Presidenza del Consiglio dei Ministri

Sistema di informazione per la sicurezza della Repubblica

RELAZIONE

SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA

2015

Relazione sulla politica dell'informazione per la sicurezza 2015

EXECUTIVE SUMMARY

Con la presente Relazione, il Governo riferisce al Parlamento, ai sensi dell'art. 38 della Legge n. 124 del 2007, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti nel corso del 2015.

In **PREMESSA** sono delineati il quadro di riferimento, la missione, i tratti peculiari e le responsabilità dell'intelligence, che si confronta con minacce nuove per natura ed impatto ed è chiamata ad una sempre maggiore integrazione nei processi decisionali. *pagg. 5 – 24*

Sono enucleate, in primo luogo, tre macro tendenze configurabili come altrettanti corridoi analitici nei quali si è incanalata la produzione info-valutativa del Comparto: l'ambiente digitale, gli *spin-off* della globalizzazione, le situazioni di instabilità geopolitica. Sono quindi declinate le priorità dell'azione informativa, identificabili in una sfida territoriale, centrata sul "Mediterraneo allargato", e tre sfide di sistema, rappresentate dal terrorismo jihadista, dalla minaccia cibernetica e da quella economico-finanziaria. Seguono poi alcune parole chiave utili a rappresentare e a qualificare lo sforzo dell'intelligence per incrementare, in un modello "a tendere", le proprie capacità operative e per essere all'altezza del compito: un'intelligence visionaria, che sappia cogliere dalla contingenza segnali e tendenze per il futuro; transnazionale, cioè in grado di realizzare sempre più efficaci forme di *information sharing* con i Servizi esteri per la prevenzione e il contrasto delle minacce di portata globale; integrata, innanzitutto al proprio interno, secondo il modulo di coordinamento avanzato assicurato dal DIS; "ad azionariato diffuso", quale prodotto di uno sforzo partecipato

che trasformi in attori della sicurezza i potenziali obiettivi di azioni ostili. Nella stessa linea espositiva è evocata, come requisito indispensabile per il "salto di qualità" dell'azione intelligence, la piena complementarietà tra il fattore umano – che rende essenziale il momento del reclutamento – ed il fattore tecnologico, fondamentale per rafforzare la capacità di agenti operativi e analisti del Comparto informativo.

La struttura del documento riflette i temi alla prioritaria attenzione: il terrorismo di matrice jihadista, con le sue proiezioni in direzione dell'Italia e dell'Europa e la sua interazione con le crisi d'area; la spinta migratoria verso lo spazio Schengen che, proprio in connessione con l'evoluzione della minaccia terroristica, introduce ulteriori profili di rischio; le sfide al Sistema Paese, dalle vulnerabilità di natura economico-finanziaria alle aggressioni di matrice spionistica e criminale; le dinamiche dell'antagonismo oltranzista e le pulsioni di stampo eversivo. In chiusura, il consueto *outlook* sul "dove andiamo", nonché l'allegato Documento di Sicurezza Nazionale previsto dal dettato normativo (art. 38, comma 1-*bis* della legge 124/2007).

Il primo capitolo, dedicato a **I FRONTI DEL *JIHAD***, muove dal protagonismo di DAESH sulla scena globale per delinearne l'incidenza sulla minaccia terroristica dentro e fuori l'Europa, alla luce anche di una strategia comunicativa sempre più sofisticata. *pagg. 25 – 29*

La caratura e le implicazioni del cambio di passo segnato dagli attacchi di Parigi sono rappresentate nel paragrafo dedicato alla **MINACCIA IN EUROPA**, tratteggiata con i connotati che erano stati già evocati nelle Relazioni degli anni scorsi e che, nel 2015, hanno dato concretezza agli scenari di rischio ad essi associati: *foreign fighters*, *returnees* e *commuters*, nonchè *commandos*, cellule dormienti e lupi solitari sono tutti attori reali o potenziali di una minaccia incombente e polimorfa. A seguire sono descritti i principali circuiti di finanziamento del terrorismo, che attingono ad un novero ampio ed eterogeneo di fonti ed attività illecite. *pagg. 29 – 37*

Il secondo paragrafo descrive **LE DECLINAZIONI REGIONALI DEL *JIHAD* E LA GEOMETRIA VARIABILE DELLE RELAZIONI INTERNAZIONALI**, passando in rassegna gli sviluppi d'area di maggior rilevanza sul piano della sicurezza in chiave di tutela degli interessi nazionali. Il filo conduttore della narrazione è rappresentato dall'attivismo di DAESH e dal suo interagire, per lo più in competizione, con le componenti della galassia qaidista, nonché dalle situazioni di instabilità che ampliano gli spazi d'intervento del *jihad* combattente e, conseguentemente, l'esposizione al rischio di cittadini e interessi occidentali. In coerenza con le priorità dell'azione intelligence, il primo *focus* è riservato al contesto libico, dove le precarie condizioni di *pagg. 37 – 49*

sicurezza hanno favorito le formazioni autoctone del Maghreb, specie le agguerrite espressioni dell'estremismo tunisino, e lo stesso DAESH, che ha consolidato gradualmente la propria presenza sia in Tripolitania che in Cirenaica. Sono quindi illustrate le alleanze tattiche e i "matrimoni di convenienza" che hanno qualificato i rapporti tra frange terroristiche nell'Africa sub-sahariana e nel Corno d'Africa. Specifica attenzione è quindi riservata al conflitto nel teatro siro-iracheno, catalizzatore di storiche contrapposizioni ed epicentro di criticità sul piano umanitario e di sicurezza, con ricadute a livello regionale e non solo. La trattazione si sofferma inoltre sulle germinazioni di DAESH nel Sinai e nella Striscia di Gaza, spostandosi poi sui Paesi del Golfo e sull'innalzamento della tensione fra Arabia Saudita ed Iran, tanto più rilevante in una fase contrassegnata dall'aggravarsi del confronto fra forze sciite e sunnite in diversi contesti di crisi, nonchè dalle prospettive di riposizionamento di Teheran introdotte dall'accordo sul *dossier* nucleare. Si prosegue con gli sviluppi in Yemen e con l'espansione di DAESH nella regione dell'*Af-Pak*, sino ai fermenti jihadisti nel Sud-Est asiatico.

Il secondo capitolo è centrato sul ***DOSSIER* MIGRATORIO** nella prospettiva intelligence, vale a dire sulle connotazioni del fenomeno in chiave securitaria. Sono quindi evidenziate le principali direttrici utilizzate dai migranti, le filiere criminali che gestiscono il traffico e le possibili aree di contaminazione tra immigrazione clandestina e terrorismo. Proprio in relazione al rischio di infiltrazioni terroristiche, ancora non specificamente riscontrato per quel che concerne il pur imponente flusso dalle coste libiche, particolare accento viene posto sulle insidie della rotta balcanica. *pagg. 51 – 58*

Al complesso dell'attività informativa e d'analisi riferibile a **IL PRESIDIO DEL SISTEMA PAESE**, è dedicato il terzo capitolo, che esordisce con il quadro generale di congiuntura, internazionale ed interna, nel cui contesto si è mossa l'azione di AISE ed AISI, della quale vengono tracciate le principali aree d'intervento: il supporto, in termini di concorso informativo, alle politiche di internazionalizzazione del Sistema Paese e di attrazione degli investimenti esteri; le vulnerabilità del sistema bancario e finanziario; il contrasto allo spionaggio cibernetico, volto all'illecita acquisizione di informazioni sensibili ai danni di aziende operanti in settori strategici per il Paese e ad elevato *know-how*; la sicurezza delle fonti di approvvigionamento energetico e delle reti infrastrutturali. Il richiamo alle zone grigie dell'economia vale a introdurre, altresì, il tema della criminalità organizzata, specie per il pervasivo intreccio tra corruzione, circuiti affaristici ed interessi mafiosi. Una sezione del capitolo è riservata, *pagg. 59 – 73*

infine, alle mafie d'importazione, che nelle espressioni più strutturate mostrano elevata influenza sulle comunità di riferimento, a discapito dei processi di integrazione.

LE STRUMENTALIZZAZIONI DEL DISAGIO sociale sono trattate nel quarto capitolo, che illustra le principali risultanze dell'intelligence sui fermenti antagonisti e sull'area eversiva. Con riguardo alla sinistra antagonista sono richiamati i temi più significativi della protesta – dall'emergenza abitativa alle campagne ambientaliste ed antimilitariste – nonché le linee di frattura interne al movimento. Sul versante eversivo, il riferimento è soprattutto alla minaccia anarco-insurrezionalista, concreta ed attuale, ed ai progetti di più lungo periodo riferibili all'estremismo marxista-leninista. Si dà conto, infine, di quanto emerso in relazione al frammentato quadro della destra radicale. *pagg. 75 – 85*

In chiusura, il capitolo **SCENARI E TENDENZE: UNA SINTESI** fa da ponte tra l'attività svolta, i *trend* rilevati e le prospettive dell'azione intelligence in connessione con l'evolversi del panorama della minaccia. In queste pagine della Relazione sono quindi compendiati i concetti chiave e le sfide che, in via prioritaria, continueranno a catalizzare l'impegno informativo nell'immediato futuro. *pagg. 87 – 92*

L'allegato **DOCUMENTO DI SICUREZZA NAZIONALE** fa, innanzitutto, il punto sulle iniziative architetturali intese a potenziare le capacità cibernetiche nazionali, con specifico rilievo per il ruolo d'impulso esercitato dall'intelligence, in un contesto di ampliate sinergie interistituzionali e di accresciuta collaborazione pubblico-privato: ciò con particolare riguardo alle attività sviluppate in seno al Tavolo Tecnico *Cyber* e al Tavolo Tecnico Imprese. Segue, per la prima volta in questa sezione della Relazione, una disamina sulla minaccia cibernetica in Italia, nelle sue diverse declinazioni quanto a matrice e tecniche d'attacco, corredata da serie statistiche e quadri previsionali. *pagg. 1 – 31*

Relazione sulla politica dell'informazione per la sicurezza

2015

La Relazione al Parlamento in versione digitale

Dall'edizione 2014, la Relazione è disponibile *online*, oltre che in versione PDF, anche in formato *e-book*.

È possibile visualizzare e scaricare il documento accedendo al seguente *link*: *www.sicurezzanazionale.gov.it/relazione2015* oppure utilizzando il *QR Code* riportato in basso.

Dato alle stampe il 15 febbraio 2016

INDICE

PREMESSA

Il 2015 come cesura paradigmatica

L'anno appena trascorso ha segnato una cesura paradigmatica nello scenario della minaccia, in una congiuntura storica nella quale i processi decisionali risultano sempre più condizionati dalla qualità e tempestività delle informazioni, accrescendo su chi le origina il portato di responsabilità.

Gli attacchi perpetrati a Parigi il 13 novembre hanno colpito al cuore la civiltà occidentale al pari dell'11 settembre, con un significato e con riflessi altrettanto inediti.

Allora fu un evento di "bassa probabilità ed alto impatto" a rendere manifesta l'asimmetria della minaccia, e dunque a sollecitare l'intelligence a riparametrare le proprie modalità d'azione e metodologie d'analisi al mutato scenario, per garantirne la congruità e l'efficacia.

Oggi, l'inusitata strutturazione e complessità di quell'eccidio – che ha visto per la prima volta nella piazza continentale europea l'azione di attentatori suicidi in così elevato numero – ha drammaticamente dimostrato quanto il terrorismo internazionale possa essere, ad un tempo, incombente e camaleontico, territoriale e liquido, organizzato e molecolare, imponendo ancora una volta, al presidio avanzato della sicurezza nazionale, di essere all'altezza di una sfida tutt'affatto nuova per natura, portata ed implicazioni, e destinata a protrarsi.

È peraltro, *mutatis mutandis*, tratto tipico di tutte le minacce emergenti quello di prescindere dalle frontiere sempre più porose degli Stati, lasciando tuttavia sempre a questi ultimi la responsabilità di farvi fronte, ed in ciò configurando il concetto stesso di sicurezza secondo caratteristiche intrinseche di dinamismo evolutivo. Connotati, questi, che pongono, a loro volta, in capo all'intelligence – strumento per sua natura non convenzionale, chiamato a svolgere un ruolo non esclusivo, ma comunque decisivo, a protezione e promozione dei beni e

valori collettivi – l'obbligo di colmare, ogni giorno, l'inevitabile divario fra le aspettative delle istituzioni, dell'opinione pubblica, dei soggetti economici, che legittimamente e doverosamente le chiedono di trovarsi "un passo avanti" rispetto alla minaccia, e l'effettiva capacità di risposta.

In un mondo nel quale si sopravvive, si compete, si conta, per ciò che si sa e per ciò che, conseguentemente, si decide, ci si attende dunque, e ha effettivamente preso corpo, un'intelligence in grado di operare a protezione dei diritti, oltre che dei poteri.

Gli Organismi informativi del nostro Paese hanno inteso sostenere questa prova cruciale, che involge la loro ragion d'essere ed il loro posizionamento istituzionale, proseguendo ed approfondendo, con un'intensità il più possibile commisurata all'evoluzione del contesto, il cammino di trasformazione intrapreso negli anni precedenti. Ciò in un continuo processo di reinvenzione della loro fisionomia, saldamente ancorato all'essenza della loro missione, che è, e rimarrà, quella di trasformare le informazioni in conoscenza utile e tempestivamente disponibile per l'assunzione di decisioni volte a tutelare i cittadini, le famiglie, le imprese, la Nazione ed il suo profilo nello scenario internazionale.

Decifrare la contemporaneità: tre corridoi analitici

Difficilmente si possono contenere i rischi e, ad un tempo, cogliere le pur feconde opportunità che, in termini di sviluppo, promozione sociale ed ampliamento dei diritti di cittadinanza, l'epoca dell'interdipendenza comporta, senza dispiegare un'adeguata attitudine alla lettura immersiva della contemporaneità, finalizzata a decifrarne le zone d'ombra ed a scorgere i margini di manovra utili a perseguire con compiutezza gli interessi nazionali: a leggere in profondità la realtà, senza per ciò stesso perderne il quadro d'insieme.

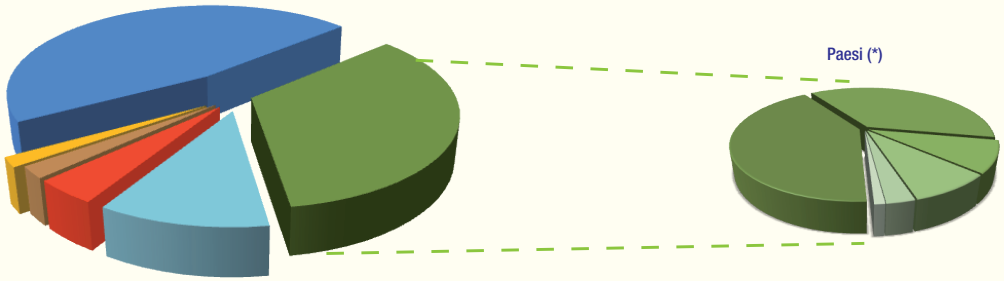
In tal senso, la copiosa produzione infovalutativa del Comparto è andata sempre meno riferendosi alla necessaria, ma non sufficiente, gestione corrente della quotidianità, incanalandosi sempre più lungo taluni "corridoi analitici" intesi a cogliere i vettori del cambiamento (*vedi grafici sulla produzione di AISE ed AISI).*

Grazie a tale scandaglio delle profonde trasformazioni intervenute nel contesto securitario globale, si sono delineate talune macro tendenze, che appaiono – nel disegnare un panorama di minacce ubique ed insieme geolocalizzate – peculiari del mondo odierno ed anticipatrici di quello che verrà. Ne sono emerse, fra altre, soprattutto tre, a bilancio di un'annata complessa quant'altre mai.

La prima ha riguardato l'**ambiente digitale**: spostando continuamente in avanti la frontiera dell'innovazione, le tecnologie hanno comportato il duplice effetto collaterale di azzerare la dimensione spaziale, mettendo definitivamente in crisi l'idea di confine politico difendibile solo con strumenti convenzionali, e parimenti di destrutturare internet, rendendo sempre più difficoltoso individuare in tempo utile chi

AISE

INFORMATIVE/ANALISI INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA
ANNO 2015



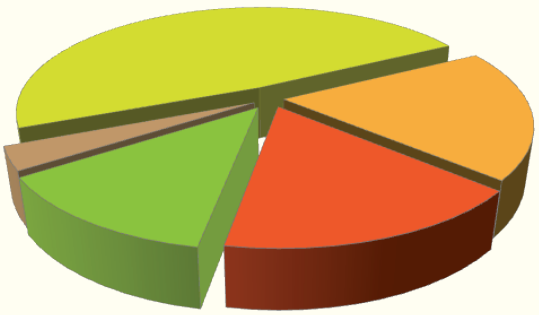
- 47% Minaccia terroristica ed estremismo di matrice internazionale
- 34% Paesi
- 11% Immigrazione clandestina e criminalità organizzata
- 4% Minacce alla sicurezza economico commerciale e finanziaria ed al Sistema Paese
- 2% Minaccia allo spazio cibernetico ed alle infrastrutture critiche
- 2% Proliferazione delle armi di distruzione di massa e dei relativi vettori

- 42% Medio Oriente
- 37% Africa (Nord Africa, Corno d'Africa, Africa subsahariana)
- 9% Asia
- 8% Comunità Stati Indipendenti, Caucaso e Asia centrale
- 3% Balcani ed Europa centrale
- 1% America meridionale

(*) Inclusa la produzione info-valutativa nel contesto della tutela dei Contingenti nazionali dislocati nei teatri di crisi

AISI

INFORMATIVE/ANALISI INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA
ANNO 2015



- 48% Minaccia terroristica ed estremismo di matrice internazionale
- 19% Immigrazione clandestina e criminalità organizzata
- 16% Eversione ed antagonismo
- 14% Minacce alla sicurezza economica nazionale ed al Sistema Paese
- 3% Minacce allo spazio cibernetico ed alle infrastrutture critiche

lo popola e con quali intenzioni. L'arena virtuale del *web*, oltre a trascendere, per sua natura, la dimensione statuale, ed a moltiplicare le possibilità di accesso alla vita sociale, accresce gli strumenti a disposizione degli attori ostili e, allungando a dismisura i tempi di cognizione della minaccia, può indurre una percezione falsata di sicurezza. A rischio non sono soltanto gli Stati, ma anche gli attori privati, spesso oggetto di mire acquisitive ed esposti alla sottrazione di dati sensibili del loro patrimonio industriale e di conoscenze, ed ogni singolo individuo, che, in quanto nodo della rete, può subire in qualsiasi momento, e da qualsiasi punto della stessa, un impulso a venire colpito, nella dimensione digitale o con un attacco fisico nel territorio in cui vive.

Lungo la rete corrono le minacce che mirano a danneggiare i sistemi informatici da cui sono regolati i processi produttivi e le infrastrutture critiche. Quelle che puntano, attraverso la propaganda o la disinformazione, a radicalizzare le nostre società, ad influenzare surrettiziamente le nostre decisioni e le nostre affiliazioni. Quelle riferibili alla minaccia terroristica: DAESH *(vds. box n. 1)* si muove nella blogosfera come in un suo *habitat* naturale, ed i gruppi mossi da precisi disegni ideologici, o comunque ispirati al più cieco fondamentalismo, sfruttano l'agibilità di tale spazio senza confini per imporre, attraverso

box 1

DAESH, ISIL, ISIS O IS ?

Il termine DAESH rappresenta l'acronimo arabo di *al Dawla al Islamiya fi'l Iraq wa'l Sham*, ovvero *Stato Islamico dell'Iraq e dello Sham* (ISIS) o *Stato Islamico dell'Iraq e del Levante* (ISIL).

Nel tempo, l'organizzazione terroristica ha più volte modificato la propria denominazione. Sorta per iniziativa di Abu Musaab al Zarqawi come *al Tawhid wa'l Jihad* (*Unicità Divina e Jihad*), mutò nome in concomitanza con la dichiarazione di affiliazione ad *al Qaida* (2004), divenendo *al Qaida nella Terra dei due Fiumi* ovvero *al Qaida in Iraq* (AQI). Successivamente, dopo la morte di al Zarqawi (2006), alla sigla AQI iniziò ad affiancarsi, sulla scena eversiva irachena, quella di *Stato Islamico dell'Iraq* (ISI), prima filiale qaidista ad aver tentato – come evidenziato nella Relazione 2009 – di assumere rango di soggetto statuale. Sotto la guida di Abu Bakr al Baghdadi, l'ampliamento dell'attività operativa in Siria, alla fine del 2012, si accompagnò alla ridenominazione del gruppo in *Stato Islamico dell'Iraq e del Levante*, funzionale a coniugare la dimensione territoriale con quella di una realtà "di governo" che – abbracciando porzioni di due Paesi – non riflette i confini nazionali, poichè guarda alla dimensione transnazionale della *Ummah*. Infine, nel giugno

2014, il gruppo ha annunciato la costituzione dello *Stato Islamico*, confermando l'aspirazione ad espandersi oltre la regione mediorientale in attuazione dell'antico progetto, caro alla propaganda qaidista, di costituire un califfato mondiale.

A tutt'oggi, nei media come nei principali consessi internazionali la formazione di al Baghdadi è quindi richiamata con diversi acronimi: DAESH (peraltro "rifiutato" dall'organizzazione terroristica per la sua assonanza con un verbo arabo che significa "calpestare, distruggere, causare tensioni" e che evoca pertanto una valenza dispregiativa) e i suoi corrispettivi in lingua inglese ISIS/ISIL, nonchè il più recente IS.

Nella presente Relazione, ci si riferirà alla formazione terroristica con la denominazione di DAESH.

la violenza e la paura, le loro istanze politiche e la loro visione del mondo.

La seconda lente che i "Servizi segreti" hanno inforcato per leggere la realtà è riconducibile ai polimorfi ed indesiderati ***spin-off* della globalizzazione**. Protagonisti delle grandi dinamiche di cambiamento sono oggigiorno attori che si muovono al livello transnazionale, non necessariamente condizionati dall'esigenza di commisurare i mezzi disponibili agli obiettivi che coltivano, laddove gli Stati si confrontano, sovente, con stringenti vincoli di bilancio nel perseguire il rispettivo interesse nazionale.

L'imponente processo di redistribuzione del potere e della ricchezza su scala mondiale, in continuo e problematico divenire, ha quindi cambiato la natura delle sfide da fronteggiare, che promanano da cause assai diverse dai rapporti di potenza del "vecchio mondo". Occorre, piuttosto, guardare ad altri fattori: i vuoti di potere, che si creano là dove la sovranità statuale viene erosa da spinte disgregatrici di matrice identitaria, religiosa, etnica, tribale; i sottoprodotti della frammentazione e della regionalizzazione del sistema delle relazioni internazionali; le migrazioni di massa su scala globale (oltre 60 milioni di persone sottoposte a esodi forzati, delle quali circa 1,2 milioni sono entrate in Europa nel 2015 attraverso le rotte nordafricana ed anatolico-balcanica); l'incessante urbanizzazione che, in connessione con la scarsità di risorse alimentari ed idriche e con i cambiamenti climatici, provoca tensioni e porta all'esplosione di veri e propri conflitti; i centri di interesse antagonisti e concorrenti, intenzionati talvolta a colpire gli anelli deboli dei nostri assetti industriali, finanziari, scientifici, tecnologici, con lo scopo o l'effetto di appropriarsene e causarci un vero e proprio *downgrade* strutturale; le nuove possibilità di parcellizzazione internazionale dei processi produttivi, che aprono a loro volta inediti fronti di esposizione a contagi recessivi transnazionali.

Terzo binario, infine, quello delle **situazioni di instabilità geopolitica**, foriere di minacce "tradizionali", ma non per questo meno insidiose, anzi, in certi casi più raffinate e più aggressive che in passato: nella dimensione statuale, le consuete forme di ingerenza ostile, le attività di spionaggio, la proliferazione delle armi di distruzione di massa ed anche le battaglie di retroguardia di singoli attori inclini a colpi di coda totalitari, tenuto conto che solo il 40% della popolazione mondiale vive in condizioni di piena democrazia; quanto ai riverberi nel tessuto sociale, le insidie promananti dalla criminalità organizzata transnazionale e dai fenomeni eversivi.

La definizione delle priorità

Alla luce di tale affresco analitico, e nella cognizione di come il suo naturale orizzonte visuale rimanga il mondo, l'intelligence nazionale si è adoperata con costanza e determinazione per incrementare la sua capacità operativa ottimizzando il suo *mix* di risorse.

Tuttavia, nessuna intelligence, quali che ne siano "taglia" e prontezza di risposta, è in grado di anticipare "in qualsiasi momento qualsiasi minaccia da qualsiasi angolo del pianeta provenga". L'alea rimane inevitabile e, appunto per questo, se si vuole puntare al mondo, occorre, senza mai perdere di vista il quadro d'insieme, specializzarsi in alcune priorità. Nel caso italiano, un continuo, serrato, sintonico confronto con le Autorità politiche ha permesso di identificarle in una sfida territoriale, nonché, secondo una concettualizzazione riflessa nei capitoli che compongono la presente Relazione, in tre ulteriori grandi sfide di sistema.

Obiettivi "limitati", nei quali peraltro non si esaurisce tutta l'attività svolta nel 2015, ma che si sono rivelati di elevatissima valenza, là dove, corrispondendo alle richieste delle Amministrazioni e sovente anticipandole, si è riusciti a consentire al Governo di assumere le decisioni necessarie per garantire l'intangibilità delle componenti costitutive dello Stato e la sicurezza dei suoi cittadini, per preservare i fattori di crescita e di competitività del sistema economico, per perseguire i primari interessi statali.

Una sfida territoriale…

Il naturale campo di intervento dell'Italia, quello che conosciamo meglio, è il Mediterraneo, inteso come "Mediterraneo allargato", in termini geopolitici il *Broader Middle East and Northern Africa* (BMENA). È uno dei teatri geostrategici più complicati e più delicati per la sicurezza del pianeta: operarvi, anche in virtù del supporto informativo dell'intelligence, con piena coscienza delle sue criticità e delle sue opportunità, oltre ad essere ineludibile precondizione di sicurezza, equivale a garantire al Paese il profilo internazionale che gli compete. Non è, ovviamente, concepibile, in un mondo dove tutto è interdipendente, trascurare le altre aree di crisi, suscettibili anch'esse di riverberarsi sui

nostri interessi e dunque pesantemente incidenti sulla definizione degli indirizzi politici. Ma la centralità del BMENA rimane indubbia.

Basti peraltro considerare, come più sopra ricordato, che durante il 2015, anno caratterizzatosi per una forte *escalation* dei flussi lungo la direttrice dei Balcani occidentali, sono giunti nello spazio Schengen dalle rotte mediterranee quasi un milione di migranti in fuga da povertà e guerre (il *dossier* migratorio viene specificamente approfondito nel secondo capitolo della seguente Relazione).

Altro dato significativo è che, malgrado gli importanti cambiamenti intervenuti nell'ultimo biennio per motivi di ordine congiunturale, nel *mix* di approvvigionamento energetico nazionale l'Africa settentrionale continua comunque a garantire quasi un quinto del nostro fabbisogno.

Alle dinamiche in tale quadrante è stato, pertanto, prioritariamente rivolto l'impegno del Comparto, monitorando ed analizzando tanto gli sviluppi della situazione sul terreno quanto la postura di tutti gli attori coinvolti. Ciò per assicurare con tempestività, e secondo logica previsionale, all'Autorità di governo ogni elemento info-valutativo utile a definire le più feconde, e realisticamente percorribili, opzioni di *policy* per concorrere agli sforzi internazionali volti a promuovere la stabilizzazione regionale.

Al riguardo, a sviluppo ed in continuità con analoga direttrice di intervento degli anni precedenti, rilievo assoluto è stato riservato al presidio informativo in Libia, onde innervare di un dato intelligence il più possibile capillare ed accurato il ruolo profilato e fruttuoso svolto dal Governo a sostegno di quel Paese, culminato nella Conferenza di Roma del 13 dicembre. L'instabilità libica ha favorito la formazione, in quel territorio, di strutturate filiere jihadiste e di nuclei pro-DAESH e proprio da quelle coste sono partiti, nell'anno appena terminato, circa il 90% dei clandestini giunti in Italia via mare. È assai difficile limitare le attività terroristiche ed i traffici illeciti in una Libia instabile e divisa. Da qui, il convinto, ed "informato", contributo nazionale a quanto la comunità internazionale ha fatto per sostenere ed incoraggiare l'intenso e tenace *commitment* onusiano.

e tre sfide di sistema:

A delineare il complessivo profilo strategico dell'intelligence nazionale è, altresì, intervenuta la particolare cogenza ed impellenza con cui le evoluzioni di contesto hanno connotato tre dei macro-obiettivi della pianificazione informativa: il terrorismo internazionale, la *cyber security*, la sicurezza economico-commerciale e finanziaria. Minacce assai diverse quanto a matrice, fattori trasformativi ed impatto, e nondimeno accomunate da due caratteristiche peculiari: la loro natura ibrida; il fatto che sia possibile contrastarle, prevenirle ed anticiparle non con una difesa statica, bensì soltanto con una capacità di reazione più che proporzionale, in velocità ed in grado di affina-

mento, alla loro stessa capacità di adattarsi e sopravvivere all'impegno di chi le avversa.

il terrorismo…

Si ritrova, ovviamente, nelle pagine seguenti – plasticamente, prime della Relazione, e copiose – una rappresentazione tanto della minaccia jihadista in direzione dell'Europa, quanto delle sue declinazioni regionali (entrambe pesantemente condizionate dal protagonismo di DAESH ma tali da non esaurirsi in esso).

È doveroso, nel consegnare da una prospettiva intelligence alla memoria collettiva un anno tanto doloroso, evidenziare tre aspetti.

Anzitutto, l'offensiva del 13 novembre e la drammatica sequenza di episodi ad essa precedenti e successivi in Occidente ed in ogni angolo del pianeta, hanno delineato, oltre che un cambio di passo di natura tattica, anche un inquietante salto di qualità strategico della sfida posta dal terrorismo internazionale. DAESH ha dimostrato non soltanto di coniugare la dimensione simmetrica e quella asimmetrica, ma anche di modularle vicendevolmente in funzione del rispettivo livello di efficacia o criticità. Ne è uscita, in questo, corroborata la lettura della minaccia alla quale l'intelligence era già approdata, e che viene peraltro evocata nella Relazione sul 2014: si è infatti confermato uno scenario che vedeva corrispondere, ad un arretramento del *Califfato* sul terreno del confronto militare, una proiezione extraregionale, per l'appunto, di tipo asimmetrico.

Inoltre, la minaccia direttamente promanante dall'organizzazione e dai suoi emissari non sostituisce, piuttosto integra la pervasiva e pulviscolare formula basata sul *jihad* individuale, che matura attraverso processi di radicalizzazione condotti per lo più nella blogosfera, e sull'attivazione autonoma di lupi solitari e microcellule presenti in suolo occidentale. Anche in questa prospettiva, le eclatanti azioni di Parigi, a differenza di quelle dell'11 settembre, serbano un ulteriore elemento di pericolo, che è quello della loro riproducibilità in chiave emulativa: ciò quanto a scelta degli obiettivi – attinti da un ventaglio indefinibile di *soft target* dei quali è impensabile poter assicurare la protezione fisica – ed a predeterminata mediatizzazione. La minaccia così delineata, che può concretizzarsi per mano di un novero diversificato di attori, rende il "rischio zero" oggettivamente impossibile.

E tuttavia, non è concepibile alcuna reazione al di fuori del perimetro della legalità. A maggior ragione in un anno nel quale gli apparati nazionali sono chiamati a garantire la sicurezza di un evento di portata non nazionale, ma universale, quale il Giubileo, la strada maestra rimane quella di rispondere ad una sfida alla democrazia con le armi della democrazia, tendendo l'arco delle garanzie costituzionali senza mai nemmeno accennare a spezzarlo.

