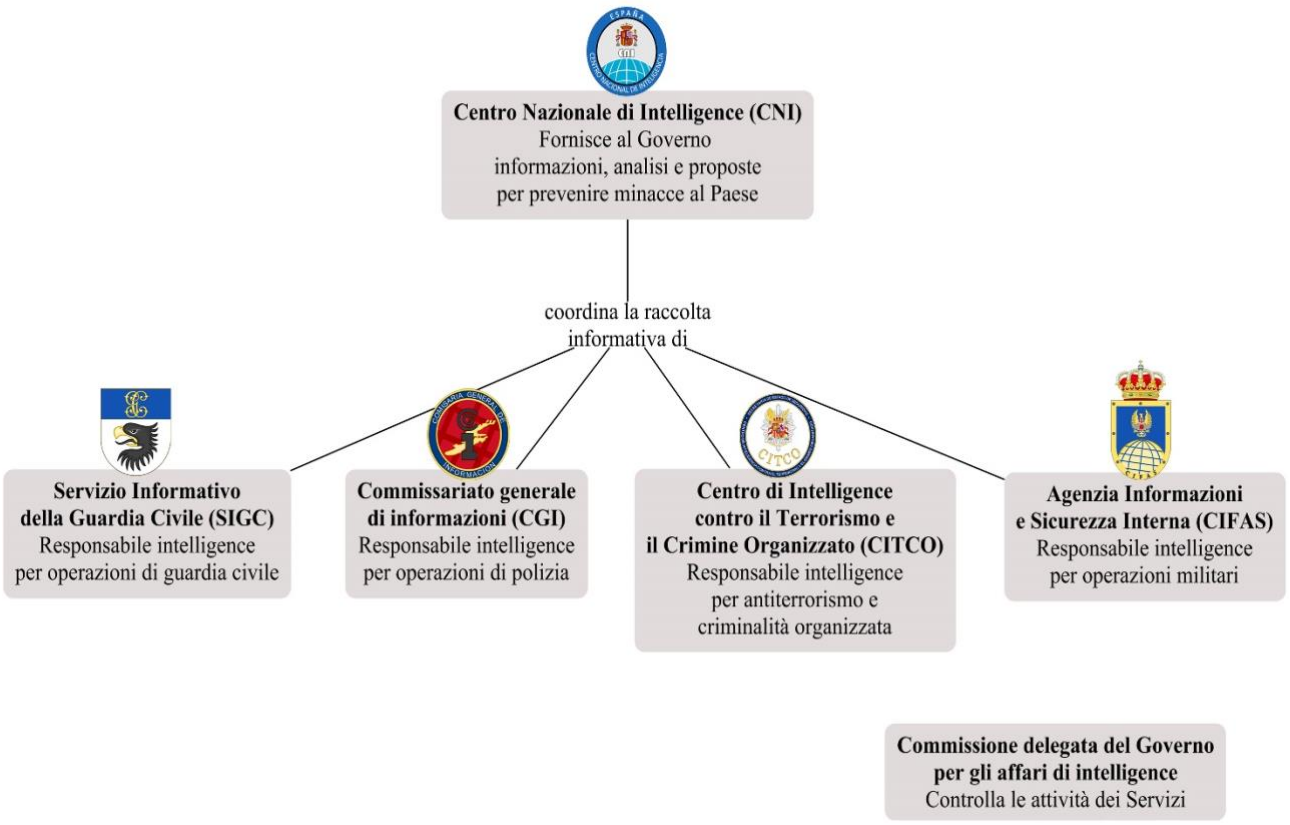

Grafico 3: Organizzazione delle unità di intelligence sancita dalla legge n. 11 del 2002

4.1 . Stato delle minacce per la Spagna

Come in Italia ogni anno viene pubblicata la Relazione dei servizi segreti al Parlamento, anche in

Spagna con cadenza annuale viene redatto dal Dipartimento di Sicurezza Nazionale (DSN) l'*"Informe Anual de Seguridad Nacional".* Questo documento certifica lo stato attuale delle minacce che affliggono il paese e i progressi che sono stati fatti o meno nel fronteggiarle, con lo scopo di rappresentare un quadro integrale dello stato di sicurezza della nazione.

