



Presidenza del Consiglio dei Ministri

**Sistema di informazione per la sicurezza
della Repubblica**

RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2013

EXECUTIVE SUMMARY

Con la presente Relazione, ai sensi dell'art. 38 della Legge n. 124 del 2007, il Governo riferisce al Parlamento sulla politica di informazione per la sicurezza e sui risultati conseguiti nel corso del 2013.

Nella **PREMESSA** viene delineato il rinnovato profilo dell'intelligence, con le linee strategiche che ne hanno caratterizzato il percorso evolutivo: la sempre maggiore apertura verso i cittadini ed il mondo delle imprese, dell'università e della ricerca; il varo di un articolato riassetto organizzativo secondo logiche di efficienza e di razionalizzazione delle risorse; la tendenza, nel pieno spirito della riforma, a consolidare l'unitarietà dell'azione intelligence in risposta alla natura multidimensionale e globale della minaccia; il consolidamento delle sinergie interistituzionali che, sullo specifico versante della sicurezza cibernetica, si è tradotto in mirate iniziative di coordinamento e di convergenza della comunità intelligence e delle diverse Amministrazioni dello Stato.

L'unitarietà di approccio e la trasversalità dei fenomeni di potenziale impatto sulla sicurezza nazionale, a partire dalle vulnerabilità del cyberspazio e dalle dinamiche economico-finanziarie, si riflettono nella linea espositiva della Relazione, che vede ricorrenti "rimandi" tra la prima parte, centrata sulle asimmetrie della minaccia, e la seconda, focalizzata sulle instabilità regionali. Anche quest'anno, l'elaborato riporta in chiusura un breve *outlo-*

ok su tendenze evolutive e scenari di rischio. Costituisce una novità, invece, l'allegato "Documento di Sicurezza Nazionale", che, in ottemperanza al dettato normativo (art.38, comma 1-bis della legge 124/2007), riferisce sulle attività svolte in materia di protezione delle infrastrutture critiche materiali e immateriali nonché di protezione cibernetica e sicurezza informatica.

La **I PARTE** della Relazione, relativa alle **ASIMMETRIE DELLA MINACCIA**, si apre con una sezione dedicata alla **CYBERTHREAT**, fenomeno di particolare rilevanza alla luce dell'importanza che lo spazio cibernetico riveste per il benessere e la sicurezza del Paese. Viene dunque posto l'accento sui fenomeni di spionaggio digitale diretti all'acquisizione di informazioni sensibili e *know how* in danno di settori strategici e sull'utilizzo del dominio cibernetico da parte della criminalità organizzata, cui vanno imputati episodi di sottrazione di dati, specie di natura finanziaria. Viene parimenti svolta una disamina del cd. *hacktivism*, che concretizza nella "rete" attacchi di valenza propagandistica o dimostrativa volti talora a far da sponda virtuale a *campagne di lotta* ed iniziative di piazza promosse dall'area antagonista.

L'esposizione procede con le **DINAMICHE ECONOMICO-FINANZIARIE**, delineando, in un contesto caratterizzato da una acuta crisi economica, le direttrici lungo le quali si è dipanata l'azione intelligence. Al riguardo, ampio spazio è stato anzitutto dedicato all'impegno nel concorrere alla tutela del Sistema Paese rispetto a minacce in grado di depauperare la competitività tecnologica ed infrastrutturale nazionale, di incidere sulla continuità degli approvvigionamenti energetici, nonché di alterare la solidità del sistema creditizio e finanziario. E' stata inoltre illustrata l'opera di contrasto alle pratiche di evasione ed elusione fiscale su larga scala ed alle molteplici proiezioni della criminalità organizzata nel tessuto produttivo.

L'elaborato muove poi dalle perduranti difficoltà congiunturali per illustrare sia i rischi di **STRUMENTALIZZAZIONI ESTREMISTE** del diffuso disagio sociale che **LA MINACCIA EVERSIVA**. Ci si sofferma sull'attivismo di formazioni antagoniste, di sinistra e di destra, interessate a fomentare la conflittualità nonché sulle *campagne di lotta* tese a canalizzare il dissenso e le potenziali spinte ribellistiche in un'ottica antisistema. Viene quindi tratteggiata l'evoluzione della minaccia anarco-insurrezionalista e si fa riferimento alla propaganda svolta dai ristretti circuiti di ispirazione brigatista.