Si può e si deve innovare, per accrescere la capacità di prevenzione, anche con disposizioni normative inedite, quali quelle contenute nel decreto legge n. 7 del feb-

box 2

IL DECRETO LEGGE 18 FEBBRAIO 2015 N. 7 CONVERTITO CON MODIFICAZIONI DALLA LEGGE 17 APRILE 2015 N. 43 I PROFILI DI DIRETTO INTERESSE INTELLIGENCE

L'esigenza di affinare il dispositivo di prevenzione e contrasto del terrorismo, anche di matrice internazionale, a fronte di fenomeni emergenti come quello dei *foreign fighters*, ha portato al varo di un pacchetto di norme che prevedono, tra l'altro, il rafforzamento degli strumenti giuridico-operativi a supporto dell'attività degli Organismi di intelligence. Tra le misure introdotte:

- l'estensione del ricorso alle garanzie funzionali (art. 17 della legge 124) per una serie di condotte, alcune delle quali già previste come reato (tra le altre assistenza agli associati, arruolamento con finalità di terrorismo anche internazionale, addestramento ad attività con finalità di terrorismo anche internazionale, istigazione ed apologia del terrorismo, partecipazione ad associazione sovversiva e banda armata); altre di nuovo conio, introdotte dal decreto legge n. 7/2015, che puniscono anche gli arruolati e coloro che si autoaddestrano;
- la possibilità per le Agenzie di richiedere al Questore il rilascio del permesso di soggiorno allo straniero anche ai fini del contrasto dei delitti di criminalità transnazionale, con l'obiettivo di migliorare la penetrazione informativa volta a prevenire l'infiltrazione terroristica all'interno dei flussi migratori;
- la trasmissione al Comitato di Analisi Strategica Antiterrorismo (per l'informazione dei suoi componenti, ivi comprese le Agenzie), da parte dell'Unità di Informazione Finanziaria della Banca d'Italia (UIF), degli esiti delle analisi e degli studi effettuati sulle operazioni sospette riferibili ad anomalie sintomatiche di attività di riciclaggio o di finanziamento del terrorismo;
- in via transitoria, la possibilità, per gli operatori dell'intelligence – come già previsto per le Forze di polizia – di condurre colloqui in carcere con detenuti per finalità informative in materia di prevenzione del terrorismo di matrice internazionale;
- l'estensione da cinque a dieci giorni del termine per il deposito del verbale delle intercettazioni preventive di comunicazioni, tenuto conto che in molti casi gli "ascolti" dei Servizi di informazione riguardano comunicazioni in lingua estera, anche di idiomi e dialetti particolarmente rari, che richiedono un'attenta traduzione;
- previsioni dirette a garantire la tenuta della copertura degli appartenenti agli Organismi di informazione, nell'eventualità che siano chiamati a deporre in ambito giudiziario.

braio 2015 (*vds. box n. 2*) nonché nel decreto "Missioni" (garanzie funzionali per i reparti speciali delle Forze Armate), ma senza squilibrare il rapporto fra diritti e doveri dei cittadini. È eloquente, *inter alia*, che la possibilità per AISE ed AISI, previa autorizzazione dell'Autorità Giudiziaria, di *effettuare colloqui con soggetti detenuti o in-*

ternati, al fine di acquisire informazioni per la prevenzione di delitti con finalità terroristica di matrice internazionale, sia stata soggetta ad una limitazione temporale.

Si può e si deve continuare a fare pieno affidamento sulle consolidate sinergie tra intelligence e Forze di polizia, che trovano il loro alveo privilegiato in quella vera e propria *smart grid* genuinamente italiana che è il Comitato di Analisi Strategica Antiterrorismo. Al riguardo, anche nella prospettiva di continuare ad assicurare massima efficacia a tale modello, in coerenza con l'evoluzione del quadro legislativo, e nel rispetto delle competenze dei diversi soggetti istituzionali, nel maggio del 2015 il DIS ed il Ministero dell'Interno hanno sottoscritto uno specifico protocollo di intesa relativo allo scambio informativo tra i Servizi e le Forze di polizia, nel solco del continuativo impegno per la piena implementazione della Legge 124 avviato già nel 2007.

Si può e si deve conservare il sistema Schengen nella sua essenza e nell'imprescindibile patrimonio di valori che rappresenta, garantendo un nuovo equilibrio tra la libertà di movimento dei cittadini europei e la necessità di rafforzare la prevenzione della minaccia terroristica. È un bilanciamento viabile, là dove si lascia agli Stati il *data collecting*, e si compiono i dovuti salti in avanti nell'integrazione e nella interoperatività delle banche dati, intensificando contemporaneamente a tutti i livelli, a cominciare da quello intelligence, il *data sharing*.

Possiamo e dobbiamo, in ultima analisi, contenere nell'immediato ed in prospettiva sconfiggere la minaccia terroristica rimanendo uguali a noi stessi.

E per raggiungere questo obiettivo, non va dimenticato che il *jihad*, *in primis* quello incarnato da DAESH, dà prova di un elevatissimo grado di affinità con i tratti materiali ed immateriali della modernità.

Sono, in effetti, oramai emersi alla coscienza collettiva i lati oscuri della dimensione digitale e del linguaggio universale del *web*. È, però, fondamentale considerare che la capillarità di penetrazione del messaggio jihadista, e l'area di consenso che questo è riuscito a costruirsi, pongono all'attenzione un sottoprodotto indesiderato dell'era digitale che si distingue, sì, per la sua peculiare carica inquietante e per il suo specifico livello di rischiosità: ma che non è certamente l'unico.

…la minaccia cibernetica…

La rivoluzione cibernetica è suscettibile di incidere profondamente sul modo di fare intelligence. Si configura come "la" nuova frontiera, che cambia ogni fase e la natura stessa del processo informativo, ed impone un radicale cambio di abito mentale nella risposta, che deve essere veloce, organica, e preventiva.

A mente delle pertinenti disposizioni della Legge 124 del 2007 quale novellata dalla Legge 133 del 2012, è parte integrante della Relazione il Documento di Sicurezza Nazionale. Questo è ora per la prima volta comprensivo tanto dell'analisi dello stato della minaccia *cyber*, quanto di una articolata disamina del complesso di iniziative intese

a prevenirla e contrastarla, a riprova di una naturale osmosi fra l'attività svolta dall'intelligence e quella che spetta alle diverse componenti dell'architettura nazionale *cyber*.

Merita, su tutto, evidenziare come il necessario mutamento di approccio abbia concretamente preso forma nell'anno trascorso. La cornice giuridica – definita dalle leggi di riforma e dal DPCM del 24 gennaio 2013 – di un processo di modernizzazione del Sistema Paese nel quale l'intelligence assume un ruolo fondamentale sul versante della *cyber security*, si è dimostrata valida e lungimirante, poiché ha prefigurato, nella sua *ratio* e nel suo impianto, gli spazi per ulteriori, innovativi margini di intervento che consentissero di adeguare la risposta all'ininterrotto sofisticarsi della minaccia.

In particolare, il Quadro Strategico Nazionale ed il Piano Nazionale adottati nel dicembre del 2013 dal Presidente del Consiglio dei Ministri, la cui elaborazione è stata il primo punto del programma di lavoro del Tavolo Tecnico istituito presso il DIS per la "messa a sistema" delle diversificate capacità ed esperienze nazionali, ha consentito di compiere passi avanti assai importanti per il complessivo livello di crescita degli assetti *cyber* nazionali.

Dagli opportuni moduli di verifica a suo tempo previsti, è altresì emersa l'esigenza di irrobustire e fluidificare i meccanismi nodali del sistema: a tal fine, il Presidente del Consiglio dei Ministri, con apposita Direttiva del 1° agosto 2015, ha fissato puntuali linee d'azione per la realizzazione armonica degli indirizzi strategici ed operativi identificati nel Quadro Strategico e nel Piano.

Ne è elemento qualificante la triplice richiesta di procedere, con tempistica ristretta: al potenziamento del sistema di reazione ad eventi *cyber*; all'implementazione, da parte di tutti gli attori pubblici e privati dell'architettura nazionale, dei requisiti minimi di sicurezza cibernetica; all'adozione di coordinate iniziative interistituzionali rispetto a segmenti che, in quanto *game changer*, necessitano della massima integrazione degli sforzi, ossia il partenariato pubblico-privato, l'attività di ricerca e sviluppo e la cooperazione internazionale.

Ne è, parimenti, portato essenziale e di preminente valenza innovativa, l'ampliamento del coordinamento assicurato dal DIS nell'ambito dell'attività degli Organismi informativi, preordinato alla ricerca informativa di AISE ed AISI, ed inteso a conseguire, con una accresciuta leva rispetto alle minacce tradizionali, l'obiettivo di una risposta unitaria, tempestiva ed integrata al pericolo proveniente dal cyberspazio. La natura destrutturata dell'ambiente digitale sollecita infatti il Comparto a confrontarsi con un cambiamento strutturale, visto che è nella stessa rete che bisogna interagire per prevenire la minaccia. È dunque essenziale che l'intelligence rafforzi al massimo le proprie capacità di efficienza preventiva e di allertamento precoce dei fattori di rischio, ed a tale scopo una Direttiva attuativa varata dal Direttore Generale del DIS in novembre ha puntualmente disciplinato l'esercizio concreto di tale coordinamento

avanzato ed il funzionamento della prevista "cabina di regia" permanente.

Anche nella prospettiva di assicurare piena attuazione, in tutti i molteplici piani di incidenza, alla Direttiva UE in materia di sicurezza cibernetica il cui testo è stato approvato il 14 gennaio 2016, si dispone ora di una rinnovata cornice normativa, nonché di accresciute risorse finanziarie, specificamente stanziate. In tale quadro, le esistenti *partnership* pubblico-privato potranno più compiutamente ed efficacemente dispiegare le loro potenzialità, in un fruttuoso incontro dei ruoli che le imprese, e le Università ed i Centri di ricerca, rispettivamente giocano.

Forme di dedicata e rafforzata cooperazione sono, del resto, operative sin dal 2012, nel quadro dei regimi convenzionali da allora sottoscritti, e particolare significato è destinato a rivestire il *Polo Tecnologico per la Ricerca e lo Sviluppo*, varato nell'occasione dell'evento ICT4INTEL 2020, svoltosi anche nel 2015, con una cadenza annuale oramai consueta e sotto forma di "Stati Generali" della comunità intelligence nazionale con la partecipazione dell'Autorità Delegata per la sicurezza della Repubblica. Ad animare l'iniziativa è la volontà di promuovere una forte integrazione progettuale ed operativa, sul versante della sicurezza, tra intelligence, università ed aziende, ai fini della diffusione e condivisione delle capacità *high-tech* nazionali.

Il convinto e rilevante investimento nel partenariato con gli operatori privati deriva, d'altra parte, dalla consolidata cognizione che sono costoro a costituire i gangli vitali del tessuto economico nazionale, a custodire il patrimonio scientifico ed industriale che alimenta l'innovazione tecnologica di processo e di prodotto, a gestire le infrastrutture critiche i cui servizi sono essenziali per la sicurezza e la stessa sopravvivenza del Paese. Proteggerli e sostenerli, nei loro sistemi informatici e non solo, vuol dire tutelare e promuovere gli interessi italiani nel loro complesso, in termini di produttività, competitività internazionale e livelli occupazionali. In questo contesto, vale ricordare la recente presentazione del *Framework* Nazionale per la *Cybersecurity* da parte del Laboratorio Nazionale *Cyber*-CINI (Consorzio Interuniversitario Nazionale per l'Informatica): si tratta di un importante passo in avanti nel dotare le imprese italiane di ogni dimensione e settore di un quadro di autovalutazione strategica. Una progressiva adozione del *Framework* da parte del tessuto imprenditoriale nazionale permetterà di aumentare la consapevolezza del rischio anche ai massimi livelli della *governance* aziendale, in base ad un approccio di sistema ed in linea con le *best practices* internazionalmente riconosciute.

…e la minaccia economico-finanziaria

Il *driver* dell'interesse nazionale fa dunque trascendere, con determinazione e con tutti gli strumenti che la normativa mette a disposizione, la linea di divisione fra pubblico e privato, che va sfumando nei fatti ogni giorno di più. Ciò a maggior ragione nel contesto italiano, quello di un'economia di trasformazione che, sul piano congiunturale, va stabilmente incamminandosi, seppure con significative

differenze nelle dinamiche territoriali, nel sentiero di una ripresa che necessita di essere costantemente incoraggiata e sostenuta, sia nella domanda delle famiglie che nelle prospettive di investimento delle imprese.

Si apprezza, infatti, la tendenza al recupero dei livelli occupazionali pre-crisi, ad effetto dei provvedimenti riformatori varati per stimolarlo, ma non senza una inevitabile gradualità, tenuto conto del ritardo temporale con cui la domanda di lavoro segue l'attività economica, soprattutto in presenza di manodopera sottoutilizzata, come evidenziato dalla caduta dei livelli di produttività del lavoro degli ultimi anni e dalla forte contrazione dei margini di profitto. Da qui, il protrarsi di condizioni di disagio economico-sociale, con conseguenti fenomeni di strumentalizzazione ad opera di una variegata gamma di attori dell'estremismo, dei quali si dà conto nell'ultimo capitolo della Relazione.

La recessione che ha colpito l'Italia ha generato un impatto di lunga durata sulla struttura produttiva nazionale e sul prodotto potenziale. Anche per questi motivi, la ricerca di un nuovo paradigma di crescita postula un impegno corale di tutte le componenti del Sistema Paese, al quale l'intelligence, nell'assolvimento della missione istituzionale, è chiamata ad assicurare il suo peculiare contributo, riassumibile in due caratteristiche: calibrato e consapevole.

Calibrato. Ossia, secondo linee di intervento dettagliate nel terzo capitolo della Relazione, finalizzato a fornire all'Autorità politica elementi conoscitivi ed info-valutativi utili per conseguire cinque obiettivi essenziali: proteggere gli assetti strategici nazionali e le "filiere della sicurezza"; tutelare la solidità del sistema creditizio e finanziario nazionale; perseguire le economie illegali, nelle loro diverse manifestazioni, inclusi i fenomeni corruttivi; individuare le condotte pregiudizievoli per gli interessi erariali, comprese quelle sviluppate in tutto o in parte in territorio estero; discernere fra gli investimenti esteri che favoriscono l'integrazione del sistema economico nei mercati internazionali – accrescendo la dotazione di capitale fisso per addetto e generando ricadute positive in termini di occupazione e politiche industriali – e le acquisizioni straniere mosse invece da intenti puramente speculativi, o concepite per acquisire il patrimonio di conoscenze e di *know-how* tecnologico.

Consapevole, in una duplice declinazione.

Cosciente, in prima battuta – ferma restando l'assoluta necessità di non interferire nel libero svolgersi delle vicende economiche – delle condizioni strutturali di competitività dell'economia nazionale. Se, da un lato, le imprese italiane coinvolte nelle catene globali del valore svolgono, non nella loro totalità ma in prevalenza, le attività intermedie della produzione internazionale e si presentano meno terziarizzate e meno internazionalizzate rispetto a quelle operanti nei processi finali della filiera, dall'altro è assai significativo che si sia registrato un impatto attutito dell'ondata recessiva degli anni 2011-2013 sulle piccole e medie imprese italiane inserite

in processi produttivi globali. Ciò in quanto l'appartenenza a *global value chains* ha mitigato le pressioni provenienti dalle difficoltà dell'economia interna, e contestualmente ha assicurato l'accesso oltre confine a nuove nicchie per la fornitura di beni e servizi, per la sofisticazione dei processi produttivi, per l'accesso a capitali freschi e per lo sviluppo tecnologico. Si tratta di un dato cruciale per la definizione di un nuovo paradigma di crescita, da tenere in conto anche nell'utilizzo della leva intelligence, nella misura in cui, come da ultimo sottolineato anche nel *Rapporto sulla situazione sociale del Paese 2015* del Censis, "globalità, orientamento alla tecnologia ed alla creatività innovativa" sono ingredienti fondamentali per affrontare con successo i mercati. È da considerare che le nostre esportazioni, indirizzate non soltanto verso i mercati emergenti, ma anche verso quelli maturi, valgono quasi il 30% del PIL, quota cresciuta anche negli anni della crisi. Il *made in Italy* ha mostrato una elevata capacità di riadattamento al nuovo contesto globale, incarnandosi in una gamma di prodotti ad alto valore aggiunto e di servizi ancor più ampia delle consolidate e sempre vitali tipologie dello "stile italiano": va, anche in quanto tale, protetto e promosso.

Allo stesso tempo – secondo profilo della "consapevolezza" – se dato intrinseco delle dinamiche di mercato è la concorrenza basata su produttività, competitività di costo, presenza sui mercati esteri e servizi ad alta intensità di conoscenza, occorre avere lucida nozione che la fisiologia può essere alterata dall'utilizzo sleale di leve non convenzionali, e quindi da tale rischio va salvaguardata. Essendo sempre più intensa la concorrenza fra sistemi Paese per il controllo delle tecnologie chiave, l'attività occulta finalizzata ad acquisire segreti industriali e proprietà intellettuale è infatti in forte espansione in tutto il mondo. Per questi motivi, è fondamentale il ruolo dell'intelligence economica nell'individuare per tempo le minacce rivolte agli interessi scientifici, tecnologici ed industriali della Nazione. Senza, peraltro, dimenticare che l'approccio degli attori anche statuali, in questo campo, può essere sì solo "difensivo", ma può essere pure più marcatamente "offensivo".

Cosa ha fatto l'intelligence. Quattro parametri di riferimento:

Indotti dunque dalla loro "ermeneutica dei fatti" e dalla discendente individuazione di imperativi prioritari, gli Organismi informativi nazionali hanno voluto e dovuto responsabilmente porsi il problema di individuare un *mix* innovativo dei propri tratti fisionomici. Il Comparto, rimanendo immutato nel suo perimetro normativo (quale definito dalle Leggi 124 del 2007 e 133 del 2012 e dalle discendenti disposizioni attuative), fedele alla propria missione istituzionale ed ai suoi valori costitutivi, e costantemente incardinato negli strumenti di controllo – coprotagonista, nella feconda ed armonica collaborazione con il COPASIR, di una straordinaria e sempre aperta pagina di democrazia parlamentare – ha informato *modus operandi* e "cultura aziendale" a quattro parametri di

riferimento. Questi hanno dato corpo, nel loro insieme, ad un modello di intelligence "all'altezza del compito", in grado di tenere il passo delle sempre cangianti condizioni e prospettive di sicurezza, nonché grimaldello indispensabile per la competitività geopolitica e geoeconomica di un Paese come l'Italia, inevitabilmente collocato dalla geografia, dal tessuto produttivo e dalle dinamiche di cambiamento sociale lungo la linea di faglia delle grandi trasformazioni globali. Un modello "a tendere", certo, ma anche un concreto ed incessante *work in progress* a sviluppo della "rifondazione" del 2007, dimensionato sulle risorse e sulle potenzialità del sistema Paese.

…visionaria…

Un'intelligence **visionaria**, anzitutto. In quanto finalizzato agli obiettivi individuati dall'Autorità di governo ed approvati dal Comitato Interministeriale per la Sicurezza della Repubblica, il processo informativo ha continuato, nel suo impianto, ad essere definito dal ciclo di azioni articolato sulle tre fasi canoniche dell'acquisizione della notizia, della sua trasformazione analitica in contributo conoscitivo articolato e della conseguente disseminazione ai decisori. Questi ultimi, nondimeno, sono chiamati ad affrontare scenari globali caratterizzati da minacce ibride ed imprevedibili, da crescente volatilità strategica e da modelli sociali complessi, talché necessitano anche di uno "sguardo lungo", della capacità di vedere ben oltre le contingenze e le emergenze del momento. È giocoforza che il vertice politico e la classe dirigente nel suo complesso chiedano all'intelligence di estendere il loro campo visuale. Anche per corrispondere a queste aspettative, il 2015 ha segnato l'avvio di un nuovo modulo di pianificazione informativa, articolato su un respiro triennale.

…transnazionale…

Transnazionale, inoltre, sulla base di un principio di divisione del lavoro. L'attività dei Servizi è troppo intimamente legata alla sovranità di ciascun Paese per potersi mai realisticamente pensare di affidarla a veri e propri Organismi sovranazionali. Sta di fatto, però, che ogni intelligence si muove in un ambito dove la capacità di scambiare informazioni costituisce metro di valutazione della sua efficienza. Di conseguenza, se, da un lato, solo chi è in grado di acquisire autonomamente informazioni affidabili può giocare un ruolo di primo piano, dall'altro occorre puntare su formati di stretta cooperazione, basati sulla fiducia reciproca e sul condiviso interesse a prevenire e contrastare minacce di portata globale, prima fra tutte quella terroristica. L'obiettiva necessità, per ciascun Servizio, di agire in maniera complementare con gli omologhi esteri ad esso collegati implica il superamento degli steccati domestici a favore di forme sofisticate di *information sharing* al livello internazionale. Ciò in maniera non indiscriminata, ma funzionale al perseguimento delle più rilevanti priorità. È del tutto fisiologico

che, anche fra Paesi amici ed alleati, non sia sempre piena la convergenza di vedute e di obiettivi. Il peso di ciascun Comparto nazionale nel "mercato" dell'intelligence mondiale è funzione della sua capacità sia di mettere pienamente a frutto le sue autonome potenzialità che di essere selettivo nella cooperazione: lucido nella tutela dei propri interessi, attento, in un mondo caratterizzato da accesa competizione, a non farsi contaminare da quelli altrui ed altrettanto determinato a ricercare spazi di confronto, dialogo, scambio e sinergia là dove non è più né possibile né auspicabile "fare da soli".

…integrata…

Ovvio che l'intelligence debba essere **integrata,** prima ancora che verso l'esterno, in prima battuta al suo interno. I *target* da monitorare si sono moltiplicati e frammentati, sono meno visibili, più diversificati e pulviscolari rispetto ai pochi, grandi bersagli di un tempo. Le minacce asimmetriche, neutre rispetto alla marcatura territoriale, come quelle terroristica (*in primis* la galassia jihadista), economico-finanziaria, cibernetica, richiedono una raccolta informativa ed una correlata valorizzazione analitica, non più soltanto *border driven*, ma prevalentemente *topic driven*, ossia rivolte in prima battuta ai fenomeni, prima ancora che alla geografia dei vettori di rischio. La sicurezza interna e quella esterna non possono, pertanto, essere più pensate come due realtà separate. Ciò rende essenziale il coordinamento centripeto e produttivo che il DIS svolge per assicurare l'unitarietà del Sistema di informazione per la sicurezza della Repubblica, posto *in toto* sotto la responsabilità del Presidente del Consiglio dei Ministri.

È, in relazione a tanto, significativo come la funzione di coordinamento introdotta dalla Legge 124 – intesa a ricondurre l'intera attività del Comparto a livelli di responsabilità certi ed a semplificare la catena decisionale a vantaggio dell'operatività delle Agenzie – abbia progressivamente assunto un rilievo non relegato al solo ambito informativo ed operativo, bensì declinato in tutti i settori di intervento per i quali la legge richiede il raccordo delle Agenzie.

Il coordinamento è dunque concepito in termini avanzati e rafforzati, per proiettarsi in modo trasversale su tutti gli snodi del ciclo intelligence, quale prerequisito ineludibile per la compiuta integrazione del "dato *intel*" nei processi decisionali di governo: per questi motivi, esso accomuna, a diversi livelli di intensità ma sempre secondo il criterio di un cosciente "gioco di squadra", l'attività info-operativa, l'analisi, la protezione cibernetica e la sicurezza informatica, l'accesso alle banche dati, i rapporti con le Forze di polizia, gli strumenti giuridici ed operativi, l'*Open Source Intelligence*.

…ad azionariato diffuso

Nell'era delle minacce geotraslate, infine, la sicurezza del Paese può essere promossa solo attraverso uno sforzo partecipato, innestato su una cultura condivisa che renda attori

della sicurezza, al fianco dei valorosi professionisti dell'intelligence, quegli stessi soggetti che oggi possono rappresentare l'obiettivo di azioni ostili da parte di soggetti statuali, terroristici o criminali. Si tratta, peraltro, di uno sviluppo che è "nelle cose". L'essere parte della rete tecnologica, che della globalizzazione è il vero paradigma, implica, per ciascun individuo, che gli elementi essenziali della sua sfera personale siano già digitalizzati *out there* e nella disponibilità dei *big player* privati. Non può non porsi un conseguente problema di ampliamento del perimetro di azione dell'Autorità pubblica chiamata a tutelare la sicurezza nazionale. È la forza dei fatti che porta a ritracciare il confine che in passato separava sicurezza e *privacy*. L'importante è che tale adattamento non sia affidato solamente all'autodisciplina di buon senso degli Organismi intelligence, ma avvenga in un quadro di regole ben definito e sia sottoposto ad adeguati meccanismi di controllo. Fermo restando che controllore efficace è *in primis* il cittadino, nella misura in cui egli acquisisce consapevolezza della necessità che i singoli nodi della rete contribuiscano attivamente alla produzione della sicurezza, divenendo, in tal modo, socio di una "intelligence ad azionariato diffuso". La "rivoluzione digitale" si distingue infatti dalle precedenti poiché non ha al centro le masse, bensì l'individuo, *super empowered* nella sfera virtuale, verso la quale tendono a migrare, sino a sublimarsi, la sua unicità e specificità, i suoi diritti e doveri.

Dove va l'intelligence. Una maggiore capacità operativa:

Se questi sono i quattro tratti distintivi di un'intelligence moderna, che si dimostri, ad un tempo, "**adattiva, reattiva e proattiva**", gli Organismi non possono certamente permettersi di indulgere ad astrattismi da laboratorio. È invece doveroso, per essi, nell'economia del Sistema delineato dalla legge e dalle norme attuative, ordinative ed organizzative: essere realisticamente coscienti delle loro effettive possibilità; adoperare gli strumenti disponibili in ragione della concreta gittata; fare tesoro dell'esperienza accumulata per dilatare i confini del loro campo di operatività, commisurandoli agli equilibri dinamici di un mondo in continua trasformazione. Ciò, sempre nel più rigoroso rispetto della distinzione di ruoli tra la politica che crea i fatti, e l'intelligence che, a beneficio della politica, li legge oggettivamente, *sine ira et studio*, ne discerne le implicazioni, ne stimola le evoluzioni nella direzione collimante con gli interessi della Nazione e coi principi costituzionali, operando sotto il controllo parlamentare.

È sulla base di tale spirito di responsabilità istituzionale che, in un anno particolarmente complesso quale è stato il 2015, l'agenda del Sistema di informazione si è snodata lungo una linea di azione precisa: l'accrescimento della propria capacità operativa. E si è efficacemente operativi solo nella misura in cui si è aggiornati nelle caratteristiche che "fanno la differenza": nel caso dell'intelligence, lo è la piena integrazione della dimensione umana e di quella tecnologica.

il fattore umano…

Il fattore umano rimane determinante ed imprescindibile per l'assolvimento di almeno cinque dei compiti che qualificano la missione del Comparto. Il primo consiste nell'offrire al decisore politico interpretazioni di contesto e scenari previsionali, al fine di sostenerne le scelte in presenza di quadri situazionali complessi che, condizionati da variabili plurime, postulano tempi di reazione sempre più veloci. È un terreno sul quale ogni democrazia dispiega l'abilità nel gestire al meglio il proprio capitale di *soft power*, fondamentale per la resilienza e per la proiezione internazionale del Sistema Paese. Connessa a tale funzione vi è (secondo compito) quella di esercitare una capacità di influenza strategica, cambiando, allorché utile alla Nazione, la situazione sul terreno. Sono, entrambi, compiti che ne presuppongono ulteriori tre: cogliere la reale dimensione dei fenomeni, dei rischi e delle minacce; colmare, anche con metodi non convenzionali quando necessario, i *gap* informativi; valutare l'attendibilità delle informazioni raffrontandole con il patrimonio di conoscenze pre-esistente.

Si tratta, in altri termini, di essere artigianali per dedizione, cura e qualità del lavoro, ma di trascendere la limitatezza della dimensione artigianale nel peso specifico del prodotto. La politica di reclutamento ha, conseguentemente, continuato ad essere imperniata sulla selezione dei profili attitudinali e psicologici più adatti, individuando le professionalità migliori anche nella società civile, nelle università, nei *think tank*, per poi promuoverne il necessario amalgama con quelle, essenziali, provenienti dalle Amministrazioni dello Stato, a partire da Forze di polizia e Difesa. Al contempo, non sono stati lesinati sforzi e investimenti affinché la Scuola (sempre più "Campus") di Comparto proseguisse nella direzione di una moderna, capillare e continua attività di formazione, cruciale per garantire che quanto seminato fruttificasse. Del resto, i gestori del processo informativo non avrebbero potuto essere attrezzati per interpretare la realtà contemporanea con il grado di sofisticazione sopra illustrato se non avessero potuto trarre profitto da peculiari esercizi didattici ed addestrativi, affinati negli ultimi anni anche grazie ad un costante e fruttuoso *outreach* verso i poli accademici della Penisola, con il *roadshow* inaugurato nel 2013 e con esercizi dedicati. L'obiettivo guida sarà, sempre più, quello di favorire la piena integrazione di tutte le professionalità e disegnare il profilo ideale delle risorse umane dell'intelligence.

…e il fattore tecnologico

Il lavoro degli agenti operativi e quello degli analisti conserverà sempre, secondo il principio della continuità fra ricerca ed analisi, tutto il suo valore contenutistico, euristico e metodologico. Ciò, tuttavia, in chiave di costante complementarietà con quello straordinario moltiplicatore di potenziali-

tà costituito dall'impiego dell'intelligence tecnologica nelle sue varie declinazioni (*sigint, imint* e *techint*), fondamentale per rafforzare l'operatività dei professionisti sul campo.

L'intuito di questi ultimi, del quale non si potrà mai fare a meno, sarebbe monco senza tecnologia, così come un'intelligence di sola tecnologia, senza risorse umane adeguatamente preparate e formate, sarebbe cieca, incapace di "unire i puntini" e di restituire al Vertice politico la visione olistica e, ad un tempo, dettagliata delle situazioni e dei fenomeni. Quel che occorre adottare è un approccio complesso ed armonicamente sistemico delle diverse componenti del Comparto intelligence.

Agli ingredienti tradizionali dell'analisi, talvolta in comprensibile affanno rispetto ai tempi stringenti della politica, deve essere affiancato un forte investimento tecnologico per poter sviluppare, in coerenza e compiuta sinergia con il fattore umano, le differenti fasi analitiche, garantendo al prodotto informativo tempestività, accuratezza ed osmosi con i meccanismi decisionali di governo.

La tecnologia ha, in verità, mutato nel profondo la maniera di agire dell'intelligence, il cui ciclo "classico", quale ereditato dalla Guerra Fredda, non appare più calibrato a coprire il nuovo panorama della minaccia. In particolare, la capacità di accesso alle banche dati ha cambiato la natura della raccolta informativa, ampliando la costellazione delle fonti e ponendo in termini non scontati l'interazione col tradizionale strumento *humint*. La rivoluzione digitale ha, del pari, ridefinito il momento dell'analisi, che ora può beneficiare a sua volta del processo tecnologico, nonché innovato, nel rapporto col potenziale *target* di azioni ostili, i paradigmi operativi, reindirizzando progressivamente questi ultimi dalla nozione di *security service* verso quella di *protection service*.

Gli Organismi sono, quindi, determinati a perseguire l'integrazione piena dell'*Information and Communication Technology* nella loro attività con pari dignità delle più tradizionali forme dell'approvvigionamento di informazioni: ciò non come fine in sé, bensì come strumento di importanza assoluta per garantire all'intelligence il suo "futuro sostenibile", poiché sono i nuovi paradigmi a richiedere approcci e tecnologie completamente differenti rispetto al passato.

Un'intelligence tre volte responsabile

Visionaria, dunque, l'intelligence uscita dalle prove difficili di un'annata che è parsa compendiare in sé le sfide di un'epoca, ma allo stesso tempo lucidamente conscia delle proprie effettive possibilità.

Solo in termini residuali parte degli *arcana imperii*, piuttosto incline a guardare alla segretezza come ad una modalità, quando necessaria, di lavoro e di tutela collettiva, non come ad un fine in se stesso.

Conoscibile nella sua funzione e nella sua utilità sociale, in continuità con una politica di apertura coerentemente con-

dotta negli anni ad ogni livello, e giunta a puntare finanche sulla fantasia e sulla creatività dei giovanissimi studenti della scuola primaria, con l'innovativo concorso *Disegna l'intelligence*, per promuovere negli adulti di domani la necessaria cultura condivisa della sicurezza, ad ulteriore ed emblematico fondamento di quello sforzo corale che solo può garantire la protezione di supremi beni e valori che per loro natura appartengono a tutti.

Legittimata dal patto di fiducia stretto con l'Esecutivo, con il Parlamento, e con i cittadini, là dove oltre sei italiani su dieci (dato *Eurispes*) tributano un gradimento esplicito al ruolo centrale che compete agli Organismi informativi, pienamente integrati nei meccanismi decisionali di governo, per la protezione degli interessi fondamentali della Nazione.

Un'intelligence, pertanto, "tre volte responsabile". Perché gravata unanimemente della responsabilità primaria di garantire la sicurezza, che si è configurata, e viene percepita, quale figlia della prevenzione *ex ante* ben più che dei correttivi *ex post*. Perché responsabilmente impegnata a selezionare le sue priorità e ad assicurare il dimensionamento ottimale degli obiettivi rispetto ai mezzi, rispondendo delle proprie scelte. Perché all'ampliarsi del suo campo di azione, al suo svolgere sempre più una funzione di "difesa attiva" delle libertà e dei diritti, l'intelligence, entro il quadro giuridico posto dall'ordinamento al suo operato, si contraddistingue per la responsabilità di rendere la democrazia più forte, in quanto capace di decidere, più solida, poiché in grado di scegliere, più resiliente, cioè all'altezza di reggere la sfida della competizione.

Il binomio fra intelligence responsabile e cittadinanza consapevole può non essere sufficiente, da solo, a garantire alla Nazione una cornice securitaria meno insidiosa e più decifrabile. Ma è indispensabile per tali scopi, e dunque per la democrazia.

I FRONTI DEL *JIHAD*

I FRONTI DEL *JIHAD*

Il protagonismo di DAESH sulla scena globale

Il 2015 come detto ha segnato un salto di qualità nella minaccia posta da DAESH, con operazioni a forte impatto programmate e rivendicate in risposta all'intervento militare internazionale nei territori del *Califfato*.

Gli attacchi di Parigi del 13 novembre, preceduti, il 31 ottobre, dall'attentato all'aereo di linea della compagnia russa *Metrojet* nell'area del Sinai, hanno rappresentato, ad un tempo, un cambio di passo, ma anche una conferma della strategia offensiva di DAESH, la cui proiezione terroristica si accompagna all'autolegittimazione quale soggetto statuale dichiaratamente intenzionato a ridisegnare la geografia del potere nell'area mediorientale a favore della componente sunno-salafita.