Confrontando questo rapporto con il corrispettivo italiano possono essere individuate delle evidenti differenze organizzative. Mentre la Relazione è divisa in due parti, una concernente le crisi che riguardano le diverse regioni del mondo e una relativa alle minacce rivolte all'Italia, il rapporto spagnolo si compone di quindici capitoli dedicati ad altrettante sfide per la nazione, così come riportato nella Strategia di Sicurezza Nazionale.[5] Anche le minacce individuate dal documento spagnolo possono essere suddivise tramite lo stesso criterio applicato per quelle italiane.

Rientrano tra minacce, cosiddette, "classiche":

- alla Difesa Nazionale (integrità)
- alla Sicurezza marittima e dello spazio aereo
- la Criminalità Organizzata
- il Terrorismo
- lo Spionaggio
- la proliferazione di armi di distruzione di massa

Possono invece essere annoverate tra le minacce "emergenti" tutte quelle relative a:

- sicurezza informatica (attacchi informatici e cyber war)
- protezione delle infrastrutture critiche
- sicurezza economica e finanziaria
- sicurezza energetica
- immigrazione clandestina
- pandemie ed epidemie
- preservazione dell'ambiente
- protezione contro emergenze e catastrofi

Nel primo gruppo rientra quindi la **Difesa Nazionale**, concretizzatasi non solo con la protezione dello stato e dei suoi cittadini dagli attacchi di qualsiasi attore internazionale, ma anche con la cooperazione con gli altri paesi in materia di difesa specialmente per ciò che riguarda la tutela degli interessi strategici all'estero come lo sviluppo di collaborazioni e iniziative in Medio Oriente (con Emirati Arabi Uniti, Israele, Arabia Saudita, Egitto e Giordania) o Asia (con Giappone e Corea del

[5] https://www.lisainstitute.com/blogs/blog/principales-amenazas-seguridad-nacional-espana

Sud).

Per ciò che riguarda la **Sicurezza marittima e dello spazio aereo**, mentre la seconda necessitava l'adozione di una Strategia per la sicurezza aerospaziale, accompagnata dalla creazione di un Comitato specializzato a sostegno del Consiglio di sicurezza nazionale (ovvero il Consiglio di sicurezza aerospaziale nazionale), la prima esigeva una tutela più per la sua rilevanza in termini economici che per un effettivo bisogno di sicurezza in ambito militare. Gran parte degli scambi di merci a livello globale avvengono infatti tramite il commercio marittimo-internazionale, la cui rilevanza condiziona gli interessi geopolitici di quasi tutto gli stati. La sicurezza marittima è rilevante però anche nella lotta al narcotraffico dato che via mare avviene anche il traffico illecito di droga (principalmente cocaina e hashish) e tabacco diretto in Spagna.

La **Criminalità organizzata** è una delle minacce classiche di origine interna che grazie alla sua grande capacità di adattamento riesce ancora oggi ad aumentare i propri proventi tramite: il traffico di droga, il riciclaggio di denaro, la criminalità informatica, il traffico illecito di esseri umani e di armi, e la frode finanziaria.

Il **terrorismo** è invece combattuto su due fronti, a livello transnazionale e interno. Il primo, principalmente di matrice jihadista, è quello che ha attratto la quasi totalità degli sforzi dell'intelligence spagnola. Il declino di DAESH ha comportato il ritorno nel continente europeo di molti combattenti terroristi stranieri in fuga da Siria e Iraq, aumentando la diffusione di propaganda jihadista a livello interno. Proprio sull'indebolimento della capacità delle organizzazioni terroristiche di agire sul suolo comunitario si concentrano gli sforzi dell'intelligence spagnola in coordinamento agli altri servizi europei. Per ciò che riguarda invece il terrorismo interno gli organi giudiziari e di polizia continuano, dato per definitivamente sconfitto il gruppo ETA, il monitoraggio di organizzazioni terroristiche anarchiche la cui rilevanza è ormai ridotta rispetto al passato.