Oggetto della sezione successiva della Relazione è **LA MINACCIA TERRORISTICA INTERNAZIONALE E LA SUA DIMENSIONE DOMESTICA**. Emergono, sul piano ideologico e del proselitismo, l'influenza tuttora esercitata dal messaggio qaidista nonché, sul piano operativo, i pericoli derivanti dalla crescente vitalità di formazioni jihadiste nelle regioni nordafricana e mediorientale. Viene trattata in questo contesto la tematica dei cd. *foreign fighters*, ovvero dei volontari che si recano in teatri di crisi per aderire al *jihad*, e dei rischi correlati ad un loro eventuale ritorno nei Paesi di origine, fenomeno noto come "reducismo". Tra propaganda *on line*, percorsi di radicalizzazione e desiderio di concorrere alla "causa" è collocato il fenomeno dell'estremismo *homegrown*, cui si associa l'incognita di estemporanee ed autonome attivazioni offensive di segno anti-occidentale.

Segue poi una sezione riservata allo sviluppo di programmi di **PROLIFERAZIONE DI ARMI NON CONVENZIONALI**, rimasto, nel 2013, al centro di importanti contenziosi. Specifica attenzione viene riservata al *dossier* iraniano ed in particolare all'Accordo di Ginevra del 24 novembre. Un ulteriore passaggio illustra le problematiche connesse con l'utilizzo di armamento chimico in Siria nonché gli sforzi per la messa in sicurezza e la distruzione di quell'arsenale. Infine, viene dato conto del riproporsi con rinnovata intensità, nei settori missilistico e nucleare, della sfida tra la Corea del Nord e la Comunità internazionale.

La **II PARTE** dell'elaborato, dedicata alle **AREE DI INSTABILITÀ**, si sofferma tanto sulle conseguenze dei processi evolutivi innescati dalle rivolte popolari del 2011 quanto su quei Paesi che, sebbene non interessati da forme di protesta destabilizzanti, sono apparsi ugualmente esposti a significativi riassetto politici interni.

Si inizia con gli **SCENARI DI CRISI IN AFRICA**, a partire dalla sponda Sud del Mediterraneo, richiamando i molteplici risvolti, in termini di rischi ed anche di opportunità per gli interessi nazionali, dei processi di cambiamento in atto. In questa prospettiva vengono passati in rassegna gli sviluppi intervenuti nel corso dell'anno in Egitto, Libia e Tunisia nonché le dinamiche che hanno interessato Algeria e Marocco. Si fa poi riferimento alla cornice di sicurezza nel Sahel e nel Corno d'Africa come pure alle criticità regionali in Africa orientale e centrale.

Nel paragrafo sul **CONFLITTO SIRIANO E IL MEDIO ORIENTE** sono delineati i rischi connessi con l'aggravarsi dell'emergenza umanitaria in Siria e con l'impatto del conflitto sia sulle vicende libanesi, con specifica attenzione agli eventuali pericoli per la sicurezza del contingente italiano, che sulla Giordania, esposta al rischio di tensioni socio-politiche. Si fa cenno, poi, al processo di pace israelo-palestinese, ai complessivi equilibri d'area nel Golfo, nonché agli assetti interni ed alle proiezioni internazionali e regionali degli attori di quel quadrante, con particolare riguardo al "nuovo corso" in Iran ed alla cornice securitaria in Iraq.

La II Parte si conclude con una panoramica della situazione nello **SCACCHIERE AFGHANO-PAKISTANO**, in ragione del permanere di fattori critici e delle possibili ripercussioni sulla presenza militare e civile italiana.

Il capitolo finale **SCENARI E TENDENZE: UNA SINTESI** ripercorre il novero dei fattori di rischio destinati a tradursi in altrettante sfide per l'intelligence. Vengono, al riguardo, evocate in via prioritaria la necessità di continuare a "fare sistema" nel prevenire e contrastare la minaccia cibernetica, nonché la calibrata azione di monitoraggio e ricerca informativa cui è chiamata l'intelligence economico-finanziaria. Sono inoltre tracciati *trend* relativi ai profili della minaccia interna, ai potenziali riflessi sulla sicurezza nazionale dei processi di radicalizzazione di matrice jihadista ed alle future evoluzioni nei teatri di crisi.

IL DOCUMENTO DI SICUREZZA NAZIONALE declina le attività svolte dal Comparto in materia di tutela delle infrastrutture critiche nonché di protezione cibernetica e sicurezza informatica, sotto il duplice profilo di supporto all'implementazione dell'architettura nazionale *cyber*, così come previsto dal DPCM del 24 gennaio 2013, e di rafforzamento delle attività intelligence nello specifico settore.