L'insediamento nel contesto siro-iracheno di una realtà "di governo" di matrice jihadista s'inscrive nel più ampio progetto di califfato globale – evocato anche da altri gruppi terroristici, inclusa *al Qaida* – e si prefigge l'annientamento del "nemico", identificato negli "infedeli" occidentali, negli ebrei e nei cristiani, ovunque presenti, oltre che nei musulmani sunniti "apostati" e negli sciiti "eretici".

In tale prospettiva, la determinazione a consolidare DAESH in Iraq ed in Siria, sia attraverso le conquiste militari che tramite una intensa opera di indottrinamento – anche forzoso – delle popolazioni locali, e l'ambizione ad estendere il *Califfato* al di là del Medio Oriente rappresentano due aspetti peculiari del medesimo processo.

La campagna espansionistica territoriale ha assunto quindi un rilievo centrale nella propaganda di DAESH, interessato, da un lato, a sfruttare il "ritorno d'immagine" correlato al moltiplicarsi dei segnali dei consensi raccolti (anche a detrimento

di *al Qaida*) nei quadranti africani e asiatici più segnati dall'attivismo jihadista e, dall'altro, a stabilire in Libia una roccaforte dalla quale poter coordinare gruppi, cellule e militanti che nella regione nordafricana hanno giurato fedeltà ad al Baghdadi. In altre parole, la spinta espansiva di DAESH si è mossa, allo stesso tempo, sul piano propagandistico e tattico-operativo, facendo perno sulle aspirazioni di formazioni locali, dichiaratesi alleate e, in qualche caso, anche *wilayat* (province) del *Califfato*, termine che evoca la connotazione territoriale e amministrativa propria di un'entità statuale.

Così la formazione irachena, a differenza di *al Qaida*, ha mostrato di incoraggiare e "accettare" l'affiliazione di realtà jihadiste anche eterogenee. In tale cornice si inseriscono l'ufficializzata alleanza con la nigeriana *Boko Haram*, l'attivismo nel Maghreb di cellule che si richiamano all'organizzazione di al Baghdadi, l'adesione a DAESH di *Ansar Bayt al Maqdis* in Egitto, che ha associato alla propria denominazione quella di *Wilayat Sina'* (Provincia del Sinai), l'emergere di sigle pro-DAESH a Gaza, nello Yemen, nel quadrante afghano-pakistano e nel Sud-Est asiatico, con ulteriori interventi in Asia Centrale, specie nel Daghestan e in Cecenia, e nella regione del Caucaso.

Lungo il medesimo asse afro-asiatico, alle velleità di DAESH ha corrisposto – con vari livelli di visibilità – la persistente determinazione operativa dei gruppi riconducibili ad *al Qaida*.

La comunicazione multidimensionale

L'attività di propaganda si è confermata uno dei pilastri su cui si fonda la proiezione espansiva di DAESH, che ha creato una complessa rete di diffusione dei propri messaggi, soprattutto sul *web*, diretta alla sensibilizzazione e alla radicalizzazione di eterogenei *target* di pubblico attraverso l'utilizzo di numerosi canali e piattaforme.

Si tratta di una strategia "promozionale" che non conosce confini – come senza confini è l'uditorio di riferimento, rappresentato, nelle intenzioni di al Baghdadi, dall'intera comunità dei musulmani (*Ummah*) – rispondente a finalità diverse e complementari: l'affermazione di potenza, il reclutamento di *mujahidin*, l'estensione dell'area di sostegno, l'amplificazione dei "successi" ottenuti, la pressione sul "nemico", la giustificazione pseudo-religiosa delle violenze più efferate.

L'uso a scopo propagandistico dei *media* appare dunque funzionale alla capacità d'imporsi di DAESH, che sfrutta le potenzialità del mondo della comunicazione mediante una narrativa a modulo variabile e di grande impatto: dalle minacce all'Occidente all'esaltazione del sistema sociale vigente nel *Califfato*, dall'incitamento a colpire i Governi dei Paesi musulmani che cooperano con i nemici alle invettive nel segno dell'odio settario. Tutte chiavi, queste, di un distorto e radicale pan-islamismo populista che:

- assume la violenza come elemento costitutivo della propria identità;

- enfatizza e celebra la *bellezza* del *sacrificio* e promette *redenzione, ordine e giustizia*;
- rifiutando confini e nazionalità, acquista valenza unificante agli occhi dei volontari provenienti da tutto il mondo, per certi versi accreditando, nell'immaginario dei *mujahidin*, un superamento dell'idea stessa di *foreign fighter* (chi è "straniero" quando i confini sono aboliti ed un "nuovo ordine" si sta creando?).

La modulazione del linguaggio, ora pseudo-ieratico, ora didascalico e semplificatorio, è favorita dalla varietà degli strumenti e dei veicoli impiegati. L'organizzazione si avvale a tale scopo: dell'*expertise* delle sue case di produzione (la più nota delle quali è *al Hayat Media Center*) che si rivolgono ad un pubblico soprattutto occidentale; di una vasta platea di sostenitori e simpatizzanti che si raccordano utilizzando i *social network*; della pubblicazione di alcune riviste, anche in lingue occidentali (su tutte, *Dabiq*, edito sin dal 2014 in inglese, *Dar al Islam* in francese, *Costantinople* in turco, *Èctok* in russo); della divulgazione di una consistente quantità di video di ottima fattura e dalle tecniche diversificate, nei quali la violenza delle immagini – propria di certa "guerra psicologica"– si alterna a filmati di taglio documentaristico/celebrativo.

Nel quadro di tale strategia propagandistica rientrano inoltre: la pubblicazione di *brochure* che incoraggiano a trasferirsi nei territori sottoposti al controllo di DAESH; la produzione di canti ed inni, principalmente affidata alla *Ajnad Media Foundation*, specializzata proprio nella realizzazione di *file* audio; la diffusione di videogiochi; la progettata apertura di un'emittente televisiva, *KhilafaLive,* ispirata ai canali *all-news*; l'attività di controinformazione in stile giornalistico.

A fronte della vitalità dimostrata da DAESH nel cyberspazio per tutto quello che attiene al piano propagandistico, è opinione concorde che la formazione – e, più in generale, il terrorismo jihadista – nella fase attuale non abbia la capacità di sferrare attacchi di portata rilevante nell'ambiente digitale, ma è possibile che nel tempo tale capacità possa essere acquisita e sfruttata (*vds. box n. 3).*

LA MINACCIA IN EUROPA

Estremisti *homegrown, foreign fighters, returnees, commuters…*

Nel quadro dell'avanzata di DAESH sulla scena internazionale ed alla luce delle evidenze attestanti il ruolo giocato da *foreign fighters* di estrazione europea nella promozione, pianificazione e realizzazione di azioni violente nel Vecchio Continente, hanno assunto peso crescente, nel panorama della minaccia, i cd. *homegrown mujahidin*, soggetti nati o cresciuti o radicalizzatisi in Occidente (sia convertiti sia *reborn muslims*, vale a dire immigrati di seconda/terza generazione che hanno riscoperto l'Islam in chiave estremista), pronti a convergere verso le zone del *Califfato* o a compiere il *jihad* sui territori di residenza.

box 3

IL *CYBER JIHAD*

Nel dominio cibernetico non si ha evidenza, a tutt'oggi, di azioni terroristiche finalizzate a distruggere o sabotare infrastrutture ICT di rilevanza strategica, ma è ragionevole ipotizzare che, nel futuro, tali obiettivi possano effettivamente rientrare negli indirizzi strategici del cd. *jihad* globale, aggiungendo, quindi, una nuova dimensione alla minaccia terroristica.

A tale proposito sono da notare:

- la campagna di ricerca e reclutamento *on-line* di *hacker* mercenari o ideologicamente motivati, per sostenere le operazioni di DAESH;
- la crescente casistica di attacchi informatici (invero sinora a basso impatto) realizzati ai danni di sistemi informativi di soggetti pubblici e privati occidentali, non particolarmente sensibili, da *crew*, che, per la denominazione o il contenuto delle loro rivendicazioni, fanno chiaro riferimento al *jihad* e a DAESH. Ad oggi, comunque, non si è riscontrata l'effettiva riconducibilità di tali *crew* al contesto jihadista e a DAESH in particolare, in quanto potrebbe anche trattarsi di una mera trasposizione emulativa nel dominio cibernetico delle iniziative propagandistiche di matrice jihadista. In ogni caso, i sistemi *target* risultano essere stati selezionati e colpiti in ragione delle loro vulnerabilità di configurazione.

Il fenomeno dei *foreign fighters* ha ormai superato, in termini numerici, qualsiasi precedente afflusso di combattenti stranieri in un teatro di *jihad* (Afghanistan, Bosnia, Iraq). Gli aspiranti *mujahidin* partiti per la Siria e l'Iraq sarebbero, secondo stime, circa 30.000 (tra combattenti attivi, rientrati nei Paesi di origine, arrestati e deceduti), provenienti da più di 100 Nazioni. Quasi il 60% di essi sarebbe partito dal Medio Oriente (con Arabia Saudita e Giordania in testa) e dal Nord Africa (principalmente da Tunisia e Marocco). Più di 5.000 combattenti proverrebbero inoltre dall'Europa. Significativamente nutrita sarebbe la componente dei Balcani occidentali, con più di 900 volontari da Kosovo, Bosnia Erzegovina, FYROM e Albania, a conferma della centralità assunta dalla regione d'Oltreadriatico nelle dinamiche dell'estremismo islamista.

Un altro dato di rilievo è rappresentato dall'accresciuto afflusso nei teatri di *jihad* di interi nuclei familiari e di giovani donne, cui sono assegnati spesso, ma non solo, compiti domestico-amministrativi (*vds. box n. 4*).

box 4

LE DONNE DEL *JIHAD* COMBATTENTE

La presenza di donne nel terrorismo di matrice jihadista ha conosciuto una rapida espansione in concomitanza con l'affermarsi di DAESH, come dimostrato dal crescente numero di aspiranti *mujahidat* europee, per lo più giovani e di varia estrazione sociale, che tentano di raggiungere il teatro siro-iracheno.

Il loro compito principale è quello di essere mogli e madri dei *mujahidin*: a questo fine, scopo del viaggio è solitamente il ricongiungimento con il proprio coniuge già sul fronte o l'unione con un militante conosciuto anche via internet nel *jihad al nikah* ("matrimonio per il *jihad*"), in adesione ai proclami di DAESH nei quali si esortano le musulmane a contribuire al popolamento del *Califfato* e ad "allevare" le nuove generazioni, nonché a sostenere il morale dei combattenti. Tuttavia, non mancano casi di estremiste impegnate in attività di proselitismo e reclutamento (soprattutto *on-line*, ove esisterebbero dei circuiti ad "esclusivo" ambito femminile), di supporto logistico (ad esempio, trasportando denaro) e di natura operativa. Emblematica, tra l'altro, la creazione in Siria e Iraq di due brigate di DAESH composte da sole donne (tra le quali la "celebre" *al Khansaa*, attiva a Raqqa), entrambe con compiti prevalentemente di "polizia", specie per la rigida verifica che la condotta della popolazione femminile sia in linea con i dettami sharaitici.

Il montante fenomeno del *jihad* al femminile ha imposto un affinamento degli strumenti di contrasto all'estremismo violento. Vanno lette in questo senso, ad esempio, le *Good Practices on Women and Countering Violent Extremism*, adottate nell'ambito del *Global Counter-Terrorism Forum*, intese, da un lato, a prevenire il coinvolgimento di donne e ragazze in attività terroristiche e, dall'altro, a supportare le numerose vittime femminili di estremismo e terrorismo.

Per le sue implicazioni nel medio e lungo periodo, il fenomeno dei *foreign fighters* va considerato anche in relazione a quello collegato del reducismo, che annovera – oltre agli ex combattenti "disillusi" – soggetti dal profilo diversificato, ma tutti con addestramento militare ed esperienza maturata sul campo di battaglia. Nella casistica a maggior rischio figurano in particolare:

- individui che, dopo il loro ritorno in Patria, evidenzino disagio psicologico e problemi comportamentali (es. violenze nei confronti di altre persone, con apparenti segni di stress post-traumatico);
- elementi rientrati dall'area di conflitto a causa di ferite o problemi familiari/individuali, ma che continuino a coltivare idee estremiste e propositi offensivi;
- militanti autodeterminati a compiere attacchi nei Paesi in cui ritornano, da soli o in coordinamento con altri (inclusi *supporters* locali), ovvero apposita-

mente inviati da organizzazioni terroristiche interessate a costituire cellule dormienti.

Ai *returnees* sono associati, in termini di potenziale della minaccia, i cd. *commuters* (pendolari), ovvero quei soggetti in grado di viaggiare più volte dal teatro di *jihad* all'Occidente e viceversa, sfuggendo alle maglie dei controlli.

Anche in Italia, il fenomeno dei *foreign fighters,* inizialmente con numeri più contenuti rispetto alla media europea, è risultato in costante crescita, evidenziando, quale aspetto di particolare criticità, l'auto-reclutamento di elementi giovanissimi, al termine di processi di radicalizzazione spesso consumati in tempi molto rapidi e ad insaputa della stessa cerchia familiare.

Massima vigilanza informativa è stata pertanto riservata al pericolo derivante dal possibile arrivo di *returnees* o dai movimenti di *commuters* – soprattutto ove si tratti di soggetti dotati di titoli di viaggio che consentono loro di muoversi liberamente in area Schengen – già residenti sul nostro territorio o in altri Paesi europei.

…commandos, cellule dormienti e lupi solitari

Già nella precedente Relazione, con riferimento agli attentati compiuti nel gennaio 2015 dai fratelli Kouachi e da Amédy Coulibaly, l'estremismo *homegrown* e la progressiva affermazione di DAESH venivano richiamati quali fattori determinanti per l'avvenuto innalzamento del livello della minaccia terroristica sul continente europeo.

La manifesta determinazione e la capacità di colpire i "nemici crociati" nel cuore dell'Europa si sono accompagnate, nel corso dell'anno, ad una serie di attentati falliti, in qualche caso con vittime tra i civili, o sventati, nonché ad un incremento dei *warning* e delle evidenze informative attestanti l'eventualità che ad un arretramento di DAESH sul terreno del confronto militare potesse corrispondere una sua decisa ed eclatante proiezione extraregionale di tipo asimmetrico.

Secondo questo paradigma, l'azione condotta contro la Francia ha verosimilmente inaugurato una strategia di attacco all'Occidente destinata a consolidarsi, anche nelle modalità attuative: forme di coordinamento orizzontale flessibile – seppure stabile e continuativo grazie anche alle comunicazioni su *social network* e *chat* criptate – tra una "direzione centrale", presente in territorio siriano o iracheno, e cellule delocalizzate, chiamate a gestire in autonomia i dettagli della pianificazione operativa, calibrando logistica, obiettivi, tempi e luoghi secondo capacità ed opportunità.

Conseguentemente, è da ritenere elevato il rischio di nuove azioni in territorio europeo, ad opera sia di emissari inviati *ad hoc*, inclusi *foreign fighters* addestrati in teatri di conflitto, sia di militanti eventualmente già presenti (e integrati/mimetizzati) in Europa, che abbiano ricevuto ispirazione e *input* da attori basati all'esterno dei Paesi di riferimento.

Le acquisizioni informative raccolte dall'intelligence, così come le valutazioni condivise in sede di collaborazione internazionale, non consentono, peraltro, di ritenere superato il pericolo riferibile a formazioni terroristiche collegate ad *al Qaida*. Anche se queste ultime risultano segnate da defezioni individuali a favore di DAESH, esse hanno continuato a far registrare una certa effervescenza tanto sul piano del reclutamento quanto su quello operativo, e proprio la competizione con DAESH potrebbe rafforzare la determinazione qaidista a intervenire sulla scena globale con atti eclatanti.

Nel contempo, resta il pericolo di un'autonoma attivazione di estremisti *homegrown* che, individualmente o in microgruppi, potrebbero porsi in chiave emulativa sulla scia dei fatti di Parigi, concretizzare propositi violenti in relazione ad aspirazioni frustrate di raggiungere i teatri di *jihad* o comunque raccogliere gli appelli all'azione lanciati da DAESH e da altre organizzazioni terroristiche.

Minaccia "strutturata" e minaccia "puntiforme"

La minaccia "strutturata", dunque, che promana direttamente dall'organizzazione terroristica, non sostituisce, bensì integra, la minaccia "puntiforme", riferibile all'universo composito di elementi autoctoni ed autoreclutati, rendendo quest'ultima, oltre tutto, ancora più concreta ed attuale.

Malgrado non siano emersi specifici riscontri sull'esistenza di piani terroristici in territorio nazionale, nella propaganda jihadista ("a marchio" DAESH, ma anche *al Qaida*, volendo considerare i due videomessaggi di *al Qaida nel Maghreb Islamico*/AQMI del gennaio 2016) non sono mancati i riferimenti al nostro Paese come "nemico" a motivo della sua *partnership* con gli Stati Uniti e Israele, delle relazioni che intrattiene con Governi arabi ritenuti "apostati", dell'impegno nella lotta al terrorismo internazionale, nonché per il suo passato coloniale in Libia.

Sulla base di queste premesse, quindi, l'Italia appare sempre più "esposta" quale:

- *target* potenzialmente privilegiato sotto un profilo politico e simbolico/religioso, anche in relazione alla congiuntura del Giubileo straordinario;
- terreno di coltura di nuove generazioni di aspiranti *mujahidin*, che vivono nel mito del *ritorno al califfato* e che, aderendo alla campagna offensiva promossa da DAESH, potrebbero decidere di agire entro i nostri confini.

A tale riguardo vanno valutati con estrema attenzione i crescenti segnali di consenso verso l'ideologia jihadista emersi nei circuiti radicali *on-line*, frequentati da soggetti residenti in Italia o italofoni: si tratta di individui anche molto giovani, generalmente privi di uno specifico *background*, permeabili ad opinioni "di cordata" o all'influenza di figure carismatiche e resi più recettivi al "credo" jihadista da crisi identitarie, condizioni di emarginazione e visioni paranoiche delle regole sociali, talora frutto della frequentazione di ambienti della microdelinquenza, dello spaccio e delle carceri. Ne

è conferma la diffusione di testi elaborati o tradotti nella nostra lingua, con i quali:

- da un lato, si sostiene la legittimità del *Califfato*, invogliando gli accoliti a raggiungere la nuova "Patria" di tutti i musulmani;
- dall'altro, si esortano i *lupi solitari* ad agire, adottando un codice comportamentale improntato a segretezza e cautela.

Da non sottovalutare, inoltre, i rischi derivanti dalla generazione di estremisti della "prima ora", già facenti parte di reti di supporto logistico/finanziario al *jihad* smantellate tra i secondi anni '90 e primi 2000, che – sfuggiti all'azione di contrasto o tornati in libertà dopo un periodo di detenzione – potrebbero sentirsi nuovamente "chiamati alla causa" ed attivarsi direttamente o fornendo assistenza a emissari provenienti dall'estero.

Per le attività di proselitismo, indottrinamento e istigazione al *jihad* sul nostro territorio, sebbene i *forum on-line* d'area si siano confermati il principale bacino di riferimento, è la frequentazione personale a rappresentare un collante primario nel processo che dalla radicalizzazione ideologica conduce al coinvolgimento diretto e al reclutamento. In quest'ottica è risultata ancora incisiva l'influenza esercitata da:

- contesti parentali e amicali, all'interno dei quali sono tuttora mantenuti rapporti con estremisti espulsi dall'Italia o con *foreign fighters* intenzionati a reclutare nuovi adepti;
- componenti islamiste costituitesi su base etnica, come quelle di matrice balcanica, maghrebina o pakistana, al cui interno si muovono elementi che simpatizzano per gruppi armati anche di matrice qaidista;
- circuiti "sensibili", come quello legato agli ex combattenti libici giunti nel tempo in Italia anche per cure mediche, con trascorsi e/o propensioni radicali;
- luoghi di aggregazione islamica permeabili alla propaganda estremista;
- ambienti carcerari, ove i detenuti per reati comuni sembrerebbero i più vulnerabili a percorsi di radicalizzazione ideologico-religiosa e, qualora indottrinati, potrebbero, all'atto della scarcerazione, decidere di raggiungere i territori del *Califfato* o comunque nutrire sentimenti di rivalsa nei confronti del nostro Paese.

Il finanziamento del terrorismo

Coerentemente con l'evoluzione della minaccia terroristica di matrice jihadista, anche sul terreno del contrasto ai connessi flussi finanziari l'azione informativa si è prioritariamente focalizzata sui canali di alimentazione economica di DAESH, rappresentati soprattutto dalle risorse ottenute grazie alle diversificate e redditizie attività illegali poste in essere dai miliziani nelle vaste aree delle regioni occupate di Siria ed Iraq. Ciò vale in primo luogo per il contrabbando di greggio e di prodotti derivati dalla raffinazione del petrolio, fattore propulsivo della "macchina da guerra" jihadista. Le dimensioni di tali traffici, basati su un'articolata

rete di contrabbando esistente nelle zone occupate, hanno mantenuto valori importanti nonostante l'intensificazione dei *raid* aerei della Coalizione e le difficoltà legate all'estrazione. Il *trend* complessivo, infatti, sebbene in calo, non è in declino*:* ciò soprattutto grazie alla gestione dei numerosi giacimenti petroliferi occupati sia in Siria (principalmente tra Deir Ez Zowr e Hasakah) sia in Iraq (all'interno delle province di Salahuddin e Ninive e a ridosso del confine con il Kurdistan), per il tramite di efficienti sistemi di controllo, veri e propri presidi militari, e solide capacità organizzative, decisive nella pianificazione e nel perfezionamento delle operazioni di trafugamento, trasporto e commercializzazione del greggio sui mercati finali.

Di rilievo, inoltre, è il traffico illecito di reperti archeologici sottratti dai siti storici presenti nelle aree occupate. Si calcola che più di un terzo dei dodicimila siti archeologici iracheni e siriani, molti dei quali dichiarati dall'UNESCO patrimonio dell'umanità, sarebbe sotto il controllo di DAESH ed oltre il 90% di essi insisterebbe nelle zone di guerra dei due Paesi. I reperti, dopo essere stati trafugati da tombe, chiese, palazzi antichi ed altri siti di inestimabile valore storico, grazie alla presenza *in loco* di esperti di settore appositamente assoldati dai miliziani, sarebbero rivenduti ad intermediari locali di acquirenti internazionali.

Significativi introiti legati al controllo del territorio derivano altresì dalle appropriazioni indebite e dai saccheggi di denaro proveniente da istituti bancari, nonché dalle estorsioni operate in danno di cittadini, minoranze religiose e attività economiche locali.

Specifica menzione meritano, poi, le donazioni provenienti da varie entità presenti in Paesi del Golfo. Tali risorse rivestono centralità in ragione del ricorso strumentale a:

- sistemi bancari non ancora dotati di adeguati meccanismi di controllo sulle operazioni sospette di finanziamento del terrorismo, che pertanto fungono da vere e proprie camere di compensazione per i fondi destinati a raggiungere le milizie jihadiste attive nel quadrante siro-iracheno, pregiudicando la tracciabilità dei flussi finanziari;
- associazioni caritatevoli, utilizzate come copertura per azioni di proselitismo religioso radicale e capillari penetrazioni delle aree interessate, così da alimentare le filiere del jihadismo internazionale.

Per quel che concerne il supporto finanziario alle proiezioni extraregionali di DAESH, specifiche acquisizioni intelligence hanno riguardato:

- i progetti, nell'area afghano-pakistana, della proclamata *Wilayat Khorasan* di DAESH, che risultano sostenuti da risorse finanziare rese disponibili sia dalla *leadership* dell'organizzazione in *Syrak*, sia – anche qui – da *sponsor* localizzati in Paesi del Golfo. In tali contesti, la raccolta delle donazioni da parte dei sostenitori del *Califfato* avrebbe assunto carattere sistematico: i fondi raccolti verrebbero rimessi nell'area afghano-pakistana attraverso i circuiti informali dell'*hawala*, sfruttando

tra l'altro anche la capillare rete di operatori (agenzie di *money exchange* e *hawaladars*) presenti sul territorio;

- la Libia, dove le compagini terroristiche affiliate a DAESH hanno mostrato la disponibilità di risorse finanziarie in grado di sostenere la propria strategia eversiva nel Paese. Significativa, al riguardo, appare la capacità di tali fazioni di acquisire armamenti ed equipaggiamenti e di far fronte ai costi gestionali correlati al pagamento dei salari e ad altre attività logistico-operative. Si tratta di risorse provenienti sia da fondi resi disponibili dalla *leadership* di DAESH in Siria e Iraq, sia dai prelievi imposti localmente alle attività economico-commerciali e alle minoranze religiose. Inoltre, la presenza di gruppi affiliati all'organizzazione in aree attraversate dalle rotte del traffico di esseri umani, soprattutto nella parte orientale della Libia, delinea l'eventualità che ai trafficanti possano essere imposti pagamenti per consentire il transito dei convogli.

Con riguardo alle aree di operatività delle componenti della galassia jihadista non riconducibili a DAESH ed ai connessi canali di finanziamento, sono rimasti all'attenzione informativa:

- il quadrante afghano-pakistano, in cui la composita insorgenza guidata dal movimento *Taliban* ha continuato a manifestare elevate disponibilità economiche basate su fonti sia endogene che esogene. Sul piano interno, i *Taliban* hanno adottato un sistema estorsivo ad ampio spettro sulle attività legali ed illegali (*in primis* i traffici di droga) condotte nei territori controllati. Al progressivo disimpegno del Contingente internazionale ha corrisposto una rivitalizzazione delle attività militari dell'insorgenza volte, tra l'altro, ad acquisire il controllo dei centri nevralgici del narcotraffico nel Sud del Paese e delle direttrici di transito degli stupefacenti in direzione dei mercati di sbocco. Di rilievo, inoltre, le contribuzioni raccolte sia in ambito locale, sia nelle aree della diaspora con una marcata incidenza di quelle provenienti dalla Penisola arabica, queste ultime, peraltro, "contese" con le emergenti frange pro-DAESH;
- il Corno d'Africa, dove, se da un lato si registra una riduzione dei finanziamenti che *al Qaida* destina ad *al Shabaab* (tanto da incidere sul dibattito interno al movimento terroristico circa l'eventuale affiliazione a DAESH), dall'altro le capacità operative manifestate dal gruppo somalo, con la realizzazione di attacchi sia in Somalia sia nei Paesi confinanti, hanno evidenziato persistenti capacità finanziarie, derivanti, prevalentemente, da:
  - commissioni imposte sui trasferimenti di denaro operati dai *money transfer*, vere e proprie tangenti riscosse da *al Shabaab* in cambio della possibilità di operare nei territori sotto il suo controllo;
  - estorsioni a danno di attività commerciali ed imposizione di dazi sulle merci in transito nelle aree d'influenza;

- gestione in proprio del contrabbando di carbone, zucchero, avorio e droga;
- traffico di clandestini;
- raccolta di donazioni dall'estero.

A fattor comune, con riferimento alle modalità di trasferimento delle risorse finanziarie, va rilevato che, a vario livello di complessità, le dinamiche di movimentazione di denaro interessano non solo le organizzazioni terroristiche strutturate, ma anche cellule autonome, o elementi auto-radicalizzati. Questi ultimi possono essere sovvenzionati con importi esigui di difficile individuazione, anche quando in transito sui circuiti finanziari legali. In particolare, al fine di aggirare i controlli, le formazioni estremiste ricorrono spesso a tecniche fraudolente, che comprendono l'impiego di prestanome, di società di copertura e di operatori finanziari compiacenti (convenzionali e non), sovente localizzati in aree scarsamente regolamentate. Alle pratiche di riciclaggio dei proventi derivanti da un ampio ventaglio di attività criminali, si affiancano quelle di *money-dirting*, in cui fondi raccolti secondo modalità formalmente lecite vengono dirottati ai gruppi terroristici.

In tale contesto, per quanto attiene al territorio nazionale, specifica attenzione è stata riservata al trasferimento di fondi da e per l'estero, con particolare riguardo alle aree più sensibili all'integralismo islamico, mediante moneta elettronica (tra cui carte di credito prepagate e carte telefoniche), canali bancari formali e informali (*hawala*, *hundi*), circuiti formali di *money transfer* e trasferimenti (*cross border*) di contante al seguito presso le aree aeroportuali internazionali.

LE DECLINAZIONI REGIONALI DEL *JIHAD* E LA GEOMETRIA VARIABILE DELLE RELAZIONI INTERNAZIONALI

Il *vulnus* libico e il confronto interjihadista in Africa: gli spazi operativi nel Maghreb

Obiettivo prioritario dell'attività informativa sul versante estero si è confermato, anche per il 2015, il **contesto libico**, la cui stabilizzazione resta determinante non solo in un'ottica di sicurezza regionale, ma anche di prevenzione della minaccia terroristica e di tutela degli interessi nazionali.

La crisi politico-istituzionale in Libia determinata dalla conflittualità tra il Congresso Generale di Tripoli e la Camera dei Rappresentanti di Tobruk – che ha trovato una prima composizione nell'accordo tra le parti, siglato in Marocco il 17 dicembre, per dar vita, sotto egida ONU, ad un Governo di Unità Nazionale – ha favorito l'attivismo dei gruppi jihadisti nel Paese e nelle aree nordafricana e sahelo-sahariana, in particolare di *al Qaida nel Maghreb Islamico* (AQMI), *Ansar al Shariah*, *al Murabitun* (AM) e DAESH.

Tali compagini hanno beneficiato delle precarie condizioni di sicurezza del Paese per condurre attività di rifornimento logistico, addestrare i combattenti ed affinare le proprie capacità operative, anche attraverso forme di collaborazione che si sono sostanziate nello scambio di uomini, armi e mezzi. Inoltre, l'elevata disponibilità di materiale

di armamento e l'assenza di un efficace dispositivo di controllo del territorio hanno favorito i traffici illeciti delle organizzazioni terroristiche, soprattutto in armi e stupefacenti, a scopo di autofinanziamento.

Il vuoto di potere in Libia è stato sfruttato anche da DAESH, che gradualmente ha consolidato la sua posizione, collocandosi con cellule più o meno strutturate sia in Tripolitania (soprattutto a Sirte) sia in Cirenaica (Ajdabiya, Bengasi e Derna). I progetti di espansione del gruppo iracheno sono stati più volte propagandati attraverso una pressante campagna mediatica – attraverso la quale DAESH ha manifestato la volontà di organizzare la Libia in tre province, sul modello della storica divisione tra Cirenaica, Tripolitania e Fezzan – e la condotta di operazioni sul campo di notevole impatto propagandistico, quali l'attentato all'*Hotel Corinthia* di Tripoli (gennaio), l'uccisione di 21 egiziani copti (febbraio) e, il 7 gennaio 2016, l'attentato con camion-bomba contro il Centro di Addestramento delle Forze di polizia di Zliten, che ha provocato oltre 50 vittime e un centinaio di feriti. Inoltre, elementi di vertice di DAESH hanno invitato i propri adepti a restare a combattere in Libia piuttosto che trasferirsi in Siria od in Iraq.

La sempre più capillare penetrazione di DAESH nel Maghreb è confermata, altresì, non solo dal numero di formazioni che vi si richiamerebbero e/o vi starebbero aderendo, ma anche dalla crescente radicalizzazione di vasti settori della società, specie giovanili, e dal fenomeno dei *foreign fighters*, molti dei quali nordafricani.

La comparsa di un attore quale DAESH a fianco degli "storici" protagonisti della scena qaidista ha alterato e complicato il tradizionale quadro di riferimento del terrorismo regionale, contribuendo a rivitalizzare l'attivismo dei gruppi terroristici e a potenziarne gli effetti destabilizzanti. Emblematici, al riguardo, i segnali di collaborazioni tattico-operative circoscritte e contingenti, alternate a forme di contrapposizione, tra cellule che si richiamano a DAESH e frange libiche di *Ansar al Shariah*.

Altrettanto significativo é l'affacciarsi di DAESH sull'articolato panorama dell'**estremismo tunisino –** riconducibile soprattutto ad *Ansar al Shariah* e al *Battaglione Oqba Bin Nafi*, "braccio armato" di AQMI – che ha continuato a trovare nel precario contesto libico base di riferimento per l'approvvigionamento di armi, la formazione e l'addestramento di combattenti e l'affinamento delle proprie capacità operative. Non è un caso che DAESH abbia "formalmente" rivendicato tanto l'attentato al Museo del Bardo (Tunisi, 18 marzo), quanto quello al complesso turistico di Port el Kantaoui (Sousse, 26 giugno).

Contestualmente, è proseguito il dibattito interno alle organizzazioni jihadiste della regione in merito all'eventualità di rimanere nell'orbita di *al Qaida Core* o di allearsi con DAESH. Particolarmente critica sarebbe la situazione di AQMI, fra le cui file si registrerebbero numerose defezioni, l'ultima delle quali da parte di alcuni elementi appartenenti al *Battaglione al Ansar*.

Alleanze tattiche e "matrimoni di convenienza" nell'Africa sub-sahariana e nel Corno d'Africa

Un forte dinamismo è emerso, altresì, tra i numerosi gruppi attivi nell'**area maliana**. In particolare, le regioni centro-settentrionali hanno continuato a sfuggire al controllo delle Forze armate maliane e a registrare la presenza di formazioni terroristiche locali e transnazionali, quali AQMI, AM ed *Ansar el Din*, che, pur presentandosi come entità distinte, si sono dimostrate in grado di realizzare convergenze di breve periodo finalizzate al perseguimento di obiettivi comuni, tra i quali quello di impedire il processo di stabilizzazione del Paese. Un primo indicatore della penetrazione del messaggio di DAESH anche in aree sinora dominate da formazioni della galassia qaidista è stato rappresentato dalla dichiarazione di affiliazione al *Califfato* (maggio 2015) di una componente di AM. Non sono mancati, tuttavia, importanti segnali di una ritrovata convergenza, come dimostrato dall'unione fra AQMI e AM, annunciata "ufficialmente" (3 dicembre) dal *leader* di AQMI, Abdelmalek Droukdel, e già concretizzatasi, poco prima, nell'attentato (20 novembre) all'*Hotel Radisson Blue* di Bamako. Ulteriore segnale nel senso può cogliersi nel duplice attacco antioccidentale del 15 gennaio 2016 a Ouagadougou, in Burkina Faso, rivendicato da AQMI con un messaggio nel quale si dichiarava l'appartenenza degli esecutori ad AM.