La sfida del Controspionaggio consiste nell'ostacolare l'**attività informativa** dei servizi segreti degli altri paesi rivolti contro la sicurezza degli interessi spagnoli. Oggigiorno questa contrapposizione ha luogo principalmente nel cyberspazio e rappresenta una preoccupante minaccia per la sicurezza nazionale, specialmente alla luce del recente incremento dell'aggressività di alcuni servizi di intelligence che non si limitano più alla semplice ricerca di informazioni quanto all'attuazione di "operazioni ibride" volte a screditare le istituzioni statali e a manipolare l'opinione pubblica di un paese.

Un altro pericolo è rappresentato dalla **Proliferazione di armi di distruzione di massa** e del loro potenziale impiego in conflitti tra Stati o nei conflitti interni. Crescente preoccupazione è inoltre legata al traffico di materiali radioattivi ad attori non statali facenti parte di organizzazioni

terroristiche. Questa minaccia alla sicurezza nazionale non riguarda solo singoli stati, e in quanto pericolo transnazionale viene combattuto con accordi multilaterali, che in quanto fragili non vengono sempre rispettati o rinnovati, come testimonia il ritiro americano dal Trattato sulle forze nucleari a raggio intermedio (INF) del 2 agosto 2019

La **Sicurezza informatica** ha, negli ultimi anni, assunto una rilevanza sempre maggiore dato l'aumento degli attacchi informatici, sempre più sofisticati e quindi difficili da contrastare, rivolti sia al settore pubblico che privato. Basati sulla mancanza di consapevolezza e di un'adeguata formazione informatica, questi attacchi hanno come obiettivo principalmente azioni di disinformazione o propaganda, acquisti e vendite online di origine fraudolenta, e il furto di informazioni riservate per poi richiedere un riscatto economico.

In merito alla **Protezione delle infrastrutture critiche** il rapporto mostra il progressivo completamento dello schema di pianificazione strategica generato con la Legge sulla Protezione delle Infrastrutture Critiche, evidenziando l'aumento degli attacchi informatici contro settori strategici come quello dei Trasporti, Energetico e Finanziario.

La **Sicurezza economica e finanziaria** viene invece affrontata riportando i timori della Banca di Spagna in merito al forte rischio di rallentamento della crescita economica dovuto alle politiche di protezionismo commerciale di alcuni paesi e all'uscita del Regno Unito dall'Unione Europea.

Tra le minacce emergenti rientra anche la **Sicurezza energetica**, che acquista importanza se si considera la vulnerabilità che deriva dalla forte dipendenza della Spagna dalle fonti energetiche provenienti dall'estero, che la indeboliscono e la condizionano nelle sue relazioni con gli altri stati. Questa parte del rapporto promuove per ragioni di sicurezza un maggiore impegno per la realizzazione di un quadro strategico che promuova l'impiego di fonti energetiche rinnovabili, anche alla luce delle conseguenze sulla sicurezza nazionale causate dal cambiamento climatico.

La **Gestione dei flussi migratori** viene invece descritta, come la sfida che ha avuto maggiori effetti divisori sui membri dell'Unione Europea, in merito alle politiche da adottare per ridurre l'arrivo di migranti (principalmente dall'Africa) sul suolo europeo. Essendo la Spagna uno dei principali punti di ingresso nel continente, questo dibattito comunitario ha causato una forte preoccupazione sociale che ha permesso l'ascesa di forti movimenti populisti.