PREMESSA

A *perto. Efficiente. Rinnovato. Unitario. Integrato nei meccanismi di governo ed in sintonia con il Paese.* È questo il profilo dell'intelligence al quale si è inteso dare corpo nel corso del 2013, l'anno che ha segnato il completamento del percorso di riforma, avviato con la Legge 124 del 2007 e proseguito con la Legge 133 del 2012, e ha parimenti chiamato il Sistema di informazione per la sicurezza della

L'intelligence nell'impianto istituzionale

Repubblica a confrontarsi con scenari nazionali ed internazionali in continua, profonda evoluzione, tali da delineare nuove forme di minaccia ed al contempo problematizzare ulteriormente, rispetto alle linee di tendenza già evidenziate negli anni precedenti, i tradizionali fattori di rischio per la tenuta complessiva del Sistema Italia.

Una scelta non di comunicazione, ma di visione strategica. Si è anzitutto ritenu-

to di spiegare al Parlamento, all'opinione pubblica ed all'insieme degli attori pubblici e privati sui quali grava il dovere di promuovere, ciascuno per la sua parte, la sicurezza nazionale che il ripiegamento dell'intelligence su se stessa, impedendole di provare il suo valore aggiunto, rischierebbe di vulnerarne la stessa ragion d'essere istituzionale. Lo spazio di segretezza, del quale il Comparto continua comunque ad aver bisogno per poter operare in maniera appropriata, è andato sempre più configurandosi come punto di arrivo, e non più come punto di partenza, di un processo di continuo confronto con le istituzioni e con la società civile.

La politica di apertura è essenziale per la credibilità degli Organismi di informazione, a sua volta indispensabile per guadagnare loro la fiducia dei cittadini. Proprio perché l'intelligence esercita responsabilità particolari, debbono essere noti all'opinione pubblica i volti di chi ne è alla guida, i

principi ispiratori della sua azione, i criteri di adeguamento alle nuove sfide della sicurezza ed i prioritari ambiti di intervento.

L'operazione di disvelamento dell'universo dei Servizi, della sua natura, delle sue funzioni e del suo linguaggio, culminata con il varo di un portale *web* totalmente rinnovato nella veste grafica e nei contenuti ed accessibile anche da dispositivi mobili, ha riscosso nel 2013 un generalizzato interesse, a riprova che l'attendibilità del patrimonio informativo e l'affidamento che, sull'intelligence, sentono a loro volta di poter fare tanto i cittadini quanto il mondo delle imprese, dell'università e della ricerca costituiscono due aspetti strettamente interconnessi.

Gli accessi all'indirizzo *www.sicurezza-nazionale.gov.it* hanno effettivamente dimostrato come sia possibile accorciare la distanza fra i "Servizi segreti" e i cittadini, favorendo una cultura della sicurezza partecipata e consapevole, e trasmettendo, soprattutto ai giovani, il senso del legame inscindibile fra sicurezza e libertà, ancor più acuito dal carattere fluido, puntiforme e multidimensionale delle nuove minacce, ora non più solo geografiche, ma traslate da fonti lontane, immateriali, spesso proprio attraverso il *web*. Al mutare dei rischi e delle sfide globali, e non solo in ossequio ad un generico obbligo di trasparenza, gli Organismi non possono essere identificati come un luogo di riservatezza a perdere.

Il processo di apertura avviato negli anni scorsi e culminato, dopo la pubblicazione del "Glossario" dei termini *intelligence*