Anche nell'Africa sub-sahariana si sono registrate alleanze tattiche tra organizzazioni jihadiste. La presenza e le attività dei diversi gruppi sono parse in costante crescita, grazie alla strutturale debolezza degli Stati africani, all'attrattiva esercitata dalle preziose risorse naturali ed all'elevata percentuale di popolazione giovanile disoccupata e/o marginalizzata, che fornisce ai movimenti jihadisti un privilegiato bacino di reclutamento. La presenza jihadista ha trovato il suo epicentro in Africa occidentale, in particolare nell'area del Lago Ciad, dove opera il gruppo *Boko Haram* (BH), e nel Corno d'Africa, ove è da tempo attivo *al Shabaab*. Entrambe le formazioni jihadiste hanno evidenziato l'avvenuta acquisizione di una struttura transnazionale, rafforzata da alleanze strategiche con altri movimenti terroristici, quali DAESH ed *al Qaida nella Penisola Arabica* (AQAP). Non a caso BH, dopo la sua affiliazione a DAESH, in marzo, ha assunto la denominazione di *Islamic State's West African Province* (ISWAP), contribuendo all'effervescenza del radicalismo anche nei Paesi confinanti (Niger, Ciad e Camerun).

Con questo "matrimonio di convenienza", BH ha ottenuto un riconoscimento nel "*jihad* globale", mentre DAESH ha conseguito indubbi vantaggi soprattutto sul piano dell'azione propagandistica, potendo esibire come "estensione del *Califfato*" una vasta regione situata nel cuore dell'Africa. D'altro canto, obiettivo strategico di BH è la ricostituzione del *Califfato di Sokoto*, ovvero l'istituzione di uno Stato islamico in un'area ben più estesa della sua tradizionale zona di elezione nella Nigeria nord-orientale.

A fronte di tali sviluppi, le Autorità di Abuja hanno articolato l'attività di contrasto

a BH, agendo non solo sul piano militare – anche attraverso la *Multinational Joint Task Force* (MNJTF), autorizzata il 29 gennaio dal Consiglio per la Pace e la Sicurezza dell'Unione Africana – ma, altresì, nei diversi settori che costituiscono ambiti di aggregazione ed emulazione per i giovani nigeriani. Si inscrivono in questa cornice: il contrasto ideologico alla dottrina di BH/ISWAP; gli interventi per migliorare le infrastrutture (in particolare gli istituti di formazione) e l'economia degli Stati del Nord della Nigeria; la creazione di opportunità/alternative per i giovani, con l'avvio di centri di formazione professionale (*Vocational Center*).

Tale impegno dovrà misurarsi, peraltro, con le difficoltà di attuazione del mandato della MNJTF e con le carenze del dispositivo militare.

Per quanto concerne il **Corno d'Africa**, *al Shabaab* ha sviluppato nel tempo diverse forme di collaborazione con altri movimenti gravitanti nella galassia riconducibile ad *al Qaida*. Attualmente, la sigla si presenta suddivisa in due fazioni, l'una più vicina ad AQAP, l'altra favorevole invece all'adesione a DAESH. L'organizzazione somala ha adottato un atteggiamento di tipo utilitaristico, sfruttando ogni eventuale possibilità di collaborazione con entrambi i movimenti predetti, per quanto concerne sia l'afflusso di miliziani, materiale d'armamento e logistico, sia l'accesso a finanziamenti, mantenendo però una propria autonomia operativa ed ideologica.

In ogni caso, nonostante la presenza di due correnti tra loro in contrasto, il movimento somalo è riuscito fino ad ora a mantenere una sostanziale unità. Tra le defezioni a favore di DAESH, ha acquisito particolare significato quella di Sheikh Abdulkadir Mumin, *leader* spirituale di AS nel Puntland, regione quest'ultima dove è segnalata con sempre maggiore frequenza la presenza di cellule dell'organizzazione di al Baghdadi.

Per quanto attiene al **Kenya**, è verosimile che Nairobi, le località di confine con la Somalia e le città costiere continueranno a costituire un obiettivo prioritario nella strategia di *al Shabaab*, volta ad espandere la propria area di influenza a sud della Somalia e nella Regione dei Grandi Laghi. Nel Paese la formazione gode di aree di fiancheggiamento nell'ambito della nutrita comunità somala locale e di organizzazioni autoctone quali *Jaysh Ayman* e la *Muslim Youth Center/al Hijra*. Quest'ultima, fondata nel 2008 a Nairobi, a partire da un'iniziale attività di reclutamento e raccolta fondi avrebbe poi gradualmente accresciuto, dal 2014, le attività offensive a fianco di *al Shabaab*.

Il conflitto in *Syrak*: gli attori e le evoluzioni sul terreno

Centro propulsore della minaccia posta da DAESH, il conflitto nel teatro siro-iracheno si è posto, ad un tempo, quale laboratorio di alleanze inedite e allargate nel segno della lotta al terrorismo e quale critico catalizzatore di tensioni e istanze storicamente contrapposte.

Per quel che riguarda gli sviluppi sul terreno in **Siria**, si è osservato l'emergere ed il consolidarsi di centri di potere autonomi

o semi-autonomi rispetto al regime, anche nelle aree in cui i lealisti mantengono il controllo formale del territorio, ad indicare una progressiva crisi degli apparati politico-istituzionali e burocratico-amministrativi dello Stato che renderebbe più complessa la "normalizzazione" anche nell'ipotesi in cui il conflitto armato dovesse ridursi di intensità.

Costante è stato l'impegno di Damasco nel tentativo di riaccreditarsi presso la Comunità occidentale quale *partner* imprescindibile per il mantenimento della sicurezza, specie in relazione al terrorismo di matrice jihadista. Nel contempo è proseguito il supporto fornito a Damasco dall'Iran, dagli *Hizballah* libanesi e dalla Russia, che ha intensificato il proprio impegno militare nel teatro siriano ed ha avviato, a partire dal 30 settembre, *raid* aerei paralleli a quelli della Coalizione anti-DAESH. In tale contesto, l'abbattimento del velivolo russo SU-24 da parte di Ankara (24 novembre), che ha prodotto un innalzamento della tensione tra i due Paesi, ha rappresentato solo una delle linee di faglia che hanno segnato l'impegno internazionale contro DAESH.

Dal canto suo, quest'ultimo ha focalizzato primariamente la propria azione in Siria sulla difesa e sul consolidamento dei territori conquistati, contrapponendosi al nemico di turno (Forze lealiste, formazioni jihadiste concorrenti e Coalizione internazionale) e cercando di ripianare le perdite subite con il reclutamento di nuove leve, da impiegare – a seconda dei casi – in operazioni di guerra "tradizionali" o di tipo asimmetrico, fino alle azioni suicide.

Nelle regioni nord-occidentali, DAESH ha gradualmente esteso il proprio controllo dalle sue roccaforti nei governatorati di Deir Ez Zowr e Raqqah verso Ovest, servendosi di Palmira (conquistata in maggio) come avamposto per ulteriori espansioni verso Damasco e il capoluogo provinciale di Homs. Tale avanzata ha dovuto misurarsi, comunque, con l'intervento militare russo e con l'accelerazione della campagna anti-terrorismo della Coalizione. Anche nel Sud del Paese si è rilevato l'attivismo di DAESH, che ha sferrato numerosi attacchi contro i gruppi anti-governativi.

Per quanto riguarda la già ridotta componente laica e nazionalista dell'opposizione, questa è stata in parte assorbita all'interno di coalizioni locali alle quali partecipano anche formazioni jihadiste. Ne è esempio l'organizzazione ombrello *Jaish al Fatah (Esercito della Conquista*) – che comprende, oltre alla formazione di impronta qaidista *Jabhat al Nusrah*, le milizie islamiste *Ahrar al Sham e Jund al Aqsa*, *Failaq al Sham*, *Jaish al Sunna*, *Ajnad al Sham* e *Liwa al Haqq* – operante nel governatorato di Idlib e, con la denominazione di *Jaish al Fatah Halab*, anche in quello di Aleppo. Al Nord, dopo la conquista della quasi totalità del governatorato di Idlib, *Jaish al Fatah* ha lanciato offensive contro le Forze lealiste nelle province di Hama e Latakia, nel tentativo di estendere la propria influenza verso l'area costiera del Paese, ed ha costituito una sala operativa ad Aleppo. Nelle regioni meridionali, l'opposizione si è consolidata nei governatorati di Quneytra, Daraa ed as Suwayda, nonostante le offensive condotte dalle Forze del regime.

Quanto alle attività delle principali organizzazioni dell'opposizione politica siriana operanti all'estero, si è confermato il loro ruolo marginale, in ragione tanto delle perduranti divisioni interne, quanto della mancanza di rappresentatività rispetto alle componenti, armate e non, che agiscono all'interno del Paese.

Relativamente all'**Iraq**, la cornice di sicurezza ha evidenziato una perdurante criticità alimentata dalla drammatica situazione umanitaria correlata all'elevato numero di sfollati e rifugiati.

Malgrado la determinazione del Governo di al Abadi nel promuovere la stabilizzazione politica del Paese secondo principi di inclusività delle varie componenti della popolazione, la persistente presenza di DAESH nelle province nord-orientali di Ninive, Kirkuk ed Erbil, nel governatorato centrale di Salahuddin (per assumere il controllo della raffineria petrolifera di Bayji) e in quello centro-occidentale di al Anbar ha esposto l'Iraq al rischio concreto di consolidarsi quale *hub* di incubazione ed attrazione di estremisti ed ha alimentato, al contempo, il settarismo locale, ma anche regionale.

È proseguita, inoltre, attraverso azioni asimmetriche costanti, la campagna di destabilizzazione della Capitale e delle aree circostanti.

D'altro verso, l'impegno profuso dalle Forze irachene per la riconquista di porzioni di territorio controllate da DAESH ha consentito, dopo mesi di acceso confronto sul terreno, di liberare (28 dicembre) la città di Ramadi, capoluogo di al Anbar.

Al contempo, la crisi in *Syrak* non ha mancato di riflettersi sugli altri Paesi della regione e particolarmente sul **Libano**, peraltro attraversato da una logorante impasse politico-istituzionale. Sulla cornice di sicurezza libanese hanno continuato ad incidere negativamente sia l'afflusso di profughi siriani nelle aree settentrionali e nei campi profughi palestinesi, divenuti bacino privilegiato per le attività di reclutamento delle organizzazioni jihadiste, sia l'attivismo di formazioni estremiste salafite, a partire da *Jabhat al Nusra* e DAESH, quest'ultimo resosi responsabile, il 12 novembre, del duplice attentato suicida in un quartiere periferico di Beirut a maggioranza sciita.

La variabile curda

In Iraq e, soprattutto, in Siria, i curdi si sono rivelati un efficace alleato della Coalizione internazionale contro DAESH, sebbene divergenze interne ne abbiano indebolito la coesione (*vds. box n. 5*).

Per altro verso, ha conosciuto nuove fiammate di conflittualità il confronto tra il Governo turco e le componenti curde riferibili al PKK, il cui contrasto ha continuato a rappresentare una priorità nell'agenda delle Autorità di Ankara, contestualmente ingaggiate nella lotta a DAESH.

Le germinazioni di DAESH nel Sinai e a Gaza

In **Egitto** sono risultate particolarmente pervasive le attività terroristiche riconducibili alla composita galassia di gruppi islamisti. La recrudescenza degli attentati, sia nella penisola del Sinai che nella Capitale, è valsa a testimoniare la crescita organizzativa di formazioni endogene che hanno intensificato l'offensiva contro le Forze di sicurezza egiziane fungendo da sponda, altresì, alla strategia espansiva di DAESH. Emblematico, al riguardo, *Ansar Bayt al Maqdis/Wilayat Sina' – Stato Islamico/Provincia del Sinai* (ABM-WS), che, attivo soprattutto sul fronte interno nonché, a fini di reclutamento, nel Sud della Striscia di Gaza, ha rivendicato il citato attentato del 31 ottobre ai danni della Compagnia russa *Metrojet*, in ritorsione ai *raid* di Mosca contro DAESH.

Nella Striscia di Gaza, i gruppi ideologicamente vicini al *Califfato* non ancora formalmente affiliati sono parsi, invece, principalmente tesi a sovvertire il potere di *Hamas* sul territorio e ad istituire una *wilayah* a Gaza. Considerate le condizioni eco-

box 5

LA COMPOSITA REALTÀ CURDA

Nel corso del 2015, il quadro dei rapporti intercurdi ha fatto registrare in particolare:

- sul versante iracheno, all'interno della Regione Autonoma del Kurdistan (RAK), la dialettica tra il *Partito Democratico del Kurdistan* (*Parti Dimukrati Kurdistan* – PDK) di Massoud Barzani e i partiti di opposizione, specie quello dell'*Unione Patriottica del Kurdistan* (*Yeketi Nistimani Kurdistan* – UPK),
- tensioni tra il citato PDK iracheno e il siriano *Partito di Unione Democratica (Partiya Yekitiya Demokrat* – PYD), con specifico riguardo alle relazioni tra quest'ultimo e l'organizzazione separatista turco-curda *Partito dei Lavoratori Curdi* (*Partiya Karkerén Kurdistan* – PKK/KONGRA GEL).

Più in generale, l'avanzata di DAESH in *Syrak*, ma anche il suo interagire con criticità endemiche (dispute regionali per le ricchezze naturali, specie acqua e petrolio; confronto sciiti e sunniti; ingerenze di attori esterni), hanno reso quanto mai attuale la *questione curda,* che ha radici remote e perduranti implicazioni sugli sviluppi d'area.

L'identità socio-linguistica-culturale dei Curdi (gruppo etnico stimato in 25-35 milioni di individui) si è misurata per secoli con una posizione geopolitica a cavallo tra le civiltà araba, persiana e turca. Con il trattato di Losanna (1923), la comunità è stata dispersa in più Paesi (prevalentemente in Turchia, Iran, Iraq e Siria), animando cicliche ribellioni e alimentando un'incessante diaspora: evoluzione, questa, che ha concorso ad ostacolare l'affermazione di un progetto condiviso, delineando per le varie componenti rivendicazioni autonomiste altrettanto differenziate, anche in ragione della diversa postura dei rispettivi Stati di radicamento.

nomiche critiche, sembra essere aumentata la propensione di fasce della popolazione giovanile ad unirsi a gruppi terroristici.

Quanto alle dinamiche interpalestinesi, è emersa una nuova polarizzazione dello scenario politico, che ha allontanato le prospettive di riconciliazione tra *Hamas* e *Fatah*, in un clima di diffuso malcontento anche per il perdurante stallo nel Processo di Pace (*vds. box n.* 6).

Le dinamiche nel Golfo e la crisi in Yemen

Relativamente alle **Monarchie del Golfo**, in **Arabia Saudita**, l'assunzione della guida del Regno da parte di Re Salman (già Principe Ereditario) alla morte di re Abdallah (23 gennaio 2015) ha impresso una svolta al corso della Monarchia, dando luogo, nei mesi successivi, ad un rinnovato dinamismo politico-istituzionale. Riyadh, attore preminente del fronte sunnita, ha svolto un ruolo profilato nel contrasto a DAESH: di particolare rilievo, al riguardo, l'iniziativa, annunciata il 15 dicembre, della costituzione di una nuova alleanza militare islamica, composta da 34 Paesi dell'area del Golfo, del Medio Oriente, dell'Africa e dell'Asia, con sede nella Capitale saudita, per combattere il terrorismo di matrice jihadista.

Sul piano regionale, la decisione di Riyadh di procedere all'esecuzione della condanna a morte del dignitario ed attivista sciita Nimr Baqr al Nimr (2 gennaio 2016) ha provocato un innalzamento delle tensioni con l'Iran, in una fase caratterizzata, da un lato, dall'acuirsi del confronto tra forze

box 6

LA QUESTIONE PALESTINESE

Il Processo di Pace fra Israeliani e Palestinesi, interrotto dall'aprile 2014, non ha fatto registrare progressi. L'anno è stato segnato da proteste e scontri a Gerusalemme Est ed in prossimità delle colonie in Cisgiordania e del Muro nella Valle di Cremisan. Il clima di tensione è stato ulteriormente aggravato dagli episodi di settembre 2015 presso la Spianata delle Moschee/Monte del Tempio che hanno coinvolto Palestinesi e Forze di sicurezza israeliane. La cosiddetta *intifada* dei coltelli ha quindi innescato una catena di violenze, con vittime da entrambe le parti.

Allo stesso tempo, la campagna internazionale "Boicottaggio, Disinvestimenti e Sanzioni" (BDS) contro Israele e l'offensiva diplomatica promossa nei principali consessi internazionali dal Presidente dell'Autorità Nazionale Palestinese (ANP), Mahmoud Abbas (alias Abu Mazen), hanno inciso sulle prospettive di rilancio delle trattative.

sciite e sunnite in diversi contesti di crisi e, dall'altro, dalle prospettive di un riposizionamento di Teheran correlato al raggiungimento dell'accordo con la Comunità internazionale sul *dossier* nucleare (*vds. box n.* 7)

In **Arabia Saudita,** come pure in **Kuwait,** DAESH ha sferrato cruenti attacchi contro moschee sciite allo scopo soprattutto di inasprire le tensioni intersettarie. In questo quadro, la reazione delle Forze di sicurezza saudite ha condotto allo smantellamento di numerose cellule legate all'organizzazione.

La situazione che ha inciso in termini considerevoli sugli assetti regionali è stata la crisi in **Yemen**, caratterizzatasi per un conflitto prolungato da cui hanno tratto ampio vantaggio sia *al Qaida nella Penisola Arabica* che DAESH. Lo stallo nel confronto militare tra la coalizione araba e le milizie sciite degli *Houthi,* delineatosi in autunno, ha peraltro contribuito a ridare slancio alla mediazione ONU per addivenire ad un cessate-il-fuoco. La diplomazia dell'Inviato Speciale del Segretario delle Nazioni Unite, con l'ausilio

box 7

I *DOSSIER* NUCLEARI

Il *deal* iraniano

Il 14 luglio 2015 l'Iran ed i "5+1" (Stati Uniti, Russia, Cina, Francia, Regno Unito + Germania) hanno sottoscritto a Vienna il *Joint Comprehensive Plan of Action* (JCPA), che prevede:

- un consistente taglio alle scorte di uranio arricchito, con una riduzione del 98% dello stock accumulato;
- una drastica diminuzione delle centrifughe e del livello di arricchimento dell'uranio prodotto, che non potrà superare il 3,6%;
- la riprogettazione del reattore ad acqua pesante di Arak, al fine di impedire/limitare l'eventuale produzione di plutonio *weapons grade*;
- l'accesso incondizionato degli ispettori dell'Agenzia Internazionale per l'Energia Atomica/ AIEA ai siti nucleari;
- la fine del regime sanzionatorio;
- la prosecuzione temporanea dell'embargo sui sistemi d'arma;
- le trattative dirette tra le Autorità iraniane e l'AIEA per la soluzione della questione connessa alla cd. *Possible Military Dimension* (PMD) del programma di Teheran;
- l'istituzione di una Commissione congiunta, anche per la soluzione delle controversie.

A seguito dell'approvazione all'unanimità, da parte del Consiglio di Sicurezza dell'ONU (Risoluzione n. 2231 del 20 luglio), il JCPA è entrato in vigore il 18 ottobre (cd. *Adoption Day*). L'AIEA

ha quindi assolto al compito di verificare l'implementazione, da parte iraniana, delle clausole dell'accordo legittimando così UE e USA a sospendere una prima parte delle sanzioni (*Implementation Day*). Entro un limite massimo di otto anni dall'*Adoption Day*, l'Agenzia dovrà presentare un rapporto in cui attesterà che "*tutto il materiale nucleare presente in Iran è impiegato per scopi pacifici*" e contemporaneamente verranno rimosse le restrizioni in materia di armi e tecnologia missilistica. Il processo avrà termine a dieci anni dall'*Adoption Day* quando il Consiglio di Sicurezza dell'ONU dichiarerà chiusa la vicenda (*Termination Day*).

Il 2 dicembre 2015, l'AIEA ha diffuso il Rapporto finale in merito alla controversa questione legata alla cd. *Possible Military Dimension* (PMD) del programma nucleare, nel quale viene confermato che Teheran avrebbe condotto, almeno fino al 2003, una serie di attività riconducibili allo sviluppo di un ordigno a fissione. Ciononostante, il 15 dicembre 2015, il Consiglio dei Governatori dell'Agenzia di Vienna ha deciso di archiviare la relativa inchiesta per non ostacolare la positiva conclusione del JCPA.

Le iniziative nordcoreane

Nel 2015 in Corea del Nord si sono registrate nuove attività proliferanti nei settori missilistico e nucleare. Nel dettaglio:

- (maggio) è stato condotto, al largo della base navale di Sinpo, un test sperimentale di un missile balistico lanciato da sottomarino;
- (giugno) sono stati lanciati tre missili a corto raggio KN-01;
- (ottobre), in occasione della parata militare a celebrazione del 70° della nascita del locale Partito dei Lavoratori, è stato esibito un nuovo modello di vettore balistico intercontinentale noto come KN-08, in grado, secondo le dichiarazioni delle Autorità di Pyong Yang, di trasportare ordigni nucleari miniaturizzati.

La determinazione del regime a perseverare nei programmi di armamento non convenzionale si è accompagnata alla consueta retorica bellicistica ed auto-celebrativa del Presidente Kim Yong-Un. In questa cornice è intervenuto, il 6 gennaio 2016, l'eclatante annuncio dell'avvenuta sperimentazione di un ordigno termonucleare.

di diversi Paesi della regione, ha indotto le parti a partecipare ad un tavolo negoziale convocato in Svizzera a partire dal 15 dicembre al fine di promuovere una composizione del conflitto, favorire gli urgenti interventi di natura umanitaria e schiudere una prospettiva di ricostruzione del Paese. Frattanto, il deterioramento della cornice di sicurezza ha offerto spazi di agibilità alle formazioni islamico-radicali, la cui agenda è per lo più nazionale, protese a guadagnare terreno rispetto alle Forze governative ed a coltivare traffici illeciti anche fuori dai confini, specie con la Somalia. DAESH, che ha costituito, nel novembre 2014, la filiale denominata *Wilayat al Yemen* (IS-Y), è risultata molto attiva nelle province di Sanaa, Ibb, Lahij e Shabwa e nel governatorato di Hadramaut, già presidio di AQAP, e ha guadagnato posizioni con una serie di atti eversivi ai danni

della popolazione di etnia *Houthi*, nonché delle Forze governative. In prospettiva, la formazione parrebbe orientata a contendere ad AQAP il ruolo di principale gruppo terroristico in quel territorio. Decisiva in tal senso sarà la sua capacità di attrarre finanziamenti, rafforzare la propria potenzialità offensiva, aumentare il numero degli aderenti e guadagnare il sostegno delle tribù locali. Si inquadra in questo contesto l'incremento delle azioni dimostrative da parte di gruppi armati islamico-radicali riconducibili a DAESH, soprattutto nell'area di Aden, contro personalità politiche e amministrative.

La regione *Af-Pak:* la sfida del *Califfato* alla vecchia guardia qaidista e talebana

Gli eventi più rilevanti per la definizione della cornice di sicurezza nel quadrante afghano-pakistano sono individuabili nell'espansione di DAESH, nella recrudescenza dell'attività offensiva dell'insorgenza, che controllerebbe l'80% del territorio, e nell'annuncio della morte del *leader* del movimento *Taliban,* Mullah Omar (avvenuta, con ogni probabilità, già nel 2013) seguito dalla nomina del suo successore, Mohammad Aktar Mansur, che ha ricevuto il sostegno della *leadership* di *al Qaida*.

L'area ha registrato nel 2015 l'espansione della proiezione locale di DAESH, *Khorasan Shura,* avvenuta a seguito di una campagna di proselitismo e reclutamento a sostegno della "causa" siro-irachena (*vds. box n. 8*).

Il movimento *Taliban* ha tentato di opporsi a DAESH nelle province orientali e meridionali afghane, a ridosso del confine con il Pakistan, ed ha iniziato, in aprile, la consueta "campagna di primavera"contro basi militari internazionali, rappresentanti stranieri e obiettivi governativi afghani civili e militari, così corroborando la capacità dell'insorgenza di controllare vaste aree del territorio, di condurre iniziative offensive nelle grandi città, compresa la Capitale Kabul, e di autofinanziarsi con attività illecite come il traffico di droga.

Il quadro di sicurezza permane critico. La crisi interna al movimento *Taliban*, acuitasi con l'attentato al nuovo *leader* Mansur, in novembre, nonché la presenza di DAESH rappresentano veri e propri *game changer* non solo per gli equilibri interni all'insorgenza –

box 8

KHORASAN SHURA

L'organizzazione più rappresentativa di DAESH nell'area *Af-Pak*, la *Khorasan Shura*, denominata anche *Islamic State in the Khorasan Province* (ISKP), costituitasi ufficialmente il 10 gennaio 2015, è riuscita a penetrare in territorio afghano-pakistano grazie ad una campagna di proselitismo e reclutamento a beneficio degli attori jihadisti operanti nel teatro siro-iracheno. Tale espansione, per quanto concerne il Pakistan, ha riguardato, in particolare, le aree di Islamabad, Peshawar, Quetta e Karachi. Ne sono stati protagonisti soprattutto miliziani pakistani, defezionisti dell'organizzazione terroristica *Tehrik-e Taliban Pakistan* (TTP).

Nonostante non annoveri più di un paio di migliaia di adepti, ISKP conterebbe comunque su un numero cospicuo di simpatizzanti.

e alla galassia jihadista – e per le ripercussioni sugli interessi occidentali *in loco*, ma anche perché l'organizzazione di al Baghdadi potrebbe trarre profitto dalle fratture in seno al movimento *Taliban* alla luce delle connessioni, sia storiche che contingenti, tra i combattenti nei vari teatri di crisi in Africa ed in Medio Oriente. Diviene quindi determinante la capacità delle Autorità politiche afghane e pakistane di convergere su un'azione comune di contrasto alle diverse anime terroristiche, specie DAESH, e di portare altresì al tavolo negoziale il maggior numero possibile di esponenti *Taliban*.

Anche i Paesi centro-asiatici, in ragione della loro prossimità al teatro afghano-pakistano, appaiono ad elevato rischio di penetrazione da parte di DAESH, in particolare:

- il Tagikistan, dove l'*Islamic Jihad Union*, affiliato al *Califfato*, ha dichiarato di avere assunto il controllo di vaste zone di confine con l'Afghanistan;
- l'Uzbekistan e il Kirghizstan, dove si teme il ritorno di numerosi combattenti attualmente impegnati in Siria, Iraq ed Afghanistan.

I fermenti jihadisti nel Sud-Est asiatico

La cornice di sicurezza del **Sud-Est asiatico**, nel corso del 2015, è stata caratterizzata sia dall'attivismo di gruppi radicali endogeni, sia dall'azione di DAESH, volta a fare proseliti e a promuovere affiliazioni.

Il gruppo di al Baghdadi si starebbe diffondendo progressivamente nelle Filippine, in Indonesia ed in Malesia, ove numerose sigle jihadiste, alcune delle quali riconducibili ad *al Qaida*, non sentendosi più adeguatamente rappresentate dall'organizzazione di al Zawahiri, avrebbero aderito al progetto lanciato dalla formazione irachena. In questa cornice sembra collocarsi l'attentato multiplo compiuto il 14 gennaio 2016 nel centro di Giacarta, rivendicato da DAESH.

In termini di contrasto al terrorismo, le Autorità locali hanno adottato provvedimenti legislativi che hanno consentito l'arresto di numerosi miliziani intenzionati a raggiungere il teatro siro-iracheno, nonché l'eliminazione di cellule pronte a colpire obiettivi istituzionali ed occidentali.

Nel **Subcontinente indiano**, soprattutto in Bangladesh, il fenomeno della radicalizzazione ha concorso ad alimentare la minaccia terroristica espressa dalle locali formazioni estremiste islamiche ed a consolidare la presenza di *al Qaida* nel Subcontinente indiano, "istituita" da al Zawahiri, che avrebbe rivendicato l'uccisione di alcuni *blogger* e personalità della cultura bangladese accusati di blasfemia. In tale contesto si inserisce il tentativo di DAESH di penetrare l'area estendendo la propria influenza, come dimostrato dalle rivendicazioni di alcune azioni ostili ai danni di personale straniero. Tuttavia, in merito agli omicidi del connazionale Cesare Tavella (Dacca, 28 settembre 2015) e del cittadino giapponese Hoshi Kunio (Distretto settentrionale di Rangpur, 3 ottobre 2015), nonché al ferimento del Padre Missionario Piero Parolari (Distretto settentrionale di Dinajpur, 18

novembre 2015), le Autorità bangladesi hanno smentito qualsiasi coinvolgimento diretto di DAESH.

Per quanto attiene alla **Repubblica Popolare Cinese**, si è registrato un incremento dell'attivismo dei separatisti *uiguri,* stanziati nella regione nord-occidentale dello Xinjang, che avrebbero condotto azioni anche in altre aree del Paese e che conterebbero propri combattenti nelle file jihadiste operanti in vari teatri di conflitto, dall'Afghanistan alla Siria.

Ricondurrebbe alla pista uigura, tra l'altro, una delle ipotesi investigative sull'attentato al tempio induista di Bangkok (17 agosto 2015) che ha provocato 22 vittime, la maggior parte delle quali cittadini cinesi.

IL *DOSSIER* MIGRATORIO

IL *DOSSIER* MIGRATORIO

L'emergenza migratoria nella prospettiva intelligence

Il fenomeno migratorio nel Mediterraneo ha assunto anche nel 2015 proporzioni rilevanti favorite dalle precarie condizioni socio-economiche e di sicurezza in numerosi Stati africani, della fascia costiera settentrionale e di quella subsahariana, nonché nel Vicino e Medio Oriente ed in Asia.

La composizione dei flussi migratori irregolari che hanno interessato il bacino del Mediterraneo appare significativamente mutata con l'arrivo sempre più consistente di profughi, in fuga da aree di crisi e di conflitto.

Le rotte maggiormente utilizzate per l'ingresso nello spazio Schengen sono state quelle:

- nordafricana (o del Mediterraneo centrale), principale canale d'accesso alle coste italiane (*vds. box n. 9*);
- anatolico-balcanica, quale corridoio d'ingresso principale per i migranti provenienti dal Vicino Oriente (Siria, Palestina, Iraq) e dall'Asia (Pakistan, Afghanistan, Bangladesh), per via:
  - marittima (o del Mediterraneo orientale), che ha interessato soprattutto la Grecia;
  - terrestre (o dei Balcani occidentali), che ad oggi investe per lo più i Paesi dell'Europa centro-orientale.

Meno battute la rotta cd. settentrionale, utilizzata dai migranti che originano dall'Est europeo e dall'Asia e che tentano di raggiungere i Paesi Schengen attraverso la Russia e le Repubbliche dell'ex spazio sovietico, e quella del Mediterrano occidentale, che attraversa il suolo marocchino per accedere ai confini spagnoli.

box 9

I NUMERI DELLE DIRETTRICI MARITTIME

Il flusso migratorio via mare si è confermato la componente più visibile del fenomeno migratorio irregolare in direzione dell'Italia: secondo i dati del Ministero dell'Interno nel corso del 2015 sono giunte (sbarcate/intercettate) 153.842 persone, cifra inferiore a quella registrata nel 2014 (170.100). Tale decremento rispetto al 2014 è verosimilmente dovuto, più che a una diminuita pressione migratoria, alla riattivazione della direttrice anatolico-balcanica che ha riorientato l'esodo dei siriani, nonché dei migranti provenienti da Iraq, Afghanistan e Pakistan. Vanno anche considerate le difficoltà che affrontano le organizzazioni criminali libiche nel reperire naviglio in legno, in grado di trasportare un numero maggiore di migranti, e il conseguente ripiego su battelli pneumatici, che hanno una portata più limitata.

Nel flusso degli arrivi via mare in territorio nazionale:

- la rotta balcanica è del tutto residuale: anche nel 2015 la Libia è stata il Paese di imbarco per quasi il 90% degli arrivi, seguita dall'Egitto (7,2%). Gli arrivi in Italia dalla Turchia sono stati circa l'1,6%;
- si è fortemente ridimensionata l'aliquota di migranti di dichiarata nazionalità siriana, che per il 2014 è stata di quasi il 25%, mentre per il 2015 è poco meno del 5%. Dato, questo, del tutto coerente con l'impennata della corrente migratoria lungo la rotta greca e turca, che ha prodotto un "effetto domino" nel quadrante balcanico;
- tra le prime 10 nazionalità dei migranti giunti nel 2015, otto sono africane.

Il trasferimento dalle aree di origine a quelle di destinazione costituisce un *business* rilevante per diversi circuiti illegali dediti al favoreggiamento dell'immigrazione clandestina i quali, forti del controllo del territorio, assicurano il necessario sostegno logistico in termini di fluidificazione e continuità dei diversi segmenti delle direttrici di trasferimento e di *procurement* di documenti falsi o rubati.