La **Sicurezza contro pandemie ed epidemie**, generalmente sottovalutata, nell'ultimo anno si è riaffermata come pericolo per la sicurezza nazionale. Questa minaccia ha infatti assunto una pericolosità sempre maggiore a causa del processo di globalizzazione permette al giorno d'oggi la circolazione di microorganismi tramite il libero scambio di merci, ma soprattutto di persone, per cui le condizioni di viaggio sono sempre più favorevoli.

Tra le minacce emergenti rientra inoltre la **Preservazione dell'ambiente** che si riafferma come un settore sempre più cruciale per la sicurezza nazionale, a causa dei devastanti effetti del cambiamento climatico sull'ambiente, e quindi anche sulle società.

Infine, collegata al punto precedente, vi è la **Protezione contro emergenze e catastrofi**, che si afferma come misura necessaria contro il pericolo rappresentato da violenti fenomeni naturali che, aggravati dal processo di cambiamento climatico, con sempre più frequenza si abbattono sulla Spagna e sul resto del continente, come ad esempio le inondazioni e i repentini cambiamenti metereologici che causano ingenti danni alle coltivazioni.

5. Conclusioni

L'analisi comparativa del sistema di intelligence italiano e di quello spagnolo ci permette di evidenziare alcune differenze nel loro funzionamento.

Mentre l'attuale organizzazione del SISR, prevede che l'attività d'intelligence sia di competenza esclusiva di AISE e AISI, arrivando ad escludere formalmente qualsiasi altro organo da queste funzioni (come ad esempio il RIS), il sistema spagnolo si avvale della cooperazione di un numero maggiore di attori. Effettuano infatti attività d'intelligence non solo i membri del CNI, ma anche alcune sezioni responsabili per operazioni militari, della Guardia Civile, della polizia, o per antiterrorismo e criminalità organizzata. Questo sistema, funzionante grazie all'attività di coordinamento svolta dal CNI, garantisce una più equa distribuzione dei compiti.

Sempre in riferimento all'accentramento dell'attività informativa all'interno del SISR, una seconda ma sostanziale differenza col sistema spagnolo riguarda la ripartizione delle competenze tra esterno e interno del paese formalizzata con l'istituzione di AISE e AISI. Contrariamente a quanto avviene in Italia, il sistema spagnolo non prevede questo tipo di divisione, preferendo una pluralità di organi più specializzati, a cui affidare compiti più precisi. Questo criterio spiega ad esempio l'istituzione del CITCO che si occupa contemporaneamente di terrorismo e criminalità organizzata sia all'interno che all'esterno del paese.

Il sistema spagnolo risulta essere quindi più similare all'organizzazione che vigeva in Italia prima della promulgazione della legge n. 124. La decisione di dividere l'attività informativa tra interno ed esterno del paese viene ancora oggi spesso criticata per le difficoltà che essa può causare sia a livello operativo che di coordinamento durante lo svolgimento di operazioni congiunte. Non risulta però ad oggi un evidente inefficacia del SISR, e non sussistono sostanziali lamentale da parte dei membri del COPASIR nelle loro relazioni, lasciando trasparire una sostanziale fiducia e

soddisfazione per il lavoro svolto dai servizi segreti italiani.

Sembra quindi non essere necessaria una riforma completa del SISR, basata sull'istituzione di nuove agenzie create ad hoc per contrastare le minacce emergenti. Si ritiene però opportuna la creazione di nuovi organi, necessari per coadiuvare l'operato di AISE e AISI nel rispondere efficacemente a queste minacce, senza però distoglierli dalle loro competenze operative.