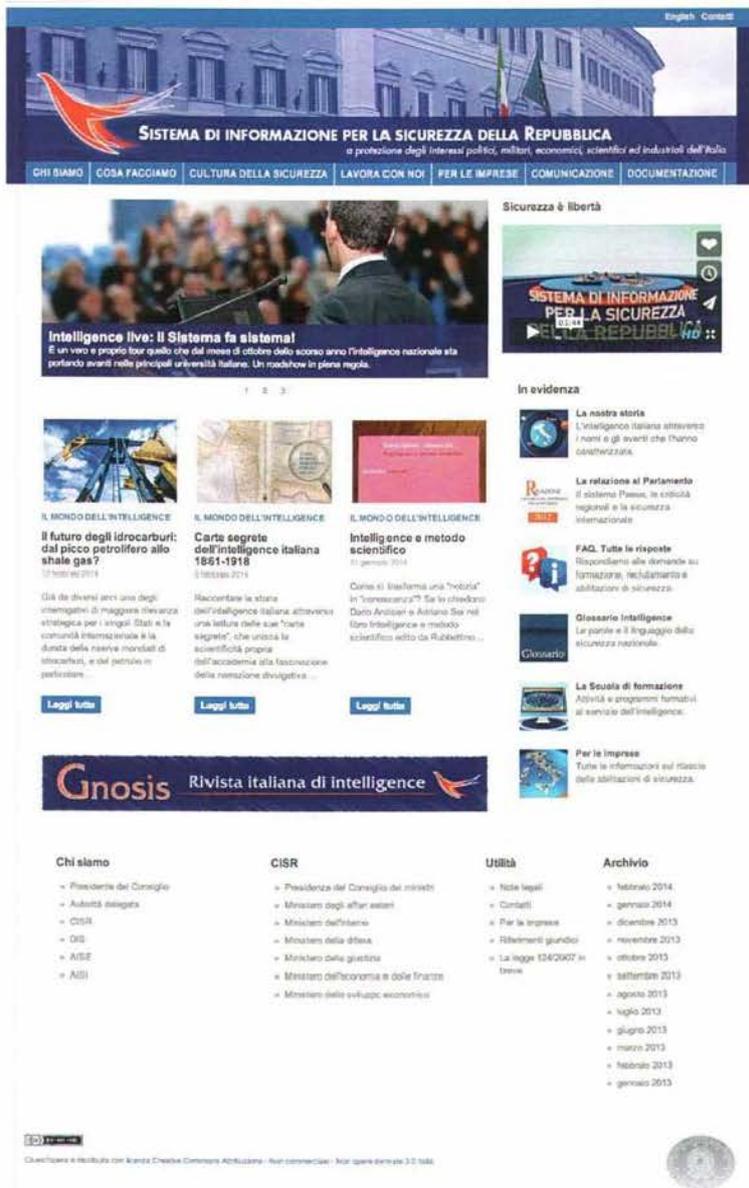
rivolto al grande pubblico, nella profonda revisione del portale, è destinato a proseguire anche in futuro con il rinnovamento della rivista "Gnosis".

Ma il *restyling* del sito è servito anche ad attrarre l'interesse e la professionalità dei giovani, grazie alla sezione "lavora con noi", intesa come strumento per creare una forma di collegamento permanente con un potenziale serbatoio di raccolta, di primario valore per l'intelligence del presente e del futuro.

È in questo contesto che è proseguito nel 2013 il processo di razionalizzazione della struttura del Comparto, virtuoso in quanto collimante con il principio di contenimento della spesa e teso a perseguire l'efficienza in una duplice dimensione, sia interna che esterna, secondo il comune criterio della multidisciplinarietà.

È in questa cornice che il Legislatore, con la Legge 133 del 2012, ha inteso affidare al DIS l'amministrazione unitaria degli aspetti gestionali del Comparto (bilancio, politiche del personale, approvvigionamenti e logistica, formazione) in un'ottica di valorizzazione dei compiti operativi delle Agenzie.

Sul piano dell'interfaccia con l'esterno, è stato ampliato il novero dei bacini di provenienza delle professionalità impiegate, non solo attingendo ad Amministrazioni diverse dai tradizionali ambiti delle Forze Armate e di Polizia, ma soprattutto operando nuove assunzioni ed immettendo nel Comparto risorse umane provenienti dai segmenti più qualificati del mondo giovanile. Nella consapevolezza che una dimensio-



Homepage del nuovo portale del Sistema di informazione per la Sicurezza della Repubblica

ne fondamentale del lavoro dell'intelligence è saper praticare un'effettiva capacità interdisciplinare, è stata messa a fattor comune una pluralità di esperienze, identificando in primo luogo nel settore delle *Information and Communication Technologies*, oltre che nel segmento dell'intelligence economico-

finanziaria, la priorità per le nuove assunzioni, quale segno tangibile della determinazione nel governare il nuovo. Nel mercato del lavoro, un impiego su cinque richiede competenze ICT avanzate ed il 90% dei posti di lavoro prevede conoscenze informatiche di base, mentre la natura dello spazio

cibernetico impone sempre più di saper agire in maniera coerente a vari livelli: informatico, logico, tecnologico, infrastrutturale, giuridico, commerciale, di sicurezza. In questo contesto, gli Organismi informativi non hanno fatto eccezione, privilegiando le professionalità nei settori strategici per la sicurezza dello Stato: degli oltre 6.000 *curricula* giunti attraverso la procedura di acquisizione *on-line*, quasi la metà hanno evidenziato la specializzazione nella *cyber security*.