La massa di persone in movimento verso lo spazio comunitario, oltre a costituire un'emergenza di carattere umanitario, sanitario e di ordine pubblico, può presentare insidie sul piano della sicurezza.

Nella medesima ottica, la ricerca intelligence è stata focalizzata sulle possibili, ancorchè non sistematiche, contaminazioni tra immigrazione clandestina e terrorismo, alla luce di alcuni indicatori.

Innanzitutto, i contesti di crisi siriana, irachena, libica, subsahariana e del Corno d'Africa sono infiltrati in parte da espressioni terroristiche di matrice islamista che pos-

sono inquinare i canali dell'immigrazione e sottoporre alla radicalizzazione elementi poi destinati ad emigrare nei Paesi europei.

Di rilievo é, inoltre, la possibilità di acquisire documenti falsi, contraffatti o autentici, nella disponibilità anche di formazioni terroristiche, che consente l'ingresso di ex combattenti o di militanti riconducibili a milizie islamiste.

Va infine considerato come l'aver vissuto in aree di guerra, talvolta partecipando attivamente ai combattimenti, possa conferire ai nuovi migranti un profilo potenzialmente critico, derivante soprattutto dall'*expertise* "militare" acquisita.

Le filiere del traffico nel bacino del Mediterraneo

La spinta migratoria ha rafforzato la competitività dei gruppi criminali dediti al trasferimento dei clandestini, ormai capaci di esercitare un capillare controllo delle aree interessate dal traffico e di fornire il necessario supporto logistico ai migranti, anche ricorrendo alla corruzione nelle aree di partenza, di transito e di imbarco.

Nel Nord Africa le organizzazioni di trafficanti, a prevalente composizione multietnica, sono per lo più libiche, egiziane, somale, eritree, sudanesi, nigeriane e maliane, mentre nel Mediterraneo orientale operano reti criminali a prevalente matrice turco-irachena, con il diffuso coinvolgimento di elementi greci e ucraini – questi ultimi impiegati soprattutto come scafisti – e talvolta anche di soggetti asiatici (afghani, iracheni, iraniani e pakistani).

L'elevata remunerativitá del traffico ha indotto numerosi sodalizi criminali, impegnati nei tradizionali settori del contrabbando e del narcotraffico, ad estendere le attività illegali anche al *business* migratorio, talvolta condividendone la gestione con formazioni armate irregolari, soprattutto in Libia. Qui operano organizzazioni di trafficanti strutturate e flessibili, a prevalente composizione multietnica, in grado di gestire tutte le fasi del trasferimento e di interagire come un *network*, anziché secondo logiche associative strutturate gerarchicamente, dimostrandosi capaci di approfittare delle favorevoli opportunità contingenti nello scenario mediterraneo, nonché delle disomogeneità tra le legislazioni dei Paesi interessati per rimodulare prontamente direttrici e forme di trasferimento.

Il territorio libico si è quindi consolidato quale snodo prioritario e privilegiato della deriva migratoria africana in direzione dell'Europa, complici la locale diffusa instabilità politica e l'assenza di un efficace dispositivo di contrasto anticrimine.

Nell'area anatolica le organizzazioni dei trafficanti sovente ricorrono alla promozione, anche tramite internet, di una "politica dei prezzi" per il trasferimento dei clandestini in Europa calibrata a seconda delle esigenze e della capacità economica del migrante. Sono state altresì rilevate iniziative di trafficanti nordafricani volte a ricercare e stabilire collaborazioni con i gruppi criminali locali ai fini della gestione comune dei trasferimenti in Europa dalle coste egiziane o turche.

In Italia si è assistito alla proliferazione di gruppi criminali etnici composti prevalentemente da soggetti egiziani, del Corno d'Africa (*vds. box n. 10*) e da ultimo rumeni, specializzati sia nella falsificazione documentale – compresa quella necessaria a concludere assunzioni fittizie in settori del lavoro stagionale – sia nel fornire assistenza ai migranti per il trasferimento dai centri di accoglienza alle località di destinazione nel Nord Europa.

È emersa inoltre l'operatività di sodalizi brindisini attivi nel trasferimento di migranti dalle coste della penisola balcanica meridionale verso il nostro Paese. Si tratta di ex contrabbandieri di tabacchi lavorati esteri (TLE), esperti scafisti capaci di eludere la sorveglianza marittima, che utilizzerebbero imbarcazioni veloci di limitate dimensioni (non oltre le venti persone) intercettando una domanda in grado di sostenere costi elevati di viaggio.

Le insidie della rotta balcanica

La rotta balcanica percorsa dai flussi migratori diretti verso i Paesi dell'Europa centrale e settentrionale – un tempo residuale per numero di transiti rispetto alla più trafficata direttrice che dalle coste nordafricane (specie dalla Libia) giunge sino alle sponde dell'Italia meridionale – ha conosciuto nella seconda metà dell'anno un considerevole impulso, raccogliendo flussi che originano dai Paesi del Medio ed Estremo Oriente e, talora, anche dall'Africa (*vds. box n. 11*).

box 10

IL *NETWORK* SOMALO

Nel quadro del fenomeno migratorio proveniente dall'Africa, particolare rilievo hanno assunto i *network* somali, in virtù delle capacità dimostrate nella gestione di tutte le fasi del flusso in uscita dal Corno d'Africa e diretto verso il Vecchio Continente. In territorio nazionale, le reti criminali somale si sono evidenziate quale connettore e snodo logistico per immigrati clandestini della medesima nazionalità. Gli ingenti proventi illeciti che ne derivano configurano ulteriori profili di rischio, in quanto appaiono di difficile tracciabilità, transitando su circuiti finanziari non convenzionali come l'*hawala*. In tale contesto si delinea non solo la possibilità che i profitti derivanti dal *business* migratorio gestito dalla rete criminale somala concorrano a finanziare l'organizzazione terroristica *al Shabaab*, ma anche il rischio che il *network* possa assicurare copertura e supporto logistico per l'ingresso e gli spostamenti nello spazio Schengen di militanti jihadisti.

Il mutamento è parso dettato dalla diminuzione delle partenze dalle coste libiche soprattutto di profughi siriani, indirizzatisi in numero crescente verso lo scenario balcanico, per il concorso dei seguenti fattori:

- la situazione assai fluida e precaria in Libia, ove l'instabilità politica e i continui scontri tra milizie costituite su base tribale per il controllo del territorio, aggravati da pericolosi innesti jihadisti, mettono significativamente a rischio l'incolumità dei migranti, soprattutto mediorientali, molti dei quali hanno pertanto preferito optare per la direttrice anatolico-balcanica;
- gli opportuni provvedimenti emanati sia dalle Autorità del Libano e dell'Algeria in materia di introduzione del visto d'ingresso per i cittadini siriani, che da quelle giordane in relazione alle attività foto-segnaletiche svolte per evitare infiltrazioni terroristiche, che hanno reso difficoltoso il transito in quei Paesi;
- la decisa azione di contrasto messa in atto dalle Autorità egiziane nei confronti dei gruppi terroristici e criminali e l'intensificata attività di sorveglianza nel Sinai, area di transito obbligata dei flussi orientali verso l'area libica.

Tale massiccia ondata migratoria ha investito un quadrante, quello balcanico, già provato da fragilità politico-economiche e caratterizzato da limitate capacità di accoglienza ed assorbimento.

Per di più, il fenomeno si caratterizza per la sua attitudine di riorientarsi a secon-

box 11

GLI ITINERARI DELLA ROTTA BALCANICA

Il territorio turco si è confermato lo snodo principale per l'instradamento dei migranti verso l'Europa occidentale lungo rotte che attraversano vari Stati balcanici.

Una parte dei flussi segue la direttrice terrestre che accede ai confini della Grecia e della Bulgaria per raggiungere poi l'Ungheria e l'Austria e proseguire verso i Paesi del Nord Europa.

Al contempo, una pressione migratoria di inedite proporzioni ha interessato la fascia costiera egea della Turchia per raggiungere via mare le isole elleniche (Kos, Leros, Symi, Lesbo, Chios, Samo, ecc.), in attesa di proseguire, per via terrestre, attraverso i Balcani occidentali, o sporadicamente per via marittima, verso l'Italia, dalle aree costiere greche sul Mar Ionio.

da delle barriere confinarie e degli interventi statuali di contenimento. Aspetto, questo, che non fa escludere la possibilità di reindirizzamenti, anche massicci, della corrente migratoria verso i confini nazionali, terrestri o marittimi.

Il rischio di infiltrazioni terroristiche nei flussi migratori, che quanto alla direttrice nordafricana, nonostante ricorrenti *warning*, non ha trovato specifici riscontri, si presenta più concreto lungo l'asse della rotta balcanica, specialmente in relazione ad un quadro informativo che attesta:

- le vulnerabilità di sicurezza legate all'imponente flusso di profughi provenienti dal teatro siro-iracheno;
- la centralità della regione quale via di transito privilegiata bidirezionale di *foreign fighters,* oltre che – come già detto – quale zona di origine di oltre 900 volontari arruolatisi nelle file del jihadismo combattente (*vds. box n. 12*);
- la presenza nell'area di realtà oltranziste consolidate, in grado di svolgere un ruolo attivo nella radicalizzazione dei migranti.

box 12

LA DIFFUSIONE DEL RADICALISMO ISLAMICO NEI BALCANI

A sviluppo di un *trend* già segnalato nella Relazione annuale 2014, il radicalismo islamico nei Balcani – retaggio delle vicende belliche degli anni '90 e delle connesse ricadute anche in termini di fragilità politiche, tensioni interetniche e infiltrazioni criminali – ha fatto registrare una decisa rivitalizzazione di pari passo con l'evolversi della crisi siriana e, soprattutto, con la progressiva affermazione di DAESH.

La diffusione del messaggio jihadista – che trova nella regione *humus* fertile specie tra le fasce più disagiate, evidenziando una significativa capacità di presa anche tra le comunità balcaniche della diaspora – si è accompagnata all'attivismo di movimenti salafiti/wahhabiti volto alla costituzione di una strutturata rete di supporto per agevolare il rientro di combattenti dalla Siria e dall'Iraq.

Tale fermento organizzativo ha riguardato tra l'altro: l'approvvigionamento e il trasferimento di armi ed esplosivi; il reperimento di documenti, anche con il supporto di organizzazioni criminali; la costituzione di Organizzazioni non Governative da utilizzare quale copertura; l'individuazione di *safe house* dove ospitare i *returnees*; il coordinamento tra le diverse aggregazioni di estrazione salafita/wahhabita e gruppi estremisti riconducibili all'irredentismo panalbanese.

Come in altri contesti territoriali, il panorama delle formazioni jihadiste operanti nei Balcani è parso esprimere due diversi orientamenti: l'uno, filo-qaidista, presente soprattutto in Bosnia e nel Sangiaccato montenegrino; l'altro, pro-DAESH, diffuso principalmente in Kosovo e in Macedonia. Non sono mancati, peraltro, segnali di dialogo e sinergie tra le due componenti.

In prospettiva, lo scenario delineato profila rischi sia per il suo potenziale destabilizzante, sia per l'eventualità di un insediamento nella regione di basi logistiche in grado di supportare pianificazioni terroristiche contro Paesi europei, incluso il nostro.

IL PRESIDIO DEL SISTEMA PAESE

IL PRESIDIO DEL SISTEMA PAESE

Le priorità dell'intelligence economico-finanziaria: assetti strategici e interesse nazionale

L'azione di intelligence si è dispiegata in un quadro economico con scenari in rapida evoluzione, caratterizzati da: espansione dell'attività economica nei principali Paesi avanzati e rallentamento della Cina; indebolimento del commercio mondiale e volatilità dei mercati finanziari e valutari; caduta dei corsi petroliferi; graduale ripresa dell'economia italiana, che per il 2015 consente di attestare allo 0,8% la stima di crescita del Prodotto Interno Lordo (PIL) (+0,7% considerando il numero dei giorni lavorativi, *vds. Banca D'Italia, Bollettino Economico gennaio 2016*). Come per le altre economie europee, l'inflazione calcolata sull'indice dei prezzi al consumo è rimasta debole (+0,1% su base annua), risentendo principalmente del calo della componente energetica nonché della debolezza della domanda (*vds. ISTAT, Prezzi al consumo dicembre 2015*).

Quanto agli altri dati congiunturali relativi al terzo trimestre 2015, i consumi delle famiglie sono aumentati moderatamente rispetto al trimestre precedente (+0,4%), in linea con la variazione prevista sull'anno, mentre gli investimenti fissi lordi hanno subito una flessione dello 0,4%, sebbene si stimi un incremento tendenziale dello 0,5% su base annua (*vds. Banca D'Italia, Bollettino Economico gennaio 2016*). Nei primi undici mesi dell'anno le importazioni sono aumentate del 3,3% rispetto allo stesso periodo del 2014, mentre le esportazioni hanno registrato un incremento pari al 3,8% *(vds. ISTAT, Commercio con l'estero novembre 2015)*. La produzione industriale nel medesimo arco temporale è aumentata dell'1,1% in raffronto all'omologo periodo del 2014 (*vds. ISTAT, Produzione industriale novembre 2015*). Il mercato del lavoro ha beneficiato anche delle norme introdotte dal *Jobs Act*, inclusi gli sgravi fiscali sui neoassunti con contratto a tempo indeterminato, che hanno comporta-

to una riduzione del tasso di disoccupazione attestatosi, in dicembre, all'11,4% rispetto al 12,9% del dicembre 2014. La disoccupazione giovanile si è stabilizzata al 37,9%, valore che permane elevato pur rappresentando il minimo degli ultimi due anni (*vds. ISTAT, Occupati e Disoccupati dicembre 2015 e 2014).*

Per quanto riguarda la finanza pubblica, il disavanzo corrente si è attestato al 2,6% del PIL e il rapporto debito/PIL è risultato pari al 132,8%, in lieve aumento rispetto al 2014 (*vds. Banca D'Italia, Bollettino Economico gennaio 2016*).

Nel quadro della graduale ripresa dell'economia italiana, il processo di internazionalizzazione del Sistema Paese e la capacità d'attrazione degli investimenti esteri rappresentano fattori di sviluppo imprescindibili, a supporto dei quali il Comparto intelligence ha continuato ad orientare la propria attività informativa. In coerenza con le consolidate direttrici di intervento, questa si è anzitutto focalizzata sulle strategie acquisitive di operatori esteri, sia industriali che finanziari, nei confronti di realtà aziendali attive nei segmenti produttivi di rilevanza strategica. Il *focus* informativo è stato indirizzato, in particolare, verso le imprese con una significativa presenza industriale e commerciale nei principali mercati internazionali. In tal senso, hanno acquisito grande importanza nel monitoraggio di intelligence i casi di progressiva sostituzione, nella compagine azionaria di imprese nazionali, di soci "industriali", legati ad una logica di sviluppo economico e produttivo di lungo periodo, con soci "finanziari", mossi da intenti speculativi di breve periodo.

A prosieguo delle linee di azione tracciate nelle Relazioni degli scorsi anni, l'attività del Comparto ha inoltre riguardato la possibile sottrazione di *know-how* scientifico e tecnologico in caso di cessione di quote societarie di imprese riconducibili alla filiera della sicurezza nazionale, nonché lo spostamento al di fuori dei confini nazionali dei centri decisionali di imprese italiane ed il correlato fenomeno della delocalizzazione produttiva, suscettibile di comportare riflessi negativi sui livelli occupazionali.

Sempre nel quadro dell'azione intelligence sviluppata a tutela del *know-how*, segnatamente nel caso delle piccole e medie imprese anche innovative, ha costituito oggetto di monitoraggio la diffusione di strumenti finanziari alternativi espressivi di un processo di disintermediazione del credito.

Nel corso dell'anno, particolare attenzione è stata poi rivolta all'individuazione dei profili di opportunità e di rischio connessi al crescente attivismo sui mercati internazionali di soggetti, in prevalenza asiatici (fra i quali taluni Fondi Sovrani), con i quali l'Italia ha avviato sinergie. Ciò in un quadro di accresciuta competizione internazionale per accedere ai flussi di capitali promananti da *player* di quel quadrante, nonché per avvalersi della possibilità di investire nei mercati orientali in virtù delle politiche di apertura verso imprese straniere.

La logica dell'attività intelligence in ambito economico e finanziario è stata quella del supporto informativo all'Autorità di governo per un utilizzo calibrato degli strumenti interdittivi previsti dalla normativa,

inteso, a fronte delle opportunità offerte dall'internazionalizzazione dei sistemi produttivi e dei mercati finanziari, a garantire un efficace presidio dei settori della difesa e della sicurezza nazionale, nonché nei segmenti di rilevanza strategica dell'energia, dei trasporti e delle comunicazioni, cosi come definiti dalla norma sulla cd. *Golden Power* (L. 56 dell'11 maggio 2012).

L'attività informativa nel contesto della proiezione internazionale dei nostri operatori economici ha riguardato anche il versante della sicurezza dei trasporti, con particolare riguardo al fenomeno della pirateria marittima (*vds. box n. 13*).

Le vulnerabilità del sistema bancario e finanziario

L'intelligence concorre informativamente a garantire la tutela del sistema bancario e degli interessi economici ed industriali del Paese. Al riguardo, l'azione si è concentrata su due aspetti principali: il riassetto del sistema bancario e finanzia-

box 13

LA PIRATERIA NELLE ACQUE AFRO-ASIATICHE

Il fenomeno della pirateria marittima costituisce un prioritario *target* informativo anche per la sua incidenza sulla sicurezza economica. Le compagnie italiane di navigazione attive nei trasporti marittimi internazionali (230 gruppi armatoriali, con circa 1.000 navi commerciali e *tanker* e un volume di merci trasportato pari a 122 milioni di tonnellate), costituiscono un settore che impiega 24.000 persone tra membri di equipaggio e addetti a terra, con investimenti per 15 miliardi di Euro.

In tale ambito, specifica attenzione è stata rivolta alle dinamiche economico-finanziarie del fenomeno nel Golfo di Guinea, in Somalia e nello Stretto di Malacca, con particolare riguardo ai canali di trasferimento e di riciclaggio dei proventi illecitamente conseguiti.

Quanto ai tratti evolutivi del fenomeno:

- in Somalia, Golfo di Aden e Oceano Indiano la minaccia è in graduale declino a causa della massiccia presenza di unità militari sia inquadrate nelle Missioni internazionali a protezione dei traffici marittimi commerciali, sia impiegate in attività di pattugliamento da parte di singoli Paesi;
- nel Golfo di Guinea, la pirateria nigeriana opera in prossimità delle città di Lagos, Port Harcout e Calabar, in una zona ricca di insenature dove i gruppi di pirati custodiscono le navi e gli equipaggi sequestrati. Di rilievo, nel contesto, è la crescente aggressività dei gruppi di pirati là dove transitano anche navi portacontainer e per il trasporto merci, in un'area ove alcune compagnie di navigazione italiane hanno acquisito la concessione di banchine portuali per la movimentazione di merci;
- nello Stretto di Malacca, i gruppi di pirati malesi ed indonesiani hanno affinato la tecnica di assalto delle navi, privilegiando attacchi *hit-and-run* per sottrarre il carico trasportato, direttamente verso piccole petroliere per il trasporto di carburanti raffinati, e rapinare i membri dell'equipaggio, avvalendosi di navi madre.

rio nazionale avvenuto nel corso del 2015, a seguito anche di alcuni cambiamenti normativi/strutturali e delle misure di supervisione adottate dalla Banca Centrale Europea, ed il possibile interesse da parte di operatori esteri a cogliere opportunità di investimento nel settore.

In particolare, sono emerse in taluni casi (soprattutto istituti di piccole e medie dimensioni) criticità in relazione alla concomitanza di diversi fattori, tra cui la lenta ripresa degli impieghi, l'ammontare delle sofferenze, le perdite di bilancio, la concentrazione degli attivi, la gravità delle carenze patrimoniali (registrate, in particolare, con riguardo ad alcuni istituti popolari), l'ingresso nell'azionariato di nuovi soci (anche attraverso l'utilizzo di veicoli societari "fiduciari") e, infine, i casi di disinvolta gestione del credito.

In ordine agli equilibri interni di governo societario, si è rilevata l'influenza esercitata da alcuni fondi d'investimento internazionali sulla *corporate governance* degli istituti di credito partecipati.

Il sistema bancario nazionale risulta permanere, principalmente, esposto a:

- forte incidenza degli accantonamenti, derivanti dall'esigenza di coprire perdite potenziali per crediti deteriorati;
- ingresso nell'azionariato di soggetti stranieri animati da intenti speculativi. Tale profilo di rischio si è rivelato particolarmente accentuato per quegli istituti in situazione di particolare criticità e per quelli che, avendo assetti economici o di *governance* non rispondenti ai criteri di stabilità disposti nell'ambito del Meccanismo di vigilanza unico europeo, hanno dovuto affrontare importanti ristrutturazioni;
- contagio, per le banche con un profilo internazionale, derivante da situazioni di instabilità in altri Paesi.

Sempre con riguardo alla tutela dei mercati finanziari e creditizi, sono state inoltre monitorate le attività di fondi di investimento svolte in violazione della normativa vigente e suscettibili di alterare il corretto funzionamento del mercato dei prodotti finanziari.

Va infine sottolineato che lo sviluppo dei processi di disintermediazione bancaria ha contribuito ad accrescere l'impiego di tecnologie *web-based* per operazioni di *funding* e pagamenti *on-line*. Con specifico riguardo alla diffusione delle "criptovalute", l'attenzione è stata focalizzata sulla tecnologia *blockchain*, sfruttata anche da *bitcoin* (*vds box n. 14*), in considerazione dei rischi di impiego di tali strumenti per finalità illecite.

Competitività e spionaggio industriale

Nel contesto della competizione tra sistemi Paese, si è rilevato un sempre maggiore ricorso agli strumenti di spionaggio cibernetico finalizzato ad accrescere la capacità conoscitiva dell'attore ostile. In particolare, questa metodologia di ingerenza appare concepita in modo da consentire ai potenziali acquirenti stranieri di svolgere attività di *due diligence* occulte e quindi di conseguire uno sleale vantaggio in-

box 14

L'EVOLUZIONE DEL SISTEMA *BITCOIN*

Il *bitcoin*, una delle prime valute virtuali decentralizzate, si basa su un *software open-source* (disponibile *on-line* dal 2009) che permette transazioni virtuali prive di qualunque attività di intermediazione e può essere utilizzata come mezzo di scambio o detenuta a scopo di investimento, nonché trasferita, archiviata e negoziata elettronicamente.

Tale *virtual currency* può essere acquistata con moneta tradizionale su una piattaforma di scambio, viene movimentata attraverso un conto personalizzato (cd. portafoglio elettronico) che permette ai titolari di effettuare transazioni con altri utenti (presso esercizi commerciali e/o persone fisiche che l'accettano) ed è riconvertibile in moneta legale.

Bitcoin rappresenta un'applicazione della tecnologia *blockchain* che consente di scambiare dati e informazioni, a prescindere dalla conoscenza delle controparti e dall'esistenza di un garante del sistema.

L'assenza di regolamentazione, di vigilanza e di obblighi informativi, nonché l'anonimato dei titolari dei portafogli elettronici, espone il *bitcoin* – così come le altre valute virtuali – a possibili utilizzi strumentali per la realizzazione di transazioni finanziarie collegate ad attività illecite, tra cui il riciclaggio di denaro e il finanziamento del terrorismo, rappresentando così un *vulnus* per l'integrità e la trasparenza del sistema finanziario.

formativo, su cui far leva nel corso delle negoziazioni miranti ad acquisire il controllo degli operatori economici *target*.

Tali attività hanno riguardato aziende operanti in settori di interesse strategico per il Paese e ad elevato *know-how*, tra cui la ricerca aerospaziale, l'energia (comprese le fonti rinnovabili) e le telecomunicazioni (*vds. box n. 15*).

Sicurezza energetica: fonti di approvvigionamento e reti infrastrutturali

In un contesto internazionale caratterizzato dal progressivo spostamento del baricentro geografico dei consumi energetici verso le economie asiatiche, la dipendenza nazionale dalle importazioni mantiene un carattere strutturale, esponendo il Paese alla volatilità dei flussi di approvvigionamento, dei corsi petroliferi e dei cambi valutari.

Sebbene l'attuale congiuntura abbia continuato a vedere un perdurante eccesso di offerta di materie prime energetiche, che ha favorito le economie importatrici come quella italiana, nondimeno i mercati internazionali hanno continuato a mostrare un profilo di elevato dinamismo e quindi richiesto un'attività costante di monitoraggio, volta a cogliere le implicazioni in termi-

box 15

LO SPIONAGGIO DIGITALE

È una pratica sempre più diffusa quella dell'attacco mirato in ambito aziendale volto a guadagnare un vantaggio competitivo da parte di altre società di settore attraverso l'acquisizione illecita di informazioni sensibili.

Proprio sul versante del *cyber espionage* sono emerse forme di aggressione particolarmente sofisticate e non rilevabili da parte dei *software* di sicurezza. In alcuni tipi di attacchi, il sistema *target*, una volta compromesso, rischia di rimanere infettato anche dopo gli interventi di ripristino, continuando quindi a "patire" la contaminazione.

Alcune campagne offensive sono risultate alla base di continuative attività di esfiltrazione dati con l'uso di *malware* sempre più avanzati, poiché riescono ad individuare e sfruttare le vulnerabilità dei sistemi prima ancora che queste emergano all'attenzione o che siano disponibili i relativi aggiornamenti risolutivi.

ni di sicurezza dei possibili sviluppi futuri.

Particolare attenzione è stata dedicata ai mercati internazionali degli idrocarburi che, in continuità con gli anni passati, hanno evidenziato rischi diversi a seconda delle fonti. Nel caso del petrolio, la scelta dell'OPEC di non procedere a un immediato taglio della produzione, anche a fronte di una domanda mondiale cresciuta meno dell'offerta, si è sommata al sostanziale mantenimento dei livelli produttivi dei Paesi non-OPEC, Stati Uniti e Russia *in primis*, determinando nel complesso un calo delle quotazioni del greggio, un aumento delle scorte e, in ultima analisi, una sostanziale assenza di rischi specifici connessi all'approvvigionamento petrolifero. In questo quadro, particolare attenzione è stata comunque rivolta al comparto nazionale della raffinazione, che, nonostante l'aumento dei margini, è interessato da una crisi strutturale dovuta sia alla contrazione dei consumi nazionali, sia all'ingresso di nuovi *competitor* nel bacino del Mediterraneo e in Medio Oriente.

Quanto all'approvvigionamento di gas naturale, l'attività informativa si è invece indirizzata alle aree di produzione e transito, ove situazioni di instabilità politica e tensioni regionali hanno determinato specifici rischi di riduzione dei flussi, sia lungo la direttrice nordafricana, sia lungo quella esteuropea. In quest'ultimo quadrante, nel corso dell'anno l'erogazione del gas russo diretto in Europa non ha peraltro fatto registrare interruzioni,

pur nel perdurare dell'incertezza collegata alla crisi ucraina (*vds. box n. 16*).

Il presidio informativo ha riguardato anche le dinamiche evolutive nel settore delle infrastrutture di adduzione, in particolare sia la realizzazione di gasdotti internazionali volti a diversificare l'origine dell'approvvigionamento nazionale, sia la sospensione e la cancellazione di progetti intesi a veicolare il gas di origine russa attraverso nuove rotte. Di rilievo anche i progetti di sviluppo infrastrutturale relativi ai rigassificatori, la cui realizzazione è stata peraltro oggetto di riconsiderazione, a causa degli elevati costi di costruzione e del rischio di un loro scarso utilizzo connesso alla debolezza dei consumi italiani ed europei.

Gli Organismi intelligence hanno assicurato anche il concorso informativo a protezione dell'integrità delle infrastrutture nazionali, anzitutto quelle del sistema elettrico, e si sono avvalsi altresì, allo scopo, degli opportuni strumenti di *partnership* pubblico-privato. La progressiva informatizzazione del settore energetico ha peraltro esposto quest'ultimo a un rischio

box 16

GLI SVILUPPI DELLA CRISI UCRAINA

Gli accordi di pace sottoscritti a Minsk il 12 febbraio 2015 dal Gruppo di Contatto (composto da Russia, Ucraina, separatisti filo-russi delle regioni orientali del Donbass e OSCE) hanno formalmente rappresentato un punto di svolta nella crisi ucraina, delineando una completa ed articolata *road map* per la risoluzione del conflitto tra le Autorità di Kiev e i separatisti (conflitto al quale sono correlate le tensioni tra Ucraina e Federazione Russa, nonché le sanzioni settoriali emanate dalla UE nei confronti di Mosca).

Tra le misure previste dal Protocollo di Minsk: l'immediato cessate-il-fuoco; il ritiro di tutte le armi pesanti e l'arretramento delle forze per la creazione di un'area-cuscinetto di 50 chilometri, quest'ultima da affidare al monitoraggio dell'OSCE; lo svolgimento di elezioni locali nei distretti occupati dai separatisti; il recupero del controllo totale sul confine statale da parte delle Autorità ucraine su tutte le zone del conflitto una volta realizzata la riforma costituzionale in Ucraina che contempli il riconoscimento di uno *status* speciale delle aree controllate dai separatisti.

L'attuazione dell'intesa – che ha consentito di avviare il ritiro degli armamenti pesanti dalla linea di contatto – è proseguita tuttavia con lentezza ed è stata scandita da periodiche violazioni della tregua.

Sul piano politico, il principale nodo irrisolto del processo negoziale attiene al livello di decentramento da riconoscere alle province secessioniste del Donbass. Sul punto, le posizioni tra le parti rimangono distanti: Kiev intende conferire allo *status* di autonomia delle regioni orientali una valenza prettamente amministrativa e comunque limitata nel tempo, mentre le componenti separatiste puntano ad una più marcata emancipazione.

crescente di attacchi *cyber*, il cui vantaggio in termini di rapporto costo-efficacia è di gran lunga superiore rispetto all'impiego di tecniche tradizionali di sabotaggio.

Inoltre, la natura degli attacchi informatici sembra essere sempre più complessa poiché mira ad accedere da remoto ai sistemi di gestione e controllo delle infrastrutture *target*. Un esempio, in tal senso, è il *malware* denominato *Energetic Bear*, che ha colpito più di mille aziende statunitensi ed europee attive in campo energetico con la finalità di compromettere il corretto funzionamento di centrali elettriche, gas *network* e turbine eoliche attraverso l'intrusione nei rispettivi *ICS (Industrial Control System)* tramite modalità di *remote access tool*.

Economie illegali e zone grigie. Evasione ed elusione fiscale

L'attività intelligence è stata orientata, in continuità con gli anni scorsi, anche all'individuazione delle patologie sistemiche che incidono direttamente sull'efficienza e sulla stabilità del sistema economico.

Sul versante del contrasto alle posizioni *off-shore* e ai paradisi fiscali, l'impegno informativo è stato rivolto ai rischi legati a tecniche societarie di pianificazione fiscale aggressiva, quali il trasferimento di profitti in Paesi a fiscalità privilegiata (*profit shifting*) o lo sfruttamento "improprio" delle disomogeneità tra i sistemi fiscali volto a ricercare situazioni di doppia mancata imposizione, quando non occasioni di frode (*reverse charge*). Tale attività si è inserita in un più ampio quadro di intervento istituzionale volto ad agevolare tanto l'emersione di capitali illeciti, quanto la cooperazione amministrativa tra Paesi per lo scambio automatico di informazioni.

Il dato saliente rilevato dalla ricerca informativa è quello di un'estensione del novero di espedienti e pratiche per l'esportazione illecita, l'occultamento o il reinvestimento – in territorio estero e non solo – di risorse derivanti da reati comuni o comunque sottratte all'erario: dalla compravendita immobiliare alla sottoscrizione di fondi d'investimento attraverso fiduciarie estere, dalla stipula di particolari polizze assicurative all'impiego di veicoli societari esteri, dall'emissione di fatture per operazioni inesistenti sino al sistematico utilizzo di strumenti di pagamento non tracciabili in Italia, in particolare di carte di credito emesse da società estere, con *plafond* mensili anche elevati, alimentate attraverso trasferimenti di somme da conti esteri ovvero tramite contante consegnato in Italia.

Sul terreno delle condotte fraudolente, sono inoltre emersi all'attenzione del Comparto:

- trasferimenti all'estero, in Europa e in Africa, di società nazionali fortemente indebitate nei confronti di fornitori e dell'erario;
- forme di abusivismo finanziario e truffe collegabili all'emissione di polizze fideiussorie (ad es. per rimborsi IVA) e di lettere di garanzia da parte di società prive di autorizzazione;
- frodi fiscali realizzate nel settore del

commercio internazionale di servizi telefonici e del commercio *on-line* di prodotti elettronici.

Si tratta di un contesto nel quale i diversi fenomeni illeciti, quali l'evasione fiscale, il riciclaggio e le frodi economico-finanziarie, condividono talora strumenti e schemi operativi. Significativa, in proposito, è la rilevata offerta di servizi a supporto di attività evasive, nel cui ambito si segnalano: la "esterovestizione" di imprese nazionali; la costituzione di false società all'estero attraverso le quali effettuare fittizie operazioni di triangolazione; la gestione di pagamenti estero su estero.