Un esempio concreto riguarda la più preoccupante delle minacce emergenti, ovvero quella relazionata con la sicurezza informatica, alla quale nessun sistema informativo sarebbe in grado di far fronte senza apportare delle modifiche alla propria organizzazione. Queste preoccupazioni in merito alle minacce alla sicurezza nazionale del cybercrime sono state sollevate per la prima volta dal COPASIR. Secondo il Comitato le attività svolte dal Governo per combattere il cybercrime hanno solo colmato singoli vuoti organizzativi, mentre una pianificazione strategica di contrasto e prevenzione alla minaccia cibernetica restava assente. Era quindi necessario istituire un centro di coordinamento in grado di fornire un'adeguata risposta in termini di prevenzione e di velocità di reazione a queste minacce.

Per raggiungere un sufficiente livello di protezione dalle minacce di origine cyber, a livello nazionale è stato quindi adottato un sistema di gestione della sicurezza cibernetica lungo tre livelli. Il primo è quello politico di cui fanno parte il Presidente e il CISR.

Il secondo, è quello operativo del **Nucleo per la Sicurezza (NSC)**, organo attivo dal 2018 per attività di formazione, prevenzione e rafforzamento della sicurezza nazionale dalla minaccia cyber. Quest'ultimo organo è stato particolarmente importante nel 2019 poiché ha: "verificato lo stato di attuazione delle misure di coordinamento interministeriale per la gestione delle crisi cyber; supportato le Amministrazioni partecipanti nell'implementazione di progetti volti ad incrementare le rispettive capacità di difesa e prevenzione; promosso e coordinato la partecipazione nazionale ad esercitazioni attività della International Cooperation Strategy, tesa a valorizzare le eccellenze industriali nazionali e a propiziare rapporti di collaborazione con primari partner esteri" (Relazione sulla politica dell'informazione per la sicurezza 2019).

Il terzo livello è invece quello tecnico del **Computer Security Incident Response Team (CSIRT)**, operativo presso il DIS dal maggio 2020 per la gestione degli incidenti informatici, consistente nella ricezione della notifica di avvenuto incidente, del monitoraggio delle conseguenze e del supporto alle vittime. Quest'organo è predisposto al rafforzamento della governance della sicurezza cyber a livello nazionale e internazionale tramite attività di cooperazione e condivisione di informazioni con i propri omologhi esteri. Il CSIRT resta però un centro di raccolta di segnalazioni, e non un vero e proprio organo predisposto ad operazioni di intelligence, che rimangono infatti accentrate nelle

funzioni di AISE e AISI e per questo parrebbe più efficace un suo posizionamento all'esterno del SISR.

Inoltre, nel 2019 il CISR aveva incaricato il Comparto intelligence di sovrintendere l'istituzione del "**Perimetro di sicurezza nazionale cibernetica**", basato, fondamentalmente, su di una forte cooperazione tra istituzioni pubbliche e private volta a contrastare qualsiasi forma di minaccia cibernetica.

In merito al rapporto pubblico-privato, Franco Gabrielli, Sottosegretario alla Presidenza del Consiglio con delega sull'intelligence, ne ha recentemente denunciato la scarsa chiarezza. La regolamentazione di questa partnership è infatti generica, dando spesso luogo a interpretazioni equivoche dello stesso sistema. In merito, Gabrielli ribadisce che nel sistema è assente "la trasparenza, la correttezza dei rapporti e la definizione di un ente regolatore pubblico, che non è nel comparto intelligence ma dev'essere al di fuori" (Cyber, si cambia. Ecco la rivoluzione targata Gabrielli).

Oltre al Perimetro di sicurezza nazionale cibernetica, ci sono state anche ulteriori evoluzioni dell'ecosistema cyber italiano. Sono state ampliate le competenze del DIS per permettergli di acquisire funzione di coordinamento tra le Autorità e i soggetti "perimetrati", garantendo la coerenza e il rispetto dell'implementazione della norma. Sono inoltre stati assegnati al Presidente del Consiglio strumenti d'immediato intervento al fine di affrontare efficacemente la minaccia cyber per la sicurezza nazionale.