Anche sul piano interno, l'impegno organizzativo, finalizzato a perseguire la massima razionalizzazione e valorizzazione delle risorse, si è dispiegato in chiave multidisciplinare. In linea di continuità con

il 2012, i piani di ricerca, elaborati dalle Agenzie in attuazione delle linee di indirizzo stabilite dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR), hanno infatti tenuto prioritariamente conto dell'interconnessione dei fenomeni oggetto di attività informativa, talché tutti i progetti, anche quelli individuati su base geografica, sono stati materialmente sviluppati in ragione della trasversalità delle minacce alla sicurezza nazionale.

Nel corso del 2013 sono stati altresì affinati i criteri tanto di gestione dei flussi informativi indirizzati alle

Un percorso di
rinnovamento

AISI INFORMATIVE/ANALISI INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA ANNO 2013

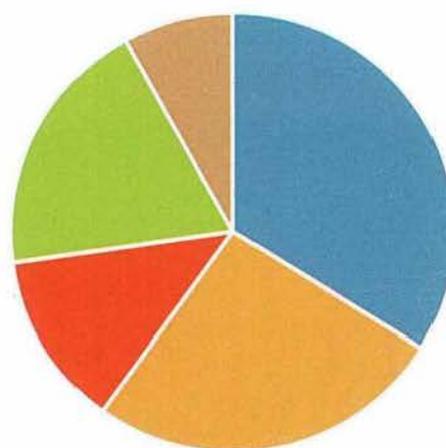


Grafico 1.

Autorità di governo (vds. grafici 1 e 2 sulla produzione delle Agenzie) quanto di verifica della rispondenza delle attività al fabbisogno informativo, tesa in misura sempre maggiore non solo a monitorare e misurare il lavoro svolto, ma soprattutto a promuovere un'efficiente ed armoniosa risposta dell'intelligence agli obiettivi fissati dal CISR.

Il processo di trasformazione del settore intelligence, avviato con la legge di riforma del 2007, ha comportato un'ampia manovra riorganizzativa, che nel 2013 è giunta al suo completamento sul piano regolamentare e ordinamentale con l'articolato riassetto interno varato il 1° aprile. L'anno trascorso ha dunque segnato l'av-