Aspetto critico ha assunto, poi, il cd. sistema delle cauzioni utilizzato per l'espletamento di gare pubbliche e per l'esecuzione degli appalti. Si è registrata, infatti, una proliferazione di fideiussioni "tossiche", prevalentemente imputabili a compagini assicurative e intermediari finanziari esteri, privi dei prescritti requisiti di solvibilità e onorabilità, cui hanno fatto ricorso società aggiudicatarie di appalti pubblici, con potenziali rischi per le casse erariali in caso di escussione dei premi per eventuali inadempimenti contrattuali.

Nelle pieghe delle zone grigie dell'economia hanno trovato spazio, infine, fenomeni di criminalità resi ancora più insidiosi e sfuggenti dal loro svilupparsi nello spazio cibernetico (*vds. box n. 17*).

La criminalità organizzata nel tessuto economico-produttivo nazionale. Mafie nostrane e fenomeni corruttivi

I perduranti effetti della crisi degli anni scorsi hanno continuato a condizionare le dinamiche competitive economico-finanziarie e sociali, lasciando spazi di agibilità alle organizzazioni criminali. In particolare, le restrizioni al credito ed il rallentamento degli investimenti, che nel passato recente hanno

box 17

LE FRODI E IL "PIZZO" NEL CYBERSPAZIO

Sul piano criminale si rilevano acquisizioni fraudolente di credenziali bancarie, dati di pagamento e di identità utili a ottenere un rapido profitto da riciclare in ulteriori attività illegali o nei contesti criminali. Particolarmente attivi risultano i gruppi di origine nigeriana che, in via autonoma o in modulo transnazionale, hanno ottenuto un elevato grado di specializzazione in attività illecite condotte prevalentemente in modalità *phishing*.

In tema di estorsioni telematiche ha continuato a registrarsi, invece, la diffusione dei *ransomware*, particolari *malware* che, una volta attivati sul *target*, cifrano i dati presenti nella postazione di lavoro e impongono il pagamento di una somma di danaro sotto forma di moneta elettronica di tipo *bitcoin* (*vds. box n. 14*), anonima e non tracciabile.

esposto la piccola e media impresa all'infiltrazione dei circuiti mafiosi, hanno consolidato la presenza nel sistema economico-produttivo del Paese di quei *clan* che hanno saputo sfruttare, grazie a un collaudato circuito relazionale crimino-affaristico, le criticità innescate dal *credit crunch*.

Le modalità di aggressione alle realtà imprenditoriali sane sono state finalizzate, come nel caso dei prestiti usurari e della partecipazione al capitale sociale, alla progressiva acquisizione delle aziende. Al contempo, i sodalizi criminali hanno dimostrato, rispetto al passato, una maggiore propensione al "mascheramento", grazie ad artifici societari, intestazioni fittizie e delocalizzazione del controllo aziendale in *trust* e società anonime *off-shore*. In tal senso la criminalità organizzata, soprattutto quella di matrice nazionale (*vds. box n. 18*), ha colto l'occasione per proporsi quale *player* di riferimento in numerosi settori dell'economia legale.

In qualche caso, si è assistito a una sorta di "contaminazione comportamentale" che porta soggetti non mafiosi, posti in condizione di gestire "quota parte" del potere pubblico, ad agire di concerto con gli stessi sodalizi criminali.

Tale cambiamento si osserva soprattutto intorno ai centri di spesa, laddove si aggregano o si scontrano *lobby* affaristiche trasversali che perseguono interessi personalistici, spesso in danno di una corretta gestione della cosa pubblica.

L'attività di intelligence si è focalizzata, in particolare, sui seguenti ambiti:

- gli **appalti pubblici**, specie con riguardo alle relazioni, strumentali agli interessi criminali, tra attori mafiosi e contesti amministrativi pubblici. Una mirata azione è stata finalizzata a verificare il grado di vulnerabilità dei contesti socio-economici e amministrativi di alcune Regioni, soprattutto con riferimento ai profili di alterazione dei processi decisionali della Pubblica Amministrazione, funzionali all'acquisizione e alla gestione illegale di risorse pubbliche. Inoltre, è emerso, nel comparto delle grandi opere, l'uso strumentale per finalità illecite del "consorzio" quale modello societario privilegiato d'ingerenza crimino-affaristica;
- il **gioco legale**, attraverso una serie di iniziative volte a tutelarne la dimensione pubblica, anche rispetto alle specifiche cointeressenze mafiose nel settore e a garanzia degli interessi erariali. Attenzione specifica è stata rivolta tanto a quello praticato nei casinò quanto a quello *on-line*, inclusa la localizzazione fisica delle infrastrutture informatiche poste alla base delle scommesse illegali;
- lo **smaltimento dei rifiuti** e le **bonifiche ambientali**, che possono rappresentare opportunità di guadagno per le organizzazioni mafiose con riflessi sulle economie locali e, soprattutto, rischi per la salute pubblica (valga su tutti il caso della "Terra dei Fuochi").

Di specifico rilievo, nel contesto descritto, le dinamiche di infiltrazione nella Pubblica Amministrazione.

box 18

MAFIE NAZIONALI: DINAMICHE ASSOCIATIVE

Nell'ambito di Cosa Nostra, alla necessità di nuovi assetti interni, seguita all'incisiva azione di contrasto, ha corrisposto l'avvicendamento ai vertici di talune importanti famiglie, pur rimanendo centrale, nella definizione delle strategie dell'organizzazione, il ruolo del carcerario. Sul piano operativo, quale conseguenza della crisi economica, oltre al ritorno ad attività criminali più "tradizionali" (narcotraffico, gioco illegale, contrabbando anche di prodotti petroliferi), si è evidenziata una continuità nei tentativi di ingerenza/infiltrazione nei processi decisionali.

La 'ndrangheta conferma le sue peculiarità rispetto alle altre organizzazioni criminali mafiose nazionali. La flessibilità della struttura di tipo orizzontale, a base familiare, legata alla tradizione ma pronta all'aderenza ai più diversificati contesti, ha consentito alla criminalità organizzata calabrese di trasformarsi, nelle sue forme più evolute, in una dinamica e spregiudicata *holding* economico-finanziaria. Tale strutturazione rende la 'ndrangheta meno vulnerabile all'azione di contrasto rispetto alle organizzazioni di tipo verticistico e le assicura anche spiccate capacità di ingerenza politico-amministrativa.

Per quanto concerne i *clan* di camorra, si ripropone la dicotomia tra le modalità gangsteristiche e predatorie adottate dai gruppi criminali attivi nel capoluogo campano, e le forme manipolatorie proprie della criminalità camorristica dotata di profilo imprenditoriale, maggiormente presente nell'*hinterland* partenopeo settentrionale, nel nolano e nel casertano. Anche la minaccia che ne deriva si mantiene bipartita. Il depotenziamento dei *clan* storici napoletani e l'ormai cronico *deficit* di *leadership* hanno fatto proliferare bande e microgruppi guidati da giovani privi di profilo strategico, tesi all'accaparramento delle piazze illecite, con modalità che destano vivo allarme sociale per l'efferata violenza. La camorra della provincia persegue un più sistematico controllo territoriale che favorisce la saldatura di interessi criminali con quelli affaristici diffusamente illegali.

La c.o. pugliese, caratterizzata in tutte le sue forme da diverse gradazioni di eclettismo e adattabilità ai contesti socio-economici, continua ad esprimersi in modo differenziato a livello provinciale, riproponendo le diversità strutturali tra i *clan* salentini e quelli foggiani e baresi. I primi riescono a bilanciare le conflittualità interne allo scopo di intensificare gli inserimenti nel tessuto affaristico-imprenditoriale locale. I secondi, penalizzati dalla loro polverizzazione e instabilità, risultano coinvolti in pratiche intimidatorie, conflittualità interclaniche e progettualità infiltrative di minor spessore.

L'imprenditoria mafiosa, grazie alla consolidata capacità di condizionamento intimidatorio e collusivo, è riuscita con crescente frequenza a disporre di informazioni sensibili sulle scelte pubbliche di investimento o a condizionare i processi decisionali politico-amministrativi. Si è dunque delineato un sistema parassitario-clientelare, espressione di un blocco affaristico in cui convergono interessi politici, imprenditoriali e criminali, che registra il protagonismo di figure "cerniera" in grado di favorire le istanze delle cosche.

Le mafie d'importazione

Con riferimento alla criminalità organizzata transnazionale, il contributo dell'intelligence, in un ambito di costante coordinamento interistituzionale, è valso a supportare l'individuazione delle principali dinamiche economiche e finanziarie connesse alle attività delle *holding* malavitose, contribuendo tra l'altro, sul versante estero, alla localizzazione di alcuni soggetti di elevato spessore.

Nella geografia dei traffici illeciti che si dispiegano nell'area mediterranea, specifico rilievo ha assunto il traffico di sostanze stupefacenti provenienti dal Nord Africa, condotto anche secondo logiche di sinergia operativa tra diverse organizzazioni transnazionali. Il fenomeno ha evidenziato proporzioni crescenti non solo nei volumi della produzione, ma anche nel novero dei Paesi utilizzati come centri di smistamento e transito. Il quadro informativo ha mostrato, in particolare, elementi di novità rispetto alle consolidate dinamiche del traffico internazionale di *hashish*, che hanno visto un reindirizzamento verso la Libia delle rotte del narcotraffico – tradizionalmente sviluppate lungo le direttrici del Mediterraneo occidentale – e un numero significativo di consorterie criminali dedicarsi contemporaneamente anche alla gestione dei flussi di migranti clandestini in direzione dell'Italia e dell'Europa.

Le organizzazioni criminali transnazionali presentano dispositivi ben articolati e strutturati, nell'ambito dei quali emergono ruoli definiti per i diversi soggetti coinvolti, a loro volta operanti anche nelle maggiori piazze finanziarie.

I circuiti criminali stranieri attivi sul territorio nazionale stanno parimenti tentando di infiltrare gli organi rappresentativi delle comunità etniche di riferimento, a detrimento dei processi di integrazione.

Tra le realtà criminali estere più attive nel nostro Paese si confermano:

- i *clan* cinesi, che tendono a espandersi su tutto il territorio nazionale, anche in quelle regioni del Meridione ove le comunità sono di più recente insediamento, sfruttando la generalizzata crisi di liquidità per effettuare vantaggiose acquisizioni immobiliari o commerciali, anche a fini di riciclaggio dei proventi illeciti. Nelle aree di più radicata presenza, si stanno invece affermando come *lobby* affaristica, dotata di un elevato livello di istruzione e di una rilevante propensione ai traffici internazionali;
- i sodalizi nigeriani, la cui diffusione appare sostenuta dal considerevole afflusso nel nostro territorio di immigrati provenienti dal Paese africano che mostrano un "competitivo" portato criminogeno, tale da agevolarne l'inserimento nei circuiti illegali internazionali;
- le reti esteuropee e caucasiche, tra le quali quella georgiana rappresenta una delle minacce criminali più "mature", risultando dotata di una efficiente struttura di tipo mafioso, in

grado di pianificare strategie operative, aggregare risorse economiche ed esercitare una energica sorveglianza sulle diaspore di connazionali. Anche il *network* romeno ha acquisito una sua specifica "visibilità" nello scenario nazionale, sino a rappresentare una delle componenti criminali più diffuse, che si contraddistingue per l'efferatezza delle azioni delittuose. La criminalità romena si è peraltro progressivamente affrancata dall'iniziale posizione gregaria rispetto ad altri gruppi per acquisire un suo livello di autonomia, coniugato con l'attitudine a tessere rapporti di collaborazione con altre compagini, anche autoctone, funzionali alla condivisione delle opportunità offerte dai mercati illegali.

Il caporalato

Piuttosto trasversale, quanto agli attori coinvolti, appare il fenomeno dello sfruttamento della manodopera straniera, per lo più nel settore del lavoro stagionale. Nella prospettiva intelligence, gli approfondimenti svolti hanno fatto emergere non solo illeciti profitti a beneficio dei "caporali", talora della medesima matrice etnica dei braccianti, ma anche forme di intimidazione con modalità mafiosa. In qualche caso, si è registrato il coinvolgimento di circuiti criminali italiani per la gestione dei lavoratori nelle aree di volta in volta più remunerative, con pesanti conseguenze sui processi di integrazione e di convivenza, specie nei contesti ove la periodica concentrazione di migranti può degenerare in episodi criminogeni o violenti.

LE STRUMENTALIZZAZIONI DEL DISAGIO

LE STRUMENTALIZZAZIONI DEL DISAGIO

La lettura dei fermenti antagonisti e delle dinamiche proprie degli ambienti eversivi, specie di matrice anarco-insurrezionalista, ha continuato ad essere una delle attività prioritarie dell'intelligence.

La sinistra antagonista. Temi "forti" della protesta, convergenze e linee di frattura

Nei primi mesi dell'anno la campagna contro l'EXPO milanese ha monopolizzato l'impegno propagandistico e organizzativo delle diverse componenti del movimento antagonista che avevano individuato nel Primo Maggio (cd. *May Day*), giornata di apertura dell'Esposizione Universale, l'occasione propizia per recuperare l'auspicata unitarietà d'azione attorno alle questioni, di forte richiamo, dello *sfruttamento* del lavoro – e, più in generale, della *precarietà, abitativa* e *lavorativa* – nonché dell'impatto ambientale.

Come più volte verificatosi nel recente passato, tuttavia, il *fronte di lotta* si è presentato alla scadenza contestativa tutt'altro che compatto. Marcate divergenze contrapponevano, infatti, una componente maggioritaria, convinta della necessità di *colpire* solo gli obiettivi con un significato sociale e politico immediatamente riconducibile alle istanze della protesta, ad un'area più oltranzista, di prevalente impostazione anarco-autonoma, propensa invece a cercare lo scontro *indiscriminato*, indicato come *l'unico modo possibile per contrastare l'EXPO*.

La deriva violenta del *May Day*, che ha di fatto oscurato il messaggio politico dei No EXPO ed inasprito il dibattito interno al movimento, ha pregiudicato l'ulteriore sviluppo della mobilitazione contro l'evento milanese.

Di contro, dopo l'estate non sono mancati, da parte dei segmenti più vitali dell'antagonismo, tentativi di rilancio della **mobilitazione *anticrisi***, imperniati sui temi "caldi" dell'opposizione alle politiche governative, specie in materia di *wel-*

fare e lavoro, e sulle rivendicazioni in tema di *diritti*, ritenute in grado di generare consensi soprattutto tra le fasce sociali più esposte al disagio. Su tale versante, la **questione dell'emergenza abitativa** ha confermato la sua valenza come motore del conflitto sociale, grazie alle potenzialità da essa evidenziate in termini di aggregazione e coinvolgimento popolare. Con specifico riferimento alla contestata attuazione del cd. Piano Casa, particolare rilievo ha assunto il progetto di innalzare il livello rivendicativo nei confronti dell'Esecutivo, tornando a occupare, produrre *riappropriazione* e stringere legami sociali per collegare le lotte nei territori. In questo quadro si colloca la settimana di *conflittualità diffusa* (10-16 ottobre) considerata, nelle intenzioni del movimento, una prima e significativa tappa della *campagna sulla povertà* finalizzata a dare sfogo alla volontà di *entrare in azione* che proverrebbe dalle molteplici espressioni del disagio sociale.

Nel medesimo contesto si inserisce il tentativo del circuito di *lotta per la casa* di sfruttare, in chiave di propaganda antigovernativa, la risonanza mediatica offerta dalla celebrazione dell'Anno Santo straordinario. In particolare gli attivisti romani, con lo slogan "*Un Giubileo contro i poveri?*", hanno esortato ad intensificare le azioni di *resistenza* sul territorio, per contrastare l'incremento nella Capitale di sfratti, pignoramenti e sgomberi, asseritamente finalizzato a *ristabilire la legalità* in occasione dell'evento religioso. Significativa al riguardo la *settimana di mobilitazione per il diritto alla casa* (7-12 dicembre) promossa a livello nazionale con occupazioni di edifici dismessi, manifestazioni e presidi di protesta in diverse città.

Alcune componenti del movimento *anticrisi* hanno continuato a esprimere una pronunciata connotazione anti-UE che, nel tempo, ha favorito a livello internazionale il consolidamento di sinergie operative con omologhe formazioni europee, volte a condividere e uniformare metodi e strategie per elevare i toni della protesta contro le *politiche di rigore*, asseritamente imposte dalle istituzioni dell'Unione e considerate la principale fonte del disagio sociale.

La tre giorni di mobilitazione (15-17 ottobre) organizzata a Bruxelles (in occasione della riunione del Consiglio Europeo) dal *network Blockupy* per protestare contro le politiche di austerità e la gestione dell'immigrazione da parte della UE ha confermato il rilievo assunto dal sodalizio quale principale arena di confronto e di sviluppo della mobilitazione *anticrisi* nel contesto comunitario. Nel corso delle giornate di protesta, cui hanno partecipato anche esponenti dell'antagonismo nazionale, sono stati attuati presidi e blocchi stradali nonché una *manifestazione conclusiva* il 17 ottobre, che ha sancito la convergenza delle lotte transnazionali sulle rivendicazioni in tema di *welfare universale*, ritenute in grado di garantire *risposte concrete alla povertà dilagante*. Fra i temi all'attenzione anche il TTIP (*Transatlantic Trade and Investment Partnership*), accordo commerciale tra Eu-

ropa e Stati Uniti che è considerato, nell'ottica antagonista, una *minaccia al benessere sociale e alla sicurezza dei consumatori*. Nelle linee d'azione del *network* figura, altresì, la promozione di una giornata di sciopero sociale europeo, reputato strumento idoneo a *sabotare* il sistema capitalistico e a contrastare i *poteri forti* della UE.

Connessa all'antieuropeismo e suscettibile di un progressivo incremento in termini mobilitativi è la questione dell'immigrazione, al centro dei dibattiti e della pubblicistica d'area. Da più parti, all'interno del movimento, è stata sottolineata la necessità di intensificare la campagna di solidarietà ai migranti e di continuare, nel contempo, a contrastare, sulla base di una comune visione *antirazzista* e *antifascista*, l'operato delle compagini della destra estrema che mirano a cavalcare strumentalmente alcune situazioni di diffusa tensione sociale in chiave anti-immigrati.

Di marcata valenza antigovernativa si sono confermate, inoltre, le **proteste di stampo ambientalista** che, strutturalmente radicate e parcellizzate nei contesti locali, hanno trovato un obiettivo unificante di lotta nell'opposizione al provvedimento governativo cd. Sblocca Italia (d.l. 133/2014), stigmatizzato come norma atta a favorire *gli interessi speculativi delle lobby del petrolio e del cemento*, impedendo di fatto la partecipazione democratica dei cittadini ai processi decisionali che interessano i loro territori.

In questo contesto, la **mobilitazione No TAV in Val di Susa**, considerata emblema delle *lotte di resistenza popolare* contro le *imposizioni* dello Stato, è parsa attraversare una fase di minor vigore, dovuta soprattutto alle forti contrapposizioni sorte, già all'inizio dell'anno, tra le due anime del movimento sul diverso modo di intendere il *sabotaggio* quale forma di lotta: da un lato, i circuiti dell'Autonomia locale che ritengono il sabotaggio una pratica da circoscrivere al territorio della Val di Susa, luogo simbolo della protesta; dall'altro, gli attivisti anarchici che sostengono la validità di tale strumento di lotta anche al di fuori del contesto valligiano, in linea con il principio da tempo propagandato del *portare la valle in città*. Emblematico, al riguardo, che al sostanziale disimpegno degli anarchici in Val di Susa abbia corrisposto un sostenuto attivismo di tali componenti – segnatamente dell'insurrezionalismo *movimentista* – in altri ambiti territoriali interessati da linee di Alta Velocità ferroviaria, con una serie di azioni di vario spessore (tranciamento di cavi elettrici, attacchi incendiari, etc.).

La tematica della *repressione* ha continuato a rivestire rilievo centrale nelle linee d'azione del movimento, alla luce della stigmatizzata recrudescenza dell'attività investigativa nei confronti dei militanti No TAV, considerata un tentativo di *intimidazione* finalizzato a disarticolarne la protesta. L'attività, in tale quadro, è stata scandita da iniziative di sostegno agli attivisti e presidi di solidarietà, specie in concomitanza delle udienze giudiziarie.

In prospettiva, è prevedibile che il movimento valsusino tenti di riconquistare il proprio potenziale di contestazione, pro-

muovendo a tal fine manifestazioni in grado di richiamare la partecipazione popolare. Al contempo, è ipotizzabile che alle tradizionali manifestazioni in Valle continui ad affiancarsi il ricorso a prassi più insidiose, proprie delle componenti radicali e in special modo dell'area anarco-insurrezionalista, con l'attuazione di azioni dirette ed estemporanee nei confronti di obiettivi a vario titolo connessi alla realizzazione della linea TAV.

Sempre sul versante delle mobilitazioni di stampo ambientalista, è parsa in progressiva intensificazione la **campagna No TRIV**, che si oppone alle operazioni di trivellazione per la ricerca di petrolio e gas, e che vede coinvolte nella mobilitazione, accanto ad associazioni e comitati cittadini, frange dell'antagonismo locale.

Significativa, infine, la **ripresa dell'attivismo antimilitarista**, passato nel corso dell'anno da una dimensione prettamente propagandistica a quella "di piazza", con l'organizzazione di iniziative di protesta e manifestazioni dirette a contestare la presenza sul territorio nazionale di basi e insediamenti militari, specie statunitensi e della NATO, nonché lo svolgimento di esercitazioni militari, considerate funzionali allo sviluppo delle *politiche di guerra*. Si tratta di un ambito d'azione condiviso da varie componenti antagoniste, accomunate da una visione anti-capitalista, che intravedono nel crescente protagonismo *militarista* dell'Unione Europea – indicata come il *nuovo polo imperialista* al fianco di quello statunitense – e nel moltiplicarsi degli scenari di crisi a livello internazionale nuove possibilità d'intervento per il rilancio ad ampio raggio del *movimento contro la guerra*.

A fattor comune, rispetto alle varie mobilitazioni antagoniste, il **cyberspazio** si è confermato sempre più non solo ambito di propaganda e *networking*, ma anche potenziale terreno di lotta (*vds. box n. 19*).

L'eversione anarco-insurrezionalista

Nel corso dell'anno, i circuiti d'area più oltranzisti, specie quelli "affini" alla **FAI/FRI** *(Federazione Anarchica Informale/Fronte Rivoluzionario Internazionale)*, hanno proseguito l'impegno volto a promuovere, attraverso il bollettino *Croce Nera Anarchica*, la ripresa delle progettualità violente.

I cardini sui quali si impernia il rilancio dell'*anarchia d'azione*, che esclude tipologie di intervento connotate da un livello di attacco "troppo basso", rimangono la *solidarietà rivoluzionaria* verso i militanti detenuti, l'*azione diretta distruttiva* e la dimensione di lotta sovranazionale. In coerenza con tale visione, i temi trainanti si sono confermati quelli relativi al carcere e alla *repressione*, con particolare attenzione alle vicende giudiziarie e alle situazioni detentive dei *compagni* prigionieri, anche di altri Paesi. A quest'ultimo riguardo, nel quadro del dialogo tra formazioni omologhe, ampio spazio è stato riservato, nella propaganda d'area, ai detenuti della *Cospirazione delle Cellule di Fuoco* (CCF), il gruppo terroristico greco cui è riconosciuto il ruolo propulsivo svolto negli ultimi anni per l'internaziona-

box 19

LA SPONDA VIRTUALE DELLE CAMPAGNE ANTAGONISTE

Dal monitoraggio delle iniziative e degli assetti organizzativi delle cellule di attivismo digitale, che operano sia a livello nazionale che internazionale, la comunità di *Anonymous* si è confermata quale sigla privilegiata cui si riferiscono numerosi *hacker* per rivendicare attacchi informatici. Nel corso del 2015, a sviluppo di un *trend* già emerso, non sono mancate campagne "allineate" con l'agenda dell'area antagonista o del movimento libertario, con iniziative a supporto di proteste di carattere ambientalista, antimilitarista o contro la *repressione*.

In questa cornice rientrano i messaggi postati sul *web* con i quali *Anonymous* ha rivendicato attacchi, tra l'altro, contro il Ministero della Difesa (con la dichiarata sottrazione di numerosi *account* riferibili a *usurpatori e gendarmi*), la Polizia penitenziaria (con il trafugamento di dati personali dei *fautori di nequizie* nelle carceri nazionali) e l'EXPO 2015 (con il boicottaggio dei servizi di biglietteria *on-line*, allo scopo di unirsi alla *lotta degli oppressi e degli emarginati di tutto il mondo*, tra cui, in Italia, coloro *che lottano contro la TAV e il MUOS*).

lizzazione dell'anarchia insurrezionale. A conferma della centralità rivestita dalla formazione greca, si pongono:

- la riproposizione del *Progetto Fenice*, "piattaforma" offensiva a sostegno dei *rivoluzionari prigionieri*, inaugurata nel maggio 2013 in territorio ellenico e diffusasi successivamente in diversi continenti, nel cui ambito sono state rivendicate a nome della FAI/FRI alcune azioni incendiarie compiute nei primi mesi dell'anno nella Repubblica Ceca, in Grecia e in Cile;
- la campagna d'azione *Per un Dicembre Nero,* promossa da detenuti della medesima CCF greca per la ripresa dell'insurrezione anarchica *dentro e fuori le prigioni* (*vds. box n. 20*), nella quale si inquadra l'attentato, rivendicato a nome della sedicente *Cellula Anarchica Acca*, realizzato con un ordigno occultato in una pentola a pressione, esploso il 18 dicembre davanti al portone della Scuola di Polizia Giudiziaria Amministrativa Investigativa/POLGAI a Brescia.

Anche la **corrente insurrezionalista** *ortodossa*, che rispetto agli *informali* preferisce l'anonimato nella pratica di lotta, si è distinta per un rinnovato attivismo propagandistico. Da un lato, sono stati elaborati nuovi progetti editoriali e ristampati documenti degli anni passati, dall'altro, si è registrata la partecipazione a incontri d'area, a livello sia nazionale che internazionale, in

box 20

"PER UN DICEMBRE NERO"

Il 10 novembre è apparso sui principali siti d'area il documento intitolato *Per una nuova posizione di lotta dell'insurrezione anarchica. Per un dicembre nero*, a firma dei detenuti Nikos Romanos e Panagiotis Argirou, membri della CCF.

Nel testo si propone l'attuazione di una sorta di coordinamento anarchico informale, da sostenere attraverso azioni multiformi (dalla semplice occupazione all'azione dinamitarda), al fine di alimentare *proposte sovversive e strategie di conflitto*. Si chiede, altresì, di *onorare la memoria* del giovane attivista greco Alexandros Grigoropoulos, ucciso nel dicembre 2008 da un agente di Polizia e del militante cileno Sebastian "Angry" Oversluij, rimasto ucciso nel dicembre 2013, durante l'*espropriazione armata* di una banca. In adesione a tale campagna sono state compiute azioni in vari Paesi contro obiettivi per lo più riferibili all'anticapitalismo e alla lotta alla *repressione*. Un paio di interventi (in Spagna e in Grecia) sono stati dedicati, fra gli altri, ai detenuti italiani Nicola Gai e Alfredo Cospito, condannati per il ferimento a Genova, nel maggio 2012, dell'Amministratore Delegato dell'Ansaldo Nucleare.

In Italia, prima del citato attacco alla Scuola POLGAI di Brescia, l'appello *Per un Dicembre Nero* era stato prontamente raccolto con un comunicato diffuso sul *web* a firma *Anarchic* fuori dalle mura per un Dicembre Nero*.

occasione dei quali è stata ribadita tanto la distanza da forme di protesta di stampo meramente *sindacalista* e *rivendicativo*, quanto la necessità di non perdere di vista l'obiettivo principale dell'*abbattimento del potere*.

Nella prospettiva anti-autoritaria di contestazione ai Centri di Identificazione ed Espulsione (CIE) si collocano alcune azioni esplosive compiute nel corso dell'anno e verosimilmente inquadrabili nella campagna di lotta contro i CIE lanciata da circuiti dell'anarco-insurrezionalismo *movimentista* (quest'ultimo già sopra richiamato nel contesto delle attivazioni contro la TAV). Alla diffusione su siti d'area, in maggio, di un opuscolo contenente un elenco di aziende impegnate nella *macchina delle espulsioni* hanno significativamente corrisposto i plichi, contenenti congegni a basso potenziale e privi di rivendicazione, inviati a quattro ditte torinesi e intercettati nei centri di smistamento postale di Bologna (28 maggio) e Milano (15 giugno). Le aziende *target* risultano citate nella pubblicazione divulgata sul *web*, secondo la consueta tecnica anarco-insurrezionalista a connotazione fortemente intimidatoria, che prevede la pubblicazione di liste di "nemici" allo scopo di fornire una selezione di possibili *bersagli* nel segno dell'azione diretta e anonima.

Alla medesima campagna sembrano da ricondurre, inoltre, i plichi esplosivi pervenuti – e deflagrati – all'Ambasciata francese a Roma e ad una società marittima di Bari (12 agosto).

Nel solco del filone ostile alle *nocività* e alla tecnologia si colloca, infine, la ripresa degli attacchi ai danni di strutture di telecomunicazione, specie ripetitori telefonici, il più delle volte rivendicati – ma sempre in forma anonima – intrecciando tematiche ambientaliste e di lotta alla *repressione*, in solidarietà a militanti inquisiti.

In conclusione, permane elevata la minaccia rappresentata dai settori più determinati dell'anarchia insurrezionale, laddove gli obiettivi privilegiati di iniziative di carattere violento rimangono legati al comparto della *repressione* e ai settori militare, tecnologico e delle *nocività*. In prima fila nel novero dei possibili bersagli rimangono altresì i *poteri economico-finanziari*, i *media di regime* e le strutture/figure rappresentative di Stati stranieri e di istituzioni transnazionali, senza poter escludere il Vaticano e la Chiesa, anche in considerazione della vetrina rappresentata dal Giubileo straordinario.

L'estremismo marxista-leninista

Sul versante degli ambienti di **matrice brigatista** continuano ad essere presenti – sebbene in un orizzonte temporale di medio-lungo periodo – potenziali rischi di una ripresa del fenomeno eversivo, legati ad alcuni aspetti non del tutto ricostruiti dalle indagini sull'ultima stagione terroristica.

I circuiti di ispirazione marxista-leninista rivoluzionaria, per quanto ridotti, hanno mantenuto l'impegno, specie attraverso alcune iniziative editoriali, a preservare e tramandare la memoria delle organizzazioni *combattenti* degli anni '70-'80, con l'evidente intento di divulgare, soprattutto presso le nuove generazioni, un'esperienza ritenuta *esemplare* per i suoi contenuti *politici* dichiaratamente volti al radicale sovvertimento del sistema costituito. Tale attività propagandistica è pertanto funzionale al proselitismo e alla formazione di nuove leve, nonché a progetti, per ora velleitari, di ricostruzione e unificazione delle *forze rivoluzionarie* residue.

Ha continuato a cogliersi, poi, una certa influenza del cd. carcerario che, sebbene non generalizzata come negli scorsi decenni, ma ormai limitata all'iniziativa di un ristretto nucleo di detenuti *politici* storici, ha tentato di indirizzare sul piano ideologico l'impegno delle formazioni attive fuori dal carcere. In proposito, l'attenzione dei militanti è stata orientata sia verso il tradizionale mondo del lavoro (senza che tuttavia siano stati conseguiti risultati di rilievo in merito al tentativo di inserimento strumentale nelle vertenze in atto), sia verso le manifestazioni più significative della protesta sociale, con l'obiettivo di conferire loro una prospettiva politica che le porti a superare la dimensione meramente rivendicativa; inoltre, gli eventi internazionali e il fenomeno migratorio hanno sollecitato un rinnovato interesse per il complesso scenario estero, cui si è tentato di fornire una lettura *di classe* e *antimperialista*.

È rimasta centrale, altresì, la solidarietà militante ai *prigionieri rivoluzionari* che, sviluppata anche sul piano internazionale, ha continuato a registrare interventi propagandistici a sostegno delle formazioni armate tuttora attive, con specifico riferimento, per quanto riguarda l'Europa, alla situazione in Grecia.

Appare sempre possibile, infine, che elementi d'area pianifichino azioni dimostrative volte a fomentare un innalzamento della conflittualità sociale nonché a verificare eventuali adesioni a percorsi di lotta orientati alla *prospettiva rivoluzionaria*.

Le diverse anime della destra radicale

Il panorama della destra radicale si conferma frammentato, privo di un progetto politico condiviso e segnato da competizione interna.

Le principali espressioni d'area identitaria, alla costante ricerca di legittimazione politica, hanno focalizzato il proprio impegno mobilitativo sui temi più sentiti dai ceti sociali disagiati (occupazione, alloggi, sicurezza), sulla difesa dei valori tradizionali e sul contrasto agli indirizzi economici dell'Unione Europea e all'integrazione degli stranieri.

Su quest'ultimo fronte, settori dell'ultradestra hanno tentato di strumentalizzare il malcontento di fasce popolari per quella che è percepita come un'*invasione*, promuovendo campagne di protesta contro le politiche governative di accoglienza e di gestione dei **flussi migratori**, e dando spazio all'emergere di pulsioni anti-islamiche.

Sul **piano internazionale**, il comune orientamento "euroscettico" delle formazioni della destra radicale continentale ha favorito il consolidamento di piattaforme politiche di respiro europeo. Oltre che con omologhe compagini europee, risultano confermati i contatti con i circuiti ultranazionalisti russi, i quali individuano in Mosca il difensore ultimo delle radici e delle autentiche tradizioni europee, dunque il capofila dello schieramento anti-statunitense e anti-UE.