Oltre all'introduzione di nuovi protocolli di difesa e l'istituzione di organi di sostegno per l'attività informativa, il fulcro della risposta statale contro le minacce emergenti, deve consistere in un continuo miglioramento e aggiornamento delle risorse umane (tramite una formazione continua sulle evoluzioni degli scenari globali) e tecnologiche (tramite l'investimento in strumentazioni sempre più all'avanguardia), rimandando ai versanti che costituiscono il fulcro dell'attività intelligence: la ricerca e l'analisi.

Un'altra arma che potrebbe risultare essenziale per fronteggiare minacce emergenti di portata transnazionale è insita in una maggiore **cooperazione internazionale dei servizi** che, seppur sottomessa agli interessi dei singoli stati, risulta necessaria come risposta a fenomeni sempre più globali e pervasivi oltre che una forma di "apertura" verso la cittadinanza (concetto di sicurezza e intelligence collettiva) basata sulla promozione e diffusione della cultura della sicurezza volta a cambiare l'immagine dei servizi rendendoli più vicini alla popolazione.

Se infatti precedentemente il sistema era eccessivamente chiuso, ad oggi, con la promulgazione della legge n. 124 è avvenuta una graduale apertura che fa conoscere il Sistema e il suo lavoro alla

società civile. Quest'evoluzione non ha riguardato solo il sistema italiano, ma anche quello spagnolo, delineando la tendenza verso una organizzazione più moderna dei sistemi di intelligence occidentali.

Riferimenti

Carrer, G. «Cyber, si cambia. Ecco la rivoluzione targata Gabrielli». (08 aprile 2021). Tratto da *Formiche*: https://formiche.net/2021/04/franco-gabrielli-rivoluzione-cyber/

«Chi siamo». Tratto da *Sistema di informazione per la sicurezza della Repubblica*: https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo.html visitato il 14 aprile 2021.

«Conversione in legge, con modificazioni, del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione», Legge n. 43 (1) (17aprile 2015).

«Conversione in legge, con modificazioni, del decreto-legge 30 ottobre2015, n. 174, recante proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione», Legge n. 198 (11dicembre 2015).

«Il controllo parlamentare». Tratto da *Sistema di informazione per la sicurezza della Repubblica*: https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/i-controlli/il-controllo-parlamentare.html visitato il 14 aprile 2021.

«Il segreto di Stato». Tratto da *Sistema di informazione per la sicurezza della Repubblica*: https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/segreto-di-stato.html visitato il 14 aprile 2021.

«L'interesse nazionale». Tratto da *Treccani*: https://www.treccani.it/magazine/atlante/cultura/Interesse_nazionale.html#:~:text=L'interesse%20nazionale%20%C3%A8%20ci%C3%B2,in%20ultima%20analisi%2C%20ai%20cittadini visitato il 14 aprile 2021.

«Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato», Legge n. 801 (24ottobre1977).

Marco, L. «Gli 007 italiani lanciano l'allarme per i crimini online. La relazione.» (23 luglio 2010). Tratto da *Il Sole 24 Ore*: https://st.ilsole24ore.com/art/notizie/2010-07-23/copasir-lancia-allarme-cybercrime-080011_PRN.shtml

«Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto», Legge n. 133 (7agosto 2012).

«Modifiche alla disciplina del Sistema di informazione per la sicurezza - A.C. 5284», n.659/0 (4luglio 2012)

«Principales amenazas seguridad nacional espana». Tratto da *LISA Institute*: https://www.lisainstitute.com/blogs/blog/principales-amenazas-seguridad-nacional-espana visitato il 14 aprile 2021

«Relazione sulla politica dell'informazione per la sicurezza 2019». (20Marzo2020). Tratto da *Sistema di informazione per la sicurezza della Repubblica*: https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-2019.html

«Rivista 22». Tratto da *GNOSIS*: http://gnosis.aisi.gov.it/sito/Rivista22.nsf/servnavig/16visitato il 14 aprile 2021