AISE
INFORMATIVE/ANALISI INVIATE A
ENTI ISTITUZIONALI E FORZE DI POLIZIA
ANNO 2013

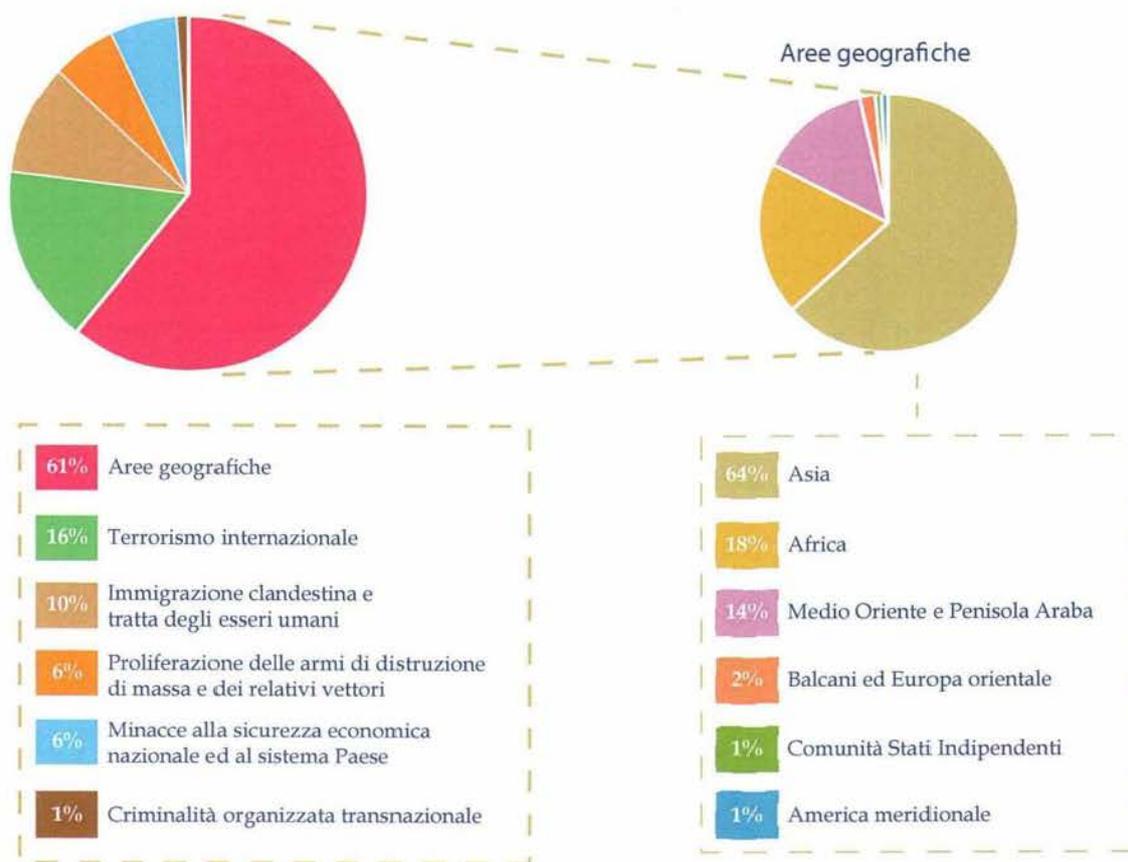


Grafico 2.

vio di una nuova fase, quella della “gestione del cambiamento”. Una fase destinata a snodarsi lungo un orizzonte di medio periodo, come è normale che accada per una riforma di sistema, che ha inteso incidere in profondità non solo sugli assetti degli Organismi e sui loro processi di lavoro, ma anche sulla loro funzione, accrescendone il ruolo di presidio avanzato a servizio della sicurezza del Paese.

Nei limiti in cui può trarsi un primo bilancio della riforma, suo tratto qualificante appare essere quello di aver saputo coniugare l’incremento nell’efficienza e nella capacità operativa del Comparto con un solido ancoraggio alla Costituzione e con il più scrupoloso rispetto dei principi fondamentali dell’ordinamento democratico. Ciò soprattutto in un contesto internazionale che, per effetto della interconnettività e della digitalizzazione della vita quotidiana, ha posto, come la cronaca recente ha fatto emergere con la vicenda del cd. “*datagate*”, seri dilemmi nel bilanciamento fra presidio della sicurezza nazionale, vera e propria preconditione di esistenza di una collettività organizzata statualmente, e tutela di diritti come la *privacy*, divenuti punti cardine del sistema delle libertà che qualificano le democrazie occidentali.

Sullo specifico vale segnalare come, nel quadro della disciplina dettata dalla legge di riforma del Sistema di informazione per la sicurezza in merito alla raccolta e trattamento delle notizie e delle informazioni, sia stato siglato, nel novembre del 2013, un apposito protocollo fra il DIS e l’Autorità

Garante per la protezione dei dati personali. Tale intesa prevede che i Servizi comunichino al Garante il piano ricognitivo degli archivi informatici delle amministrazioni cui hanno accesso, nonché le acquisizioni di dati dai gestori dei servizi di pubblica utilità, qualora queste comportino l’identificazione di singoli cittadini.

Parimenti, tanto l’ordinaria attività – operativa, di raccolta e valorizzazione delle acquisizioni informative, nonché di analisi – quanto il percorso di rinnovamento perseguito nel 2013 sono stati svolti sulla base degli indirizzi espressi dal CISR ed in piena sintonia con gli orientamenti del Comitato Parlamentare per la Sicurezza della Repubblica, le cui funzioni consultive e di controllo politico hanno continuato a costituire un’imprescindibile fonte di garanzia e di legittimazione dell’attività intelligence. È nell’ambito di questa stretta collaborazione con l’Organo parlamentare che si sono collocate le audizioni dell’Autorità di governo e dei Vertici degli Organismi informativi. Nel 2013, se ne sono tenute una del Presidente del Consiglio dei Ministri, due dell’Autorità Delegata per la Sicurezza della Repubblica, sei del Direttore Generale del DIS, cinque del Direttore dell’AISE e due del Direttore dell’AISI.

Pur essendo non unica, bensì triadica, l’articolazione degli Organismi italiani, questi hanno evidenziato, in coerenza con le leggi di riforma, una sempre più marcata tendenza all’unitarietà nel modo