Entro questa cornice ideologica, marcatamente antimondialista e filo-russa, hanno continuato a svilupparsi anche le attività propagandistiche delle **componenti eurasiatiste** che, in particolare, hanno promosso iniziative a favore della popolazione siriana e filo-Assad, nonché, come altre componenti d'area, a sostegno della Federazione Russa nel contesto della crisi ucraina (*vds. box n. 21*).

L'attenzione dell'intelligence non ha mancato, inoltre, di considerare l'attivismo del movimento ***skinhead***, d'ispirazione neonazista, dedito prevalentemente alla promozione di eventi musicali utilizzati per autofinanziamento e per sostenere i militanti inquisiti, nonché protagonista di una ripresa dell'azione più propriamente "politica" in chiave anti-immigrazione.

Sul **territorio altoatesino** è stato rilevato il crescente interesse delle componenti *skinhead* germanofone locali a sviluppare collegamenti con omologhi circuiti pangermanici tedeschi, sulla base di istanze condivise di stampo antisemita e xenofobo.

box 21

VOLONTARI ITALIANI NELLA CRISI UCRAINA

Sin dal suo inizio la crisi ucraina ha suscitato particolare interesse negli ambienti della destra radicale. Rispetto ai primi e differenziati orientamenti mostrati dalle formazioni d'area – alcune si erano professate filo-Kiev, altre filo-Mosca, altre ancora né con l'una né con l'altra ma a favore dell'autodeterminazione del popolo ucraino – è stato poi rilevato un generale ricalibramento verso posizioni favorevoli alla Russia.

Tale attivismo propagandistico ha evidenziato, in qualche caso, punti di tangenza con il fenomeno della presenza in quel teatro di cittadini italiani impegnati, in veste di combattenti, in gruppi paramilitari sia filo-russi che ucraini. Il *web* si è dimostrato lo strumento che ha permesso il consolidamento e la ramificazione dei contatti internazionali anche in chiave mobilitativa.

Il coinvolgimento di volontari nel conflitto ha registrato peraltro una progressiva flessione: è emersa, tra l'altro, la volontà di alcuni connazionali autoarruolati di far rientro in Patria, in particolare a seguito dell'approvazione della nuova normativa in materia di *foreign fighters*, che punisce la partecipazione a conflitti all'estero nei ranghi di eserciti irregolari.

Ancorché sporadica, la mobilità di militanti della destra radicale impiegati in operazioni di guerra nell'arena ucraina può presentare rischi, specie se associata ad altri fattori sensibili (*expertise* nell'uso delle armi, fanatismo/esaltazione, abitudine alla violenza, disagio socio-psicologico) riscontrabili in analoghi casi di *reducismo* e di per sé in grado di esprimere criticità sul piano della sicurezza.

Il monitoraggio informativo ha riguardato anche le storiche componenti *avanguardiste* e altre frammentate realtà minori, impegnate in un tentativo di *riaggregazione delle forze*, nonché il tifo violento organizzato, specie i gruppi più marcatamente ideologizzati.

In generale, a conferma di un *trend* più volte evidenziatosi negli ultimi anni, l'aumento dei livelli di visibilità e di attivismo delle principali organizzazioni della destra radicale ha alimentato la spirale di contrapposizione con le compagini di estrema sinistra, concretizzatasi in episodi anche violenti. Il fenomeno appare destinato a reiterarsi, in ragione del sempre più frequente convergere dei due fronti, spesso attivi nei medesimi contesti urbani su tematiche di interesse comune (quali il disagio sociale e abitativo e l'immigrazione), pur con visioni spesso opposte.

SCENARI E TENDENZE: UNA SINTESI

SCENARI E TENDENZE: UNA SINTESI

L'attività svolta dall'intelligence nel 2015 e le relative "lezioni apprese" delineano un panorama della minaccia che impone un continuo affinamento dell'azione informativa a tutela dei cittadini e degli interessi nazionali, in Italia e all'estero, con specifico riguardo alla capacità di precoce allertamento sui fattori di rischio emergenti.

Si rileva in particolare un'intima connessione tra la dimensione territoriale e fenomenica della minaccia come pure tra dinamiche interne alle società e grandi crisi internazionali, nonché tra tecnologie trasformative e conflitti.

Emblematico il caso del terrorismo jihadista, filo rosso della presente Relazione, e probabilmente di quelle future, tale da condizionare inevitabilmente l'elaborazione delle opzioni di *policy* e le strategie di sicurezza.

Almeno nel medio termine, la parabola di DAESH come entità territoriale non coinciderà con quella della minaccia terroristica, giacché anche l'auspicata sconfitta militare del *Califfato* non ridimensionerà il pericolo di attivazioni terroristiche in territorio occidentale, che potranno anzi caricarsi di un'ulteriore valenza ritorsiva.

Nel contempo, l'intelligence continuerà ad assicurare il necessario supporto informativo allo sforzo corale inteso a privare DAESH della sua base territoriale, poiché la strisciante – ma tutt'altro che silenziosa – penetrazione nei diversi quadranti dell'Africa e dell'Asia innesca ulteriori spiralizzazioni, ponendo altrettante ipoteche in termini di stabilità e sicurezza.

Nelle sue proiezioni asimmetriche, la formazione terroristica, forte anche dei consistenti introiti di origine predatoria, attinge ad un bacino incredibilmente ampio di "soldati": qaidisti della prima ora, *foreign fighters* di varia provenienza appositamente disingaggiati dal campo siro-iracheno, epicentro dell'instabilità, neofiti reclutati tra

gli *homegrown* europei da altri combattenti occidentali su mandato della *leadership*, nonché estremisti solitari, disadattati o estraniati dall'ambiente di residenza, istigati ad agire in nome del *jihad*.

Ne deriva la possibilità che in Europa trovino spazio nuovi attacchi eclatanti sullo stile di quelli di Parigi, ma anche forme di coordinamento orizzontale tra micro-cellule, o azioni individuali sommariamente pianificate e per ciò stesso del tutto imprevedibili.

Rispetto a questo scenario, il modulo virtuoso del nostro sistema di prevenzione, imperniato sullo stretto e assiduo rapporto tra intelligence e Forze di polizia, deve necessariamente integrare un più ampio dispositivo che preveda tra l'altro: l'elaborazione di mirate strategie volte a disinnescare l'azione di propaganda e proselitismo di matrice radicale; il rafforzamento dello scambio informativo a livello internazionale, con lo sviluppo di *best practices* anche con riguardo al rischio di infiltrazioni terroristiche nelle filiere migratorie e all'utilizzo di documenti falsi o contraffatti; l'adozione di formule cooperative e condivise per neutralizzare i canali di finanziamento del terrorismo.

Per quel che concerne le aree di operatività e di insediamento delle milizie di DAESH, di *al Qaida* e delle rispettive emanazioni, l'intelligence dovrà misurarsi con realtà fortemente destabilizzate e con il rischio di pericolose degenerazioni alle porte dell'Europa o dove insistono significativi interessi nazionali.

Impegno prioritario, sul versante estero, sarà riservato all'Africa mediterranea a partire dalla Libia, a sostegno dell'articolato sforzo volto ad evitare che il Paese diventi avamposto e *safe haven* di formazioni terroristiche, nonchè fulcro dell'instabilità regionale sulla spinta del serrato confronto interjihadista nel Sahel. Un'assai elevata soglia di attenzione andrà parimenti mantenuta in relazione al possibile ridispiegamento di combattenti nordafricani dal teatro siro-iracheno.

Nell'Africa subsahariana, centri propulsivi della violenza jihadista saranno ancora *Boko Haram* in Nigeria, compagine resa più assertiva dalla dichiarata alleanza con DAESH, e *al Shabaab* nel Corno d'Africa, ove le dinamiche di competizione tra l'organizzazione somala, fedele al qaidismo, e le emergenti frange filo-DAESH potranno determinare nuovi picchi di violenza ed accelerazioni in chiave espansiva.

In Medio Oriente, la guerra alle forze del *Califfato* in Siria e in Iraq rappresenterà la sfida più importante, ma certo non la sola per gli scenari di sicurezza regionale e internazionale, tenuto conto, tra l'altro: della crisi siriana, sulla quale si confrontano antagonismi storici ed aspirazioni egemoniche che ne moltiplicano il potenziale destabilizzante sui Paesi dell'area; dello stallo nel Processo di Pace israelo-palestinese; della fragilità del contesto yemenita, dove i tentativi di rilancio del dialogo arabo-sciita si innestano in una cornice di sicurezza fortemente deteriorata dall'attivismo delle concorrenti formazioni jihadiste.

Ugualmente conclamato, nell'*Af-Pak*, il confronto tra DAESH, da un lato, e

Talebani e *al Qaida*, dall'altro, secondo un paradigma contrappositivo emerso, e destinato a consolidarsi, anche in altre aree dell'Asia centrale e sud-orientale, e che può trovare espressione in attacchi anti-occidentali finalizzati ad assicurare visibilità a questa o quella formazione.

L'interdipendenza, intesa quale portato essenziale della globalizzazione, trova la sua primaria espressione sul versante dell'economia, dove il concorso dell'intelligence a presidio del Sistema Paese è chiamato ad essere sempre più multidisciplinare, trasversale quanto agli ambiti di intervento e tempestivo sul piano sia dell'analisi che della raccolta informativa.

L'azione dei Servizi si dispiega, infatti, in un contesto per sua natura contraddistinto da equilibrio instabile, funzione di numerose variabili: l'evoluzione degli scenari esteri, specie per quel che concerne le economie avanzate ed emergenti, l'andamento dei mercati finanziari e dei corsi petroliferi, ma anche gli stessi sviluppi geopolitici; le dinamiche congiunturali interne, tenuto conto che la graduale ripresa economica va consolidata, a fronte di perduranti vulnerabilità sistemiche e deficit di competitività del tessuto produttivo nazionale.

In questa cornice, l'impegno informativo dovrà muoversi su più piani e direttrici. Si tratterà, in particolare, di: assicurare ogni supporto al processo di internazionalizzazione delle nostre imprese, minimizzandone i rischi e vigilando, secondo criteri di tutela del *know-how,* sulle operazioni acquisitive di attori esterni, anzitutto quelle indirizzate alla filiera della sicurezza nazionale; analizzare e cogliere con tempestività le criticità del sistema bancario e finanziario; contrastare le manovre di spionaggio digitale riconducibili a nostri *competitor*; garantire il necessario contributo conoscitivo alle politiche energetiche del Governo; combattere l'economia illegale e l'impresa mafiosa, operando in ambito di stretta cooperazione interistituzionale.

Alla congiuntura economica, e più in generale, alle pieghe del tessuto sociale si ricollegano le dinamiche dell'antagonismo politico oltranzista, che, da opposte visioni ideologiche, tenta di cavalcare strumentalmente il disagio per acquisire consenso e visibilità.

È ragionevole valutare che alcune linee di tendenza consolidatesi negli ultimi anni siano destinate a riproporsi. Così per l'antagonismo di sinistra, interessato a connettere le diverse istanze di lotta di livello locale, tuttavia alle prese con divisioni interne e con l'azione di frange violente che, pur minoritarie, finiscono per condizionare le mobilitazioni di maggior richiamo sui temi "forti" della protesta, dall'emergenza abitativa alle proteste di stampo ambientalista. Anche la destra radicale, alla costante ricerca di accreditamento politico, appare dal canto suo frammentata in gruppi di varia ispirazione, tra i quali non mancano frange di matrice neonazista e xenofoba. In coerenza con questi *trend,* sono prevedibili, inoltre, nuovi episodi di intolleranza e di conflittualità "di piazza" tra militanti ideologicamente contrapposti.

Per quel che concerne l'eversione interna, deve ritenersi tuttora elevata la minaccia di matrice anarco-insurrezionalista che, con o senza rivendicazioni, potrà far registrare nuove sortite contro obiettivi in vario modo associabili alle campagne, anche di respiro internazionale, proprie dell'area libertaria, specialmente in tema di lotta alla *repressione* e alle diverse forme di *dominio*, incluso quello *tecnologico*. Velleitari, o comunque di non immediata viabilità, appaiono invece i progetti di rilancio dell'ideologia brigatista, tuttora coltivati da ambienti ristretti impegnati sul piano propagandistico a preservare la memoria degli *anni di piombo*, anche nel tentativo di attualizzarne il messaggio.

Si rimanda, infine, all'apposito allegato quanto agli scenari evolutivi della minaccia cibernetica, che rappresenta, in prospettiva, una vera e propria "nuova frontiera" per l'intelligence e per le Amministrazioni che concorrono alla sicurezza nazionale.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

ai sensi dell'art. 38, co. 1 bis, legge 124/07

2015

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

ai sensi dell'art. 38, co. 1 bis, legge 124/07

Premessa

A due anni dal varo della strategia italiana in materia di sicurezza cibernetica, la conclusione del 2015 segna un passaggio rilevante per la verifica funzionale dell'architettura nazionale, venendo a scadenza l'attuazione biennale del complesso degli obiettivi contenuti nel piano di sviluppo e potenziamento degli assetti cibernetici del Paese.

Si tratta di una finestra temporale dalla quale scaturiscono molteplici implicazioni che trascendono gli esiti, pur rilevanti, del doveroso resoconto e che permettono di tracciare una prima radiografia del Sistema Paese nel dominio digitale, quale democrazia matura in grado di garantire diritti e funzionalità di servizi essenziali sulla rete, di competere pariteticamente con gli alleati più avanzati, come pure di cogliere e sviluppare le potenzialità economiche del mercato neutralizzando ogni possibile fattore di rischio per la nostra sicurezza.

La valenza molteplice di tale appuntamento ha pertanto indotto una profonda riconsiderazione del "taglio" del Documento di sicurezza nazionale, con il quale sono stati finora compendiati, in allegato alle precedenti due Relazioni annuali sulla politica di informazione, solo le attività ed i risultati conseguiti sul versante dello sviluppo dell'architettura nazionale *cyber*.

Di qui, a partire dalla presente edizione, un Documento che, nell'includere anche una sezione dedicata alla trattazione della specifica minaccia cibernetica, intende offrire un innovativo contributo informativo, ad ampio spettro, idoneo a far cogliere la complessiva opera svolta dalla intelligence nazionale nell'ambiente "emerso", in qualità di manutentore del Sistema Paese, e nei circuiti "sommersi", quale attore "non convenzionale" nella prevenzione della minaccia.

La sintesi funzionale di entrambe le dimensioni consente infatti di poter ottimizzare, grazie ad una avanzata capacità predittiva richiesta per fronteggiare una minaccia dalle spiccate connotazioni di fluidità ed ibridazione, il supporto della complessiva opera di affinamento architetturale, la sensibilizzazione dei circuiti pubblici, il partenariato pubblico-privato (PPP), la feconda "impollinazione" accademica.

Si tratta di capitoli nei quali si è andata inscrivendo la storia di questo primo biennio di implementazione architetturale e sui quali il Presidente del Consiglio dei Ministri, con apposita direttiva del 1° agosto, ha ritenuto di tornare allo scopo di rendere pienamente effettiva ed operativa l'architettura delineata nel 2013, sottolineando l'urgenza di una accelerazione dei processi connessi con i citati capitoli, da garantire mediante l'assunzione di coordinate iniziative interistituzionali, in grado di evitare inutili duplicazioni e dannose sovrapposizioni.

Il Comparto intelligence, in aggiunta alle iniziative architetturali, ha continuato a contrastare in modo sempre più mirato, con strumenti e modalità *core*, una minaccia che, anche nel 2015, ha presentato caratteristiche di elevata sofisticazione, strutturazione e persistenza, specie quando ha colpito *target* di rilevanza strategica per la sicurezza nazionale. Con riguardo ad alcuni attacchi in danno di questi ultimi, l'intelligence è stata chiamata a misurarsi con eventi complessi, che hanno comportato rilevanti sforzi per l'identificazione e l'analisi dei *malware* impiegati, per l'individuazione degli attori ostili (cui è correlata la questione "aperta" della cd. *attribution*) e per il ripristino dei sistemi coinvolti. È stato confermato, inoltre, il *trend* di crescita delle azioni digitali con finalità di sottrazione di informazioni sensibili da settori industria-

li strategici, che non ha mancato di riguardare anche alcune primarie Amministrazioni Pubbliche. Conferma ha ricevuto, inoltre, l'impiego su larga scala di tecniche di attacco da parte di gruppi sponsorizzati da entità statuali, spesso mutuate dall'*underground* criminale, con finalità di infiltrazione nei sistemi *target*, allo scopo di comprometterne le capacità ovvero di danneggiarne o disattivarne il funzionamento. Da ultimo, è stato registrato l'accesso ad analoghe tecniche di attacco da parte di organizzazioni terroristiche che, attraverso l'interazione con gruppi *cyber* criminali, hanno soddisfatto le proprie esigenze di approvvigionamento, alimentandone, nel contempo, la crescita del "*business*".

Potenziamento delle capacità cibernetiche nazionali

Nel promuovere lo sviluppo delle attività di taglio architetturale, il DIS ha operato essenzialmente attraverso due strumenti: il **Tavolo Tecnico *Cyber* (TTC)** ed il **Tavolo Tecnico Imprese (TTI)**. In tali sedi sono state dispiegate le attività, rispettivamente, di raccordo interistituzionale e di sviluppo del Partenariato Pubblico-Privato (PPP).

Il filone più impegnativo dell'agenda del TTC è stata la predisposizione delle attività dirette alla **verifica dell'attuazione del Piano Nazionale** relativamente all'intero biennio di validità dello stesso (2014-2015). Gli esiti della verifica svolta nel 2014, una volta integrati con quelli riferiti al 2015, consentiranno di misurare l'effettiva crescita degli assetti cibernetici nazionali, di individuare gli eventuali *gap* di natura strutturale e di definire, rispetto a questi ultimi, le più opportune linee di intervento. La verifica biennale costituirà, altresì, il punto di partenza di un ulteriore, articolato processo, destinato a ricalibrare i contenuti dello stesso Piano – quello valevole per il 2016-2017 – sulla base, da un lato, dell'esperienza matura-

ta dagli attori dell'architettura dall'entrata in vigore del "DPCM Monti"; dall'altro, della evoluzione del quadro normativo interessato, da ultimo, dalla Direttiva *cyber* della UE in tema di *Network and Information Security*.

Ulteriore linea dell'agenda del predetto Tavolo, ha riguardato il progetto per la realizzazione di una **connettività nazionale**, in grado di consentire uno scambio informativo compatibile con le rapide evoluzioni della materia cibernetica. La "*Rete Gestione Crisi Cyber*" – che ha visto operare, in fase di preliminare verifica tecnica, il Ministero della Difesa e, successivamente, tutti i componenti del TTC per l'individuazione delle rispettive esigenze tecnico-operative e per la definizione dei correlati oneri di spesa – ha come obiettivo quello di collegare gli snodi dell'architettura, consentendo la condivisione, tra gli stessi, anche di informazioni classificate.

Il TTC è stato, altresì, il luogo di scambio analitico sulla minaccia, che si è proposto di istituzionalizzare un processo di *lessons learned* allo scopo di mettere ciascuna Amministrazione in condizione di fronteggiare autonomamente tali eventi e di meglio orientare, all'interno delle stesse, lo sviluppo di *policy*, competenze e strumenti, a complemento delle soluzioni tecnologiche reperibili sul mercato.

In aggiunta a quanto sopra – allo scopo di ridurre le sovrapposizioni di iniziative in direzione degli **operatori privati** da parte delle Amministrazioni chiamate, a vario titolo, ad interloquire con gli stessi – sono stati moltiplicati gli sforzi per l'implementazione di una direzione coordinata di tali interventi. Con le medesime modalità, si è provveduto ad ampliare, poi, il novero dei soggetti che, in aggiunta a quelli critici e strategici, sono i naturali destinatari di mirate attività di sensibilizzazione, in quanto potenzialmente esposti al rischio di attacchi di portata sistemica. In tale ambito, particolare menzione merita la predisposizione, da parte dell'**Accademia** su mandato del TTC, del "*framework* nazionale di *cyber security*", presentato ufficialmente il 4 febbraio. Tale strumento, elaborato sulla base del *National Institute of Standards and Technology* statunitense, persegue un duplice obiettivo: per un verso, consentire agli operatori pubblici e privati di valutare in modo semplice le rispettive capacità cibernetiche ed effettuare, in caso di interventi a potenziamento delle stesse, adeguate

programmazioni; per l'altro, slegare la *cyber security* da una dimensione puramente tecnica, conferendo alle criticità derivanti dalla stessa il medesimo rilievo di ogni altro rischio aziendale, così da elevarne il profilo e consentirne la trattazione nell'ambito dei Consigli di amministrazione delle aziende ovvero dei Comitati direttivi degli organismi pubblici.

Passando all'ambito del partenariato con le imprese strategiche, nel cui novero si sono aggiunti due nuovi soggetti nel 2015, il profilo più significativo delle attività svolte in seno al TTI ha fatto perno sull'*information-sharing;* processo in virtù del quale l'intelligence alimenta il suo patrimonio informativo e le imprese convenzionate arricchiscono le rispettive *knowledge-base*, così da potenziare, alla luce anche di ormai imprescindibili vincoli di spesa, le proprie capacità di difesa in modo mirato rispetto al *trend* della minaccia.

Gli incontri con le imprese, a seconda del rango dei rispettivi interlocutori, sono stati di taglio strategico ovvero di tipo più tattico-operativo. Nel 2015, nel corso delle sessioni di *policy* rivolte ai vertici aziendali ed ai responsabili delle strutture di sicurezza, sono stati effettuati punti di situazione sullo stato della minaccia cibernetica in Italia, con un particolare *focus* sulle evoluzioni delle azioni digitali effettuate per finalità di spionaggio e di cyberterrorismo, nonché sulle vulnerabilità che caratterizzano gli *Industrial Control Systems.*

Nell'ambito delle sessioni di livello tecnico – allargate, oltre che ai *Security Manager*, anche ai responsabili della sicurezza ICT delle imprese – sono stati svolti approfondimenti su "casi di studio" e sono state condivise informazioni tecniche (cd. *Indicators of Compromise*). Sotto tale profilo, l'obiettivo è stato quello di consentire, in caso di rilevazione della minaccia, la sua rapida identificazione per impedirne l'ulteriore propagazione sia all'interno dei sistemi dei *target* convenzionati, sia nell'ambito di quelli di soggetti, pubblici e privati, che mantengono relazioni con gli stessi.

Molteplici sono stati, inoltre, gli incontri bilaterali, tenutisi nella maggior parte dei casi su richiesta dei singoli operatori, per la trattazione di specifiche tematiche ovvero di puntuali ipotesi di minaccia. Lo scambio tra il Comparto ed i privati si è avvalso della funzionalità di un apposito portale, che ha conosciuto, a partire dalla seconda metà del 2015, una

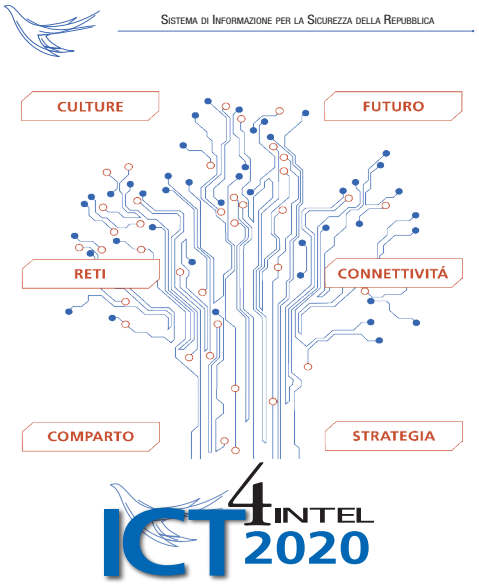
significativa implementazione tecnologica, destinata a rendere ancor più agevole, accrescendone i volumi, il richiamato *info-sharing*. Tra le principali innovazioni dell'applicativo – che sarà alimentato da dati sensibili – si evidenzia quella dell'impiego di strumenti di correlazione mirata e di analisi quantitativa per la valorizzazione del patrimonio informativo.

In ragione, poi, della **trasversalità delle tematiche** trattate, TTC e TTI hanno, in due circostanze, sviluppato iniziative congiunte. La prima, nel mese di marzo, in occasione della visita a Roma del *NATO Assistant Secretary General* per la Divisione *Emerging Security Challenges*, e la seconda, nel dicembre, per l'incontro con il Direttore Generale della *DG Connect* della Commissione Europea.

La riunione con il rappresentante della NATO, oltre a costituire utile occasione per l'illustrazione della *Enhanced Policy on Cyber Defence* dell'Alleanza, ha consentito agli attori privati di acquisire elementi sulla *NATO Industry Cyber Partnership*, quale modello di partenariato che mira, tra l'altro, ad agevolare l'innovazione e la conoscenza nell'ottica della creazione di soluzioni di *cyber* difesa interoperabili, cui hanno fatto richiesta di adesione, nel 2015, alcuni soggetti convenzionati.

L'incontro con il responsabile della *DG Connect*, invece, è stato incentrato sulla trattazione di due tematiche: la *Network and Information Security* (NIS), direttiva dell'Unione ratificata in dicembre dal Comitato dei Rappresentanti Permanenti della UE; la "*contractual Public-Private Partnership*" che include, tra i suoi princìpi fondanti, la creazione di un ecosistema ove rendere strutturale la cooperazione tra Accademia ed imprese.

Ulteriore iniziativa volta a consolidare il partenariato con gli attori convenzionati e, più in generale, con gli operatori dei settori industriali e di servizi con carattere strategico per la sicurezza nazionale, è stata l'**ICT 4INTEL 2020**, dedicata, nell'edizione 2015, al *cyber* secondo il paradigma rischi/opportunità. L'evento – che ha avuto luogo in novembre, presso la Scuola di formazione del Comparto – si è articolato in una prima sessione "chiusa" alla Comunità intelligence su temi di interesse strutturale (*agenda in tavola 1*) ed in una successiva giornata di lavori, dedicata alla *Partnership* Pubblico-Privato.



Obiettivo della seconda sessione, cui hanno partecipato anche rappresentanti di Università e Centri di ricerca, è stato quello di individuare rinnovate modalità di sinergia per meglio gestire le sfide e le opportunità connesse con il dominio cibernetico. L'ICT 4INTEL 2020 ha costituito, altresì, l'occasione per presentare ufficialmente il nuovo Polo Tecnologico quale "incubatore" di idee e soluzioni, nel cui ambito opera un "*Laboratorio Malware*" – primo esperimento di livello nazionale tra **Intelligence** (per l'individuazione delle esigenze operative), **Accademia** (per la capacità di ricerca avanzata) ed **Industria** (per la sperimentazione e la produzione di nuovi modelli tecnologici di difesa) – mirante a sviluppare una capacità in materia di *malware reverse engineering*, allo scopo di individuare metodologie di rilevazione, analisi e rimozione di codici malevoli.

tav. 1

TEMATICHE *WORKSHOP* ICT4INTEL

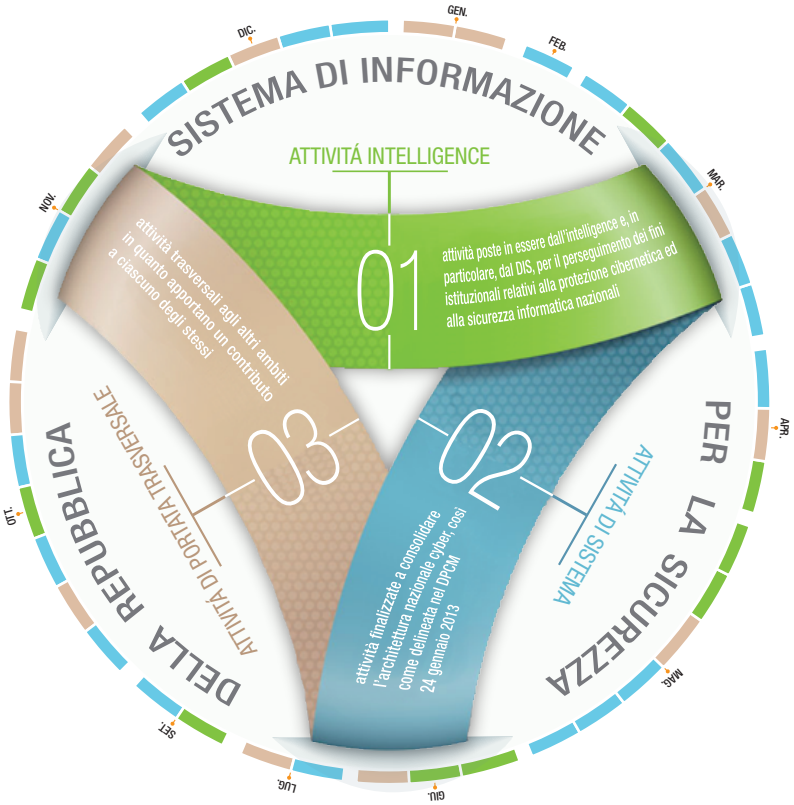
Tematiche dei *workshop* riservati al personale dell'intelligence:

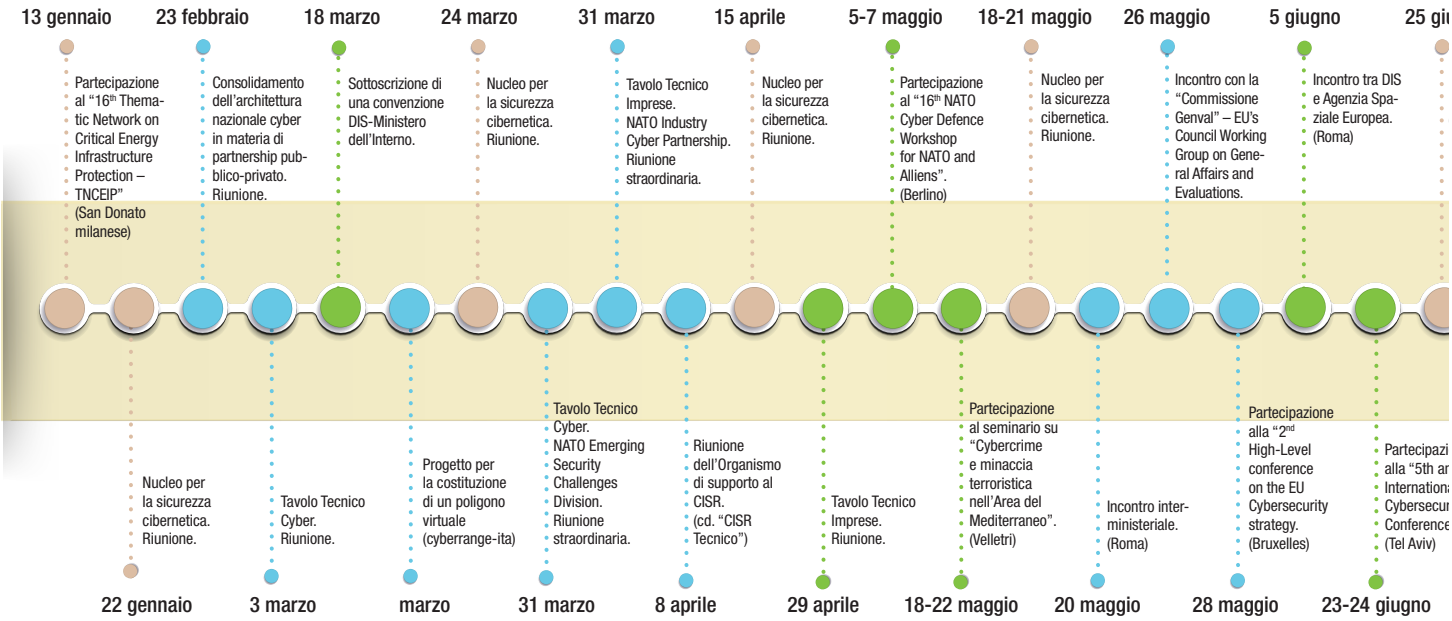
- la minaccia cibernetica: profili operativi e giuridico-legali;
- le caratteristiche dell'analisi e dell'analista *cyber*;
- il ruolo dell'OSINT nella prevenzione dei *cyber attacks*;
- la tecnologia quale "fattore abilitante" per la protezione cibernetica;
- il Centro di Eccellenza per la Ricerca *Cyber* Avanzata (CERCA) quale Polo Tecnologico di eccellenza nazionale;
- strumenti innovativi a supporto della protezione e confidenzialità delle informazioni.

QUADRO STRATEGICO NAZIONALE

Indirizzi strategici

1. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
2. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*
6. Rafforzamento della cooperazione internazionale





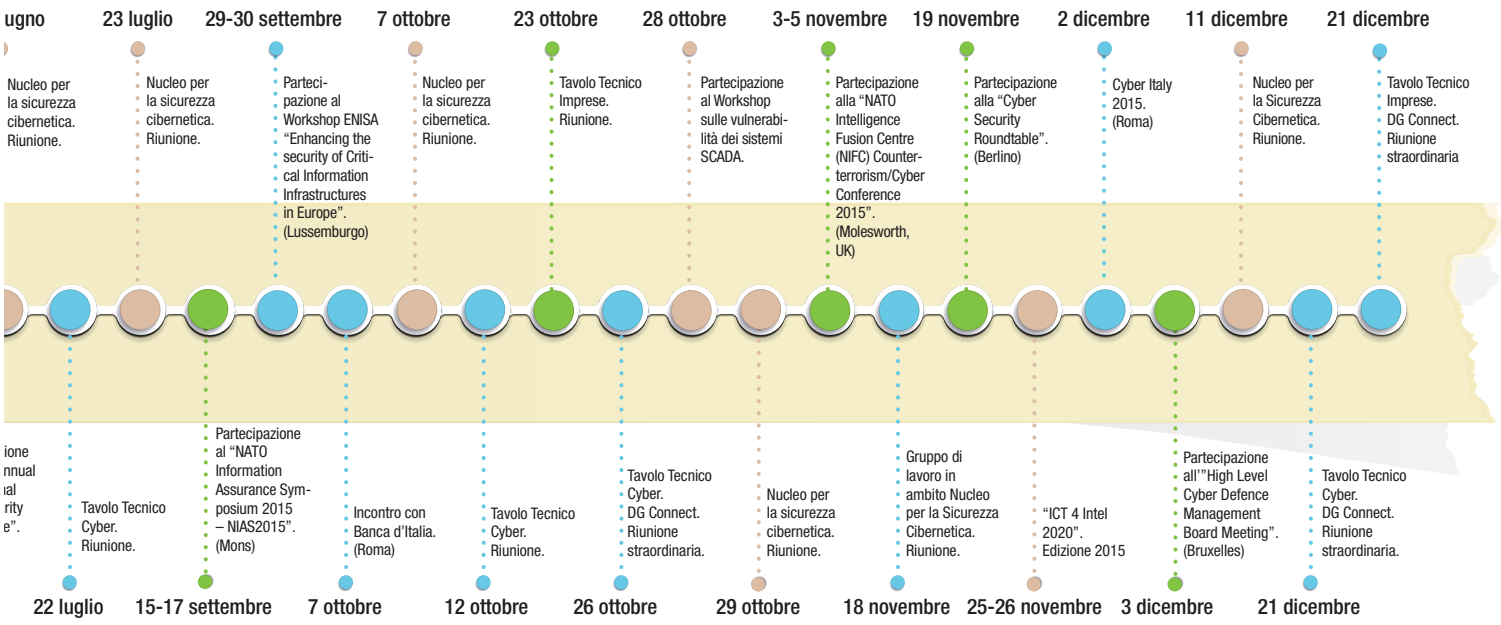
IL RUOLO DELL'INTELLIGENCE

NELLA PROTEZIONE CIBERNETICA E NELLA SICUREZZA INFORMATICA NAZIONALE

PIANO NAZIONALE

INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica
10. Risorse
11. Implementazione di un sistema di *Information Risk Management* nazionale



Stato della minaccia cibernetica in Italia

Nel corso del 2015 lo spazio cibernetico si è consolidato quale "terreno di conflittualità diffusa" confermando, ancora una volta, il divario difficilmente colmabile tra il rapido, costante ampliamento della superficie di attacco e la non altrettanto veloce capacità di garantirne una difesa efficace. In tale contesto, i repentini cambiamenti del mercato tecnologico, il costante incremento del livello di digitalizzazione delle informazioni e le indifferibili, quanto crescenti, necessità di nuove funzioni operative nell'ambito dell'informazione e dei relativi canali di comunicazione, cui sovente non ha corrisposto un adeguato potenziamento infrastrutturale degli *asset*, hanno continuato a determinare uno scenario estremamente dinamico, spesso aggravato da una persistente mancanza di conoscenza e sensibilità della minaccia. Rispetto a quest'ultima, pertanto, l'intelligence ha operato adottando un approccio olistico, basato sull'integrazione di risorse, processi e tecnologie ai fini di una più efficace attività di prevenzione, monitoraggio e risposta. In tale contesto, le strategie del Comparto hanno fatto perno:

- sull'*info-sharing* con tutti gli *stakeholder* nazionali, al fine di accrescere il patrimonio informativo attraverso la costante acquisizione di

elementi sulla minaccia, sul profilo dei suoi attori, sui *modus operandi* adottati, sui *target* d'interesse, sia attuali che potenziali, e sulla tipologia/portata dell'impatto;

- sul supporto nei confronti di soggetti di interesse strategico, volto ad orientarne le attività di *remediation*, favorendo altresì l'adozione di misure corrispondenti allo "stato dell'arte" della sicurezza cibernetica;
- su una più stretta cooperazione internazionale, nell'ambito di consessi sia multilaterali che bilaterali. In ragione di ciò, è stato possibile valutare le minacce in una cornice più ampia, comparando i diversi paradigmi comportamentali degli attori ostili ed analizzando le evidenze su vasta scala, al fine di circoscrivere le finalità delle campagne digitali d'interesse, così da meglio identificarne gli attori.

Nel corso del 2015 la **matrice statuale** ha continuato a caratterizzare le più significative attività di cyberspionaggio in danno di obiettivi nazionali di rilevanza strategica. Il *trend* registrato è stato quello di un incremento qualitativo e quantitativo delle azioni contro alcune Istituzioni e l'industria ad alto contenuto tecnologico ed innovativo, con l'obiettivo di esfiltrare informazioni sensibili e *know-how* pregiato, nonché di accedere ai rispettivi sistemi in vista di successive azioni di *disruption*.

Le principali caratteristiche di tale matrice sono state individuate ancora una volta nella scelta degli obiettivi – di norma *target* pubblici e privati operanti nei settori diplomatico, della difesa, dell'aerospazio, delle telecomunicazioni ed energetico – e nelle modalità di attacco impiegate, connotate, in alcuni casi, da una relativa semplicità attuativa, sebbene di estrema pervasività e persistenza, ed in altri, da sofisticate tecniche elusive e crittografiche e da una puntuale selezione dei *target*, nei cui confronti si è agito con intrusioni molto mirate. Il ***modus operandi*** ha continuato a tradursi in una minaccia persistente e avanzata – *Advanced Persistent Threat - APT* – con l'impiego di *software* malevolo (cd. *malware)* nelle reti informatiche dei soggetti selezionati, al fine di infettarne i relativi *computer*.

Inoltre, i "gruppi" operanti nell'ambito delle campagne APT hanno mostrato sempre più di:

- impiegare *malware* modulare, con componenti deputate allo svolgimento di specifiche funzioni e dispiegate o meno a seconda del *target*;
- reingegnerizzare i *malware*, innescando, tra l'altro, una proliferazione di tecnologie digitali facilmente reperibili nella Rete;
- fare ricorso – nella scrittura dei codici malevoli – a stringhe di caratteri in lingue diverse ovvero riconducibili ad altri attori ostili, al fine di rendere maggiormente difficoltosa ed incerta l'attribuzione di un attacco;
- sottrarre credenziali amministrative di *host* della *intranet* dell'obiettivo per preservare il controllo del sistema anche a fronte di attività di *remediation*;
- utilizzare *proxy* (individui o gruppi) nella conduzione degli attacchi, così da garantire agli attori ostili in *background* l'anonimato e la possibilità di negare ogni coinvolgimento (cd. *"plausible denial"*).

Tra gli elementi di novità, quello più significativo è stato l'affacciarsi, nel panorama dello spionaggio digitale, di gruppi *cyber*-criminali che sono riusciti ad impiegare *software* malevolo, appannaggio esclusivo in passato di attori statuali. Tali gruppi – dediti prevalentemente al furto di dati bancari e di carte di credito – hanno cominciato, grazie a più affinate capacità, a sottrarre informazioni pregiate, a collocare le stesse sul "mercato" ed ad offrire un vero e proprio servizio (il cd. *cyberespionage-as-a-service*) ad entità statuali ovvero a *competitor* commerciali. Da evidenziare, in tale contesto, come queste realtà abbiamo mostrato di possedere un *modus operandi* diverso, decisamente meno sofisticato rispetto a quello di attori statuali, caratterizzato prevalentemente dal riutilizzo di *software* malevolo compilato da altri, così da non dover sostenere i costi di sviluppo, e dalla mancanza di verticalizzazione dell'attività di *targeting*, avendo quale principale obiettivo quello di colpire quante più vittime possibili.

In linea di continuità con quanto osservato nel 2014, si è assistito al consolidamento di attività legate all'effettuazione di *due diligence* occulte

attraverso la sottrazione di dati di natura finanziaria – o relativi a piani di investimento e di politica industriale – nell'ottica di acquisizioni di pacchetti azionari di società italiane da parte di ***competitor* stranieri** ed alla veicolazione di minacce da parte di **soggetti** ed **aziende** operanti nel settore informatico e della sicurezza cibernetica.

Attenzione, infine, è stata dedicata all'evento che ha interessato i sistemi della *Hacking Team* – produttrice dello *spyware* "*Remote Control System Galileo*" – che ha determinato la compromissione dei sistemi informatici aziendali e sul quale sono ancora in corso accertamenti di natura tecnica e giudiziaria.

Il fenomeno dell'***hacktivism*** ha continuato a trovare nella comunità *Anonymous* il principale punto di riferimento sia come contesto organizzativo, sia come *brand* delle proprie azioni, ed a far registrare un ulteriore scostamento del movimento dalle originarie istanze rivendicative verso campagne di più marcata impronta antagonista e antigovernativa. Vanno ricondotte a tale ultimo ambito le offensive digitali, in danno di *target* istituzionali, che hanno tratto spunto da situazioni di tensione e di scontro sociale, tradottesi essenzialmente in attacchi *Distributed Denial of Service* (DDoS) contro siti *web* istituzionali e di esponenti della politica nazionale, in attività finalizzate alla ricerca di vulnerabilità delle infrastrutture *target* ed in azioni di disturbo digitale attraverso tecniche di *SQL Injection. Anonymous,* inoltre, in linea di continuità con il suo tradizionale approccio, non ha mancato di attivarsi a livello internazionale, in concomitanza con eventi e situazioni di particolare visibilità/interesse, dando vita, ad esempio, all'operazione *"ClimateMarch"*, in corrispondenza con il *summit* di Parigi sul clima, ovvero caricando sui *social media,* all'indomani degli attacchi parigini del 13 novembre, analogamente a quanto fatto dopo gli attentati del precedente gennaio, nella stessa Capitale francese, un video con il quale, oltre a dichiarare guerra a DAESH, ha dato avvio alla *"Operation Paris"* ed al conseguente oscuramento di risorse informatiche ritenute vicine a quella formazione jihadista.

Quanto ai **gruppi terroristici**, essi hanno continuato ad impiegare massicciamente i *social media* al fine di sfruttarne al meglio opportunità

e potenzialità. DAESH, in particolare, ha fatto costante uso della rete quale "moltiplicatore di forza" e "cassa di risonanza" per la diffusione e amplificazione dei suoi messaggi propagandistici. Frequente è stato il ricorso a:

- tecniche di manipolazione e "dirottamento" dei filoni di discussione sui *social network*, per veicolare la propaganda attraverso *hashtag* con elevata visibilità, sovente non correlati a tematiche relative all'Islam;
- specifiche applicazioni che, consentendo di ripubblicare sugli *account* dei loro utenti i *post* di DAESH, ne ha provocato di fatto un aumento esponenziale, con conseguente maggiore risonanza pubblica.

Sulla base del costante monitoraggio effettuato dall'intelligence, le capacità dei gruppi terroristici di porre in essere attacchi *cyber* non hanno raggiunto il livello analogo – per numero di vittime e rilevanza dei danni materiali – a quello di un'azione terroristica convenzionale. L'attivismo cibernetico sinora rilevato, in tale ambito, si è tradotto in attacchi il cui *modus operandi* ha fatto ricorso a tecniche di *web-defacement* e DDoS.

Sul fronte della **criminalità informatica**, è stata rilevata la crescente diffusione di *software* malevoli, riconducibili soprattutto alle tipologie *ransomware* e *banking trojan*, finalizzati entrambi all'illecito conseguimento di benefici di natura economica.

CryptoWall, *CryptoLocker* e *RansomWeb* sono tra i *ransomware* che hanno conosciuto, nel corso del 2015, una elevata propagazione, mentre con riguardo ai cd. *banking trojan*, le varianti maggiormente riscontrate sono state quelle afferibili a *Vawtrak* e *Dyre*, *software*, questi, programmati per acquisire le credenziali di accesso degli *account* dei siti di banca *on-line* al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di cybercriminali. In aggiunta, la minaccia di tipo avanzato e persistente denominata *"Carbanak"*, che consente il controllo da remoto di talune applicazioni per l'attivazione di sportelli bancomat, ha interessato i sistemi informatici anche di alcuni istituti bancari nazionali.

Serie statistiche

La minaccia sopra delineata è stata anche rappresentata, al fine di consentirne una lettura rapida ed agevole, nelle serie statistiche di seguito riportate, frutto di una attività di sistematizzazione ed analisi dei dati relativi ad eventi cibernetici rilevati, nel corso del 2015, principalmente da AISE ed AISI, ma anche da parte degli altri attori che compongono l'architettura nazionale, sia pubblici che privati.

Completa il quadro della minaccia il *ranking* frutto della comparazione delle serie statistiche del 2015 con quelle del 2014, al fine di tracciarne le tendenze, secondo la seguente legenda:

▲	▼	▶
Trend in crescita	*Trend* in diminuzione	*Trend* stabile

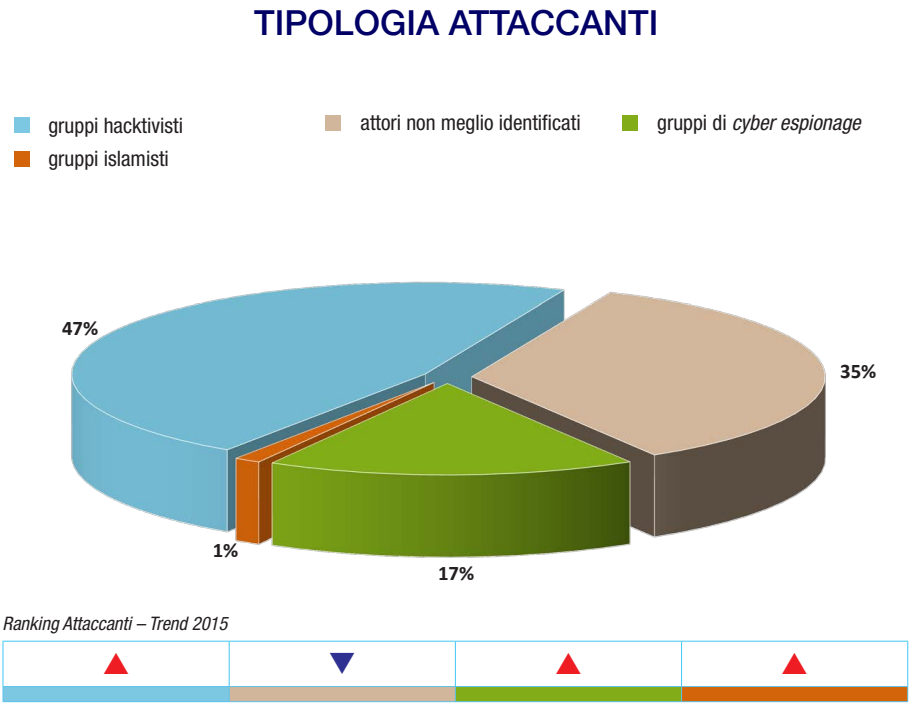


Grafico 1 – Tipologia attaccanti

Per quel che concerne la tipologia di **attori ostili**, così come mostrato nel ***Grafico 1***, questi sono raggruppabili in cinque categorie, di cui la principale – solo per percentuale di azioni svolte (47%) e non per grado di pericolosità – rimanda ai gruppi hacktivisti. Significativa è, anche, la quota di **attori non meglio identificati** (35%), che trova la sua ragion d'essere soprattutto nelle criticità poste dalla questione dell'*attribution*. Seguono, poi, **gruppi professionisti dello spionaggio digitale** (17%), nel quale, come più sopra indicato, sono coinvolti anche gruppi criminali, specializzatisi negli ultimi tempi nell'esfiltrazione di informazioni pregiate. Emergono, infine, i **gruppi *hacker* islamisti** (1%), con il ricorso a tecniche tipiche dell'*hacktivism*.

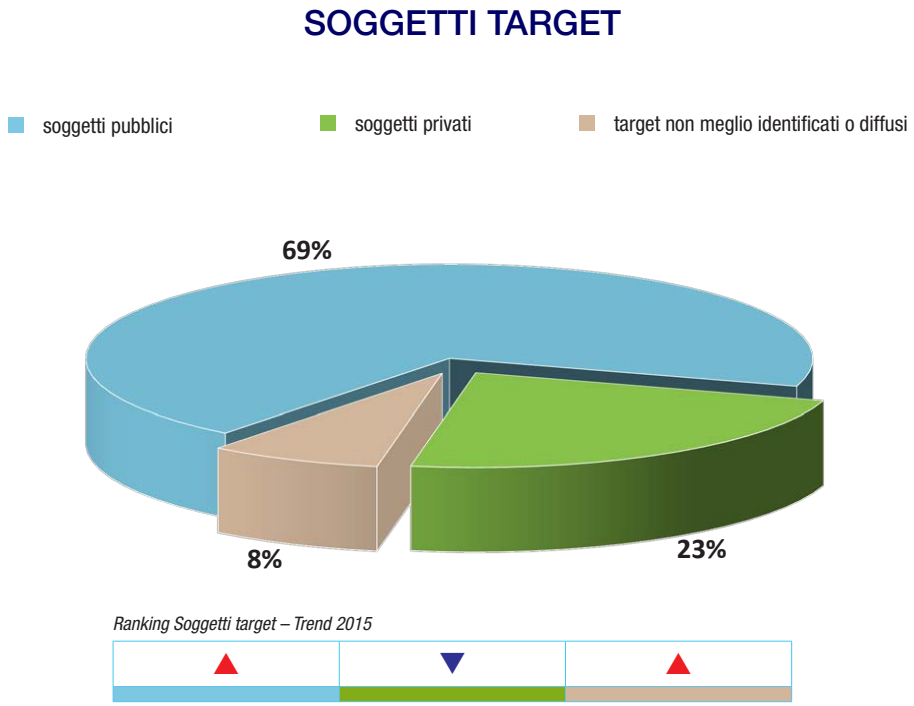


Grafico 2 – Tipologia dei soggetti target

Cambiando prospettiva, i dati sui **soggetti *target*** (***Grafico 2***) mostrano il divario tra gli attacchi perpetrati nei confronti di **soggetti pubblici**, che costituiscono la maggioranza con il 69%, e quelli in direzione di **soggetti privati**, attestati attorno al 23%. La rimanente aliquota, quella pari all'8%, è costituita generalmente da *"soft target"*, obiettivi non di rilievo strategico che presentano vulnerabilità comuni e, pertanto, semplici da sfruttare, verso i quali è di norma l'*hacktivism* a condurre attacchi.

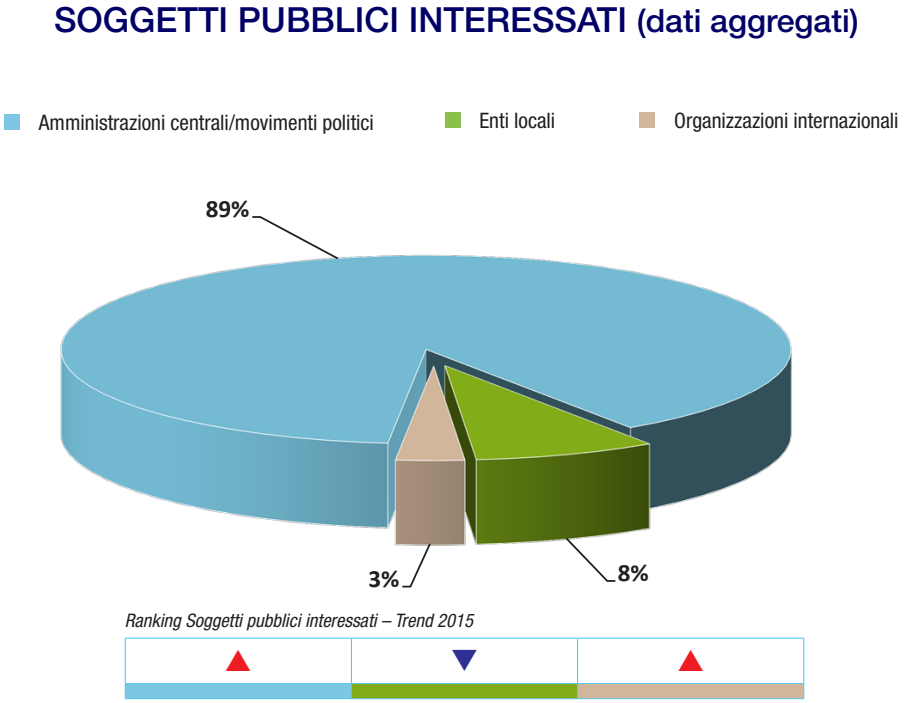


Grafico 3 – Tipologia dei soggetti pubblici interessati dagli attacchi (dati aggregati)

L'affinamento dei dati per categoria (pubblico-privato) fa emergere un maggior grado di dettaglio per quel che riguarda i **soggetti pubblici** (***Grafico 3***). La maggioranza degli Enti interessati da attacchi *cyber* sono risultate le **Pubbliche Amministrazioni Centrali** (89%), mentre quelli contro **Enti locali** hanno assunto una rilevanza pari all'8%. Le prime costituiscono *target* preferenziali per attività sia di spionaggio digitale, in quanto detentrici di informazioni pregiate sotto il profilo geo-politico e politico-strategico, sia di matrice *hacktivist*, poiché rappresentano obiettivi "simbolici", selezionati in ragione del particolare messaggio o rivendicazione da veicolare, nonché per la loro capacità di conferire agli attacchi elevata visibilità.

Da evidenziare il valore del tutto residuale (3%) delle attività ostili in danno di **Organizzazioni internazionali**, anch'esse oggetto, principalmente, di azioni dimostrative riconducibili al filone *hackivist*.

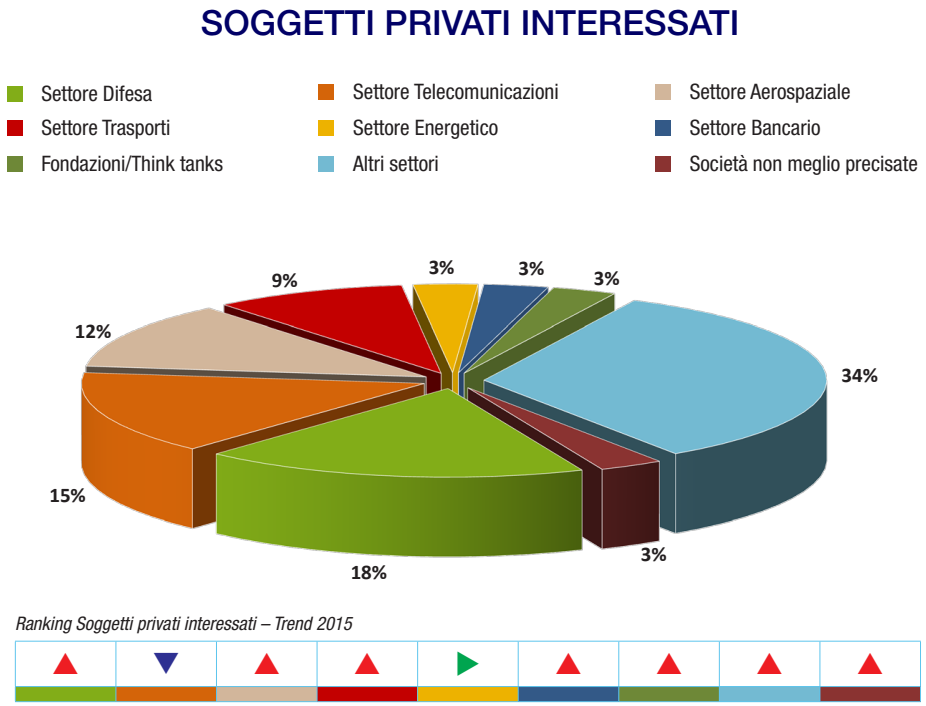


Grafico 4 – Tipologia dei soggetti privati interessati dagli attacchi

Sul fronte dei ***target* privati** (***Grafico 4***), gli obiettivi privilegiati per attacchi di spionaggio digitale sono quelli operanti nei settori della difesa (18%), delle telecomunicazioni (15%), dell'aerospazio (12%) e dell'energia, inclusa quella proveniente da fonti rinnovabili (3%). I restanti soggetti sono stati interessati da azioni di tipo *hacktivist*. Significativo, altresì, il 3% registrato nei confronti del settore bancario, verso cui sono stati impiegati i cd. *banking trojan*.

Sotto la voce "altri settori" (34%) sono state, poi, indicate tutte quelle realtà imprenditoriali – per lo più appartenenti alla categoria delle piccole e medie imprese – afferenti a molteplici classi merceologiche, i cui eventi cibernetici assumono rilevanza statistica solo se analizzati in formato aggregato. La voce "società non meglio precisate" (3%), infine, fa riferimento a quelle attività ostili condotte su larga scala contro le risorse esposte su internet di una moltitudine indiscriminata di *target*.

TIPOLOGIA DI ATTACCO

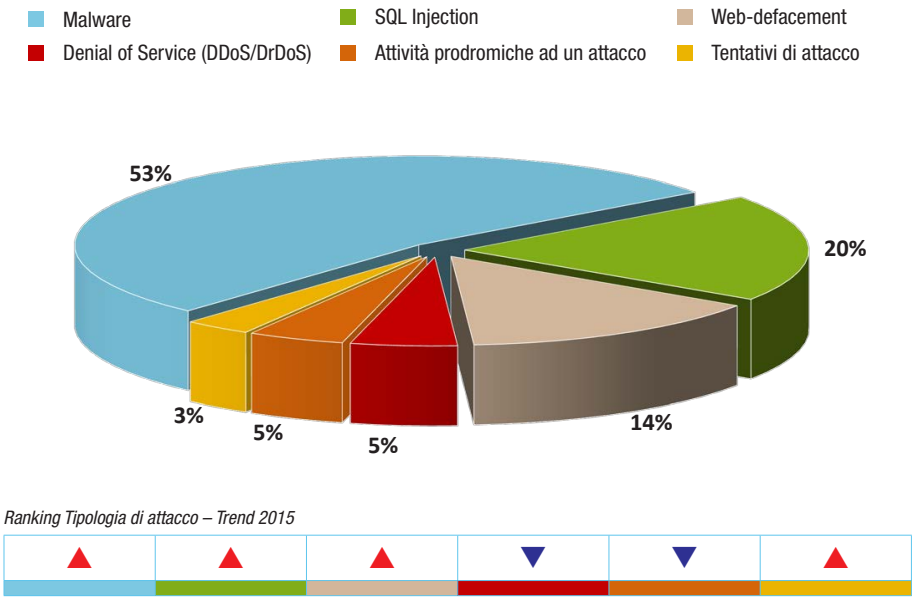


Grafico 5 – Tipologia di attacco impiegata

Con riguardo, infine, alle **tipologie di attacco** (***Grafico 5***), il 53% è costituito da *software* malevolo (*malware*), specie nella forma dell'*Advanced Persistent Threat* (APT), impiegato, come più sopra indicato, non solo per finalità di *cyber*-spionaggio, ma anche nell'ambito di logiche estorsive e di altre attività illecite di natura predatoria. Da rilevare, inoltre, il crescente ricorso a tale strumento da parte anche dei movimenti hacktivisti – oltre alla tecnica *SQL Injection* (20%) – per esfiltrare dati da riversare poi su internet. Altra modalità largamente utilizzata in tale ambito è quella del defacciamento di siti *web* (14%), mentre in calo risultano i *Distributed Denial of Service* (5%).

Valenza residuale hanno assunto le attività prodromiche ad un attacco (5%) quali, ad esempio, quelle di scansione delle vulnerabilità, di mappatura della rete del *target* e di *fingerprinting* dei sistemi, ed i tentativi di attacco (3%).

Trend evolutivi della minaccia cibernetica

Sulla base di quanto rappresentato, le evoluzioni della minaccia *cyber*, in un'ottica di breve-medio termine, continueranno a risentire, in particolare:

- delle vulnerabilità riconducibili al fattore umano, non solo per i profili collegabili alla figura dell'*insider*, ma anche per i *pattern* comportamentali *on-line*, sempre più profilabili attraverso l'impiego di tecniche avanzate di *social engineering*;
- dello sviluppo e della sempre maggiore diffusione di piattaforme per l'effettuazione di transazioni tramite dispositivi *mobile*;
- del continuo incremento della superficie di attacco, anche a seguito di politiche di riduzione del *digital divide*, della maggiore capillarità delle infrastrutture di comunicazione nelle Nazioni in via di sviluppo, nonché della crescente diffusione di dispositivi mobili e di domotica *smart* (*Internet of Things*);
- del potenziamento della digitalizzazione dei documenti e dei processi da parte sia della Pubblica Amministrazione che di società private, in grado di aumentare l'impatto di azioni ostili nel cyberspazio;

- della crescente capacità di offuscamento dei *malware*, idonei ad occultarsi nei livelli più profondi dei sistemi (*Basic Input Output System* e *firmware* di altre componenti dei sistemi informatici, *vds. tavola n. 2*) e delle reti *target*;
- dei *ransomware*, che vedranno evolvere i propri metodi di propagazione, di cifratura e di impiego più mirato;
- del potenziamento dei sistemi di comunicazione delle *botnet*, di cui esempio emblematico è l'utilizzo di connessioni satellitari per ridurre drasticamente la capacità di geo-localizzazione e la riconducibilità dei sistemi di comando e controllo utilizzati.

tav. 2

UNIFIED EXTENSIBLE FIRMWARE INTERFACE

Anche al fine di migliorare la sicurezza dei sistemi, impedendo attacchi di tipo *bootkit*, è stato sviluppato l'*Unified Extensible Firmware Interface* (UEFI), quale interfaccia *firmware* standard per pc, progettata in sostituzione del BIOS.

Appendice

Le parole del *cyber*

***Basic Input Output System* (BIOS)**. Programma che risiede sul *chip* della scheda madre e che gestisce l'avvio del sistema operativo. Questo è altresì deputato a verificare che tutte le componenti *hardware* funzionino correttamente.

***Distributed Denial of Service* (DDoS)**. Attacco DoS lanciato da un gran numero di sistemi compromessi ed infetti (*botnet*), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi *server*.

Firmware. Programma integrato in un componente elettronico e che ha la funzione di assicurarne l'avvio e l'interazione con altre componenti *hardware*.

Hacktivist. Termine che deriva dall'unione di due parole, *hacking* e *activism* e indica le pratiche dell'azione diretta digitale in stile *hacker*. Nell'ambito dell'*hacktivism* le forme dell'azione diretta tradizionale sono trasformate nei loro equivalenti elettronici, che si estrinsecano prevalentemente, ma non solo, in attacchi DDoS e *web defacement*.

Hashtag. Nell'ambito dei *social network*, identifica la parola o la frase preceduta dal simbolo cancelletto (#), che consente di indicizzare e classificare i messaggi con una parola chiave, rendendo gli stessi reperibili agli utenti interessati alla tematica.

Internet of Things (IoT). Neologismo riferito all'interconnessione degli oggetti tramite la rete internet, i quali possono così comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di applicabilità sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

Malware. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo. I *software* malevoli sono divenuti, nel tempo, sempre più sofisticati. Non solo sono adattabili a qualsiasi tipologia di obiettivo, ma sono anche in grado di sfruttare vulnerabilità non ancora note (cd. *0-day*) per infettare le risorse informatiche dei *target*. Ciò consente a tali *software* di non essere rilevati dai sistemi antivirus e di passare praticamente inosservati. Essi, inoltre, sono in grado di celarsi nell'ambito del sistema-obiettivo, di spostarsi al suo interno, così da poterne effettuare una mappatura e propagare l'infezione. Infine, grazie agli stessi, le informazioni di interesse, prima di essere sottratte, vengono compresse e criptate per celarne l'esfiltrazione con il traffico di rete generato dall'ordinaria attività lavorativa del *target*.

Malware reverse engineering. Esame del funzionamento e del comportamento di un *malware* condotta tramite analisi statica o dinamica, al fine di comprendere quali sono le istruzioni eseguite, le finalità del *software* malevolo ed il suo possibile autore.

Ransomware. *Malware* che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I *ransomware* sono, nella maggioranza dei casi, dei *trojan* diffusi tramite siti *web* malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento ed altri oggetti similari.

Social engineering. Tecnica di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Spyware. *Malware* usato per raccogliere e trasmettere informazioni da remoto. Le informazioni carpite possono riguardare, a titolo di esempio, abitudini di navigazione in rete, *password* e chiavi crittografiche.

SQL Injection. Tecnica mirata a colpire applicazioni *web* che si appoggiano su *database* programmati con linguaggio SQL, tramite lo sfruttamento di vulnerabilità quali l'inefficienza dei controlli sui dati ricevuti in *input* e l'inserimento di codice malevolo all'interno delle *query*. Tali attacchi consentono di accedere alle funzioni di amministrazione del sistema oltre che di sottrarre o alterare i dati.

Trojan. *Malware* che impiega l'ingegneria sociale, presentandosi come un *file* legittimo (ad esempio con estensione .doc o .pdf), facendo credere alla vittima che si tratti di un file innocuo, ma che in realtà cela un programma che consente l'accesso non autorizzato al sistema da parte dell'attaccante. Il *trojan* può avere diverse funzioni: dal furto di dati sensibili al danneggiamento del sistema target. Particolare categoria sono i cd. ***Banking Trojan***, programmati per acquisire le credenziali di accesso degli *account* dei siti di banca *on-line* al fine di effettuare illeciti trasferimenti di fondi verso conti bancari controllati da gruppi di cyber criminali.

Web defacement. Attacco condotto contro un sito *web* e consistente nel modificare i contenuti dello stesso limitatamente alla *home page* ovvero includendo anche le sottopagine del sito.