Presidenza del Consiglio dei Ministri

Sistema di informazione per la sicurezza della Repubblica

RELAZIONE

SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA

2014

Presidenza del Consiglio dei Ministri
Sistema di informazione per la sicurezza della Repubblica

Relazione sulla politica dell'informazione per la sicurezza 2014

EXECUTIVE SUMMARY

Con la presente Relazione, ai sensi dell'art. 38 della Legge n. 124 del 2007, il Governo riferisce al Parlamento sulla politica di informazione per la sicurezza e sui risultati conseguiti nel corso del 2014.

In **PREMESSA** si è inteso anzitutto evidenziare come l'applicazione coerente, costante nel tempo ed innovativa delle leggi di riforma abbia consentito al Governo di avvalersi dello strumento intelligence in una modalità sempre più integrata nel *decision making* nazionale. Viene, in particolare, sottolineato che nel corso del 2014 si sono configurate "minacce integrate" alla sicurezza nazionale, riconducibili anzitutto alle diverse declinazioni e forme del jihadismo, nonché agli scenari critici direttamente impattanti sugli interessi italiani ed alle perduranti sfide asimmetriche al sistema Paese, che hanno messo alla prova la capacità di risposta del Sistema di Informazione per la Sicurezza della Repubblica.

pagg. 7 – 21

Si rileva, al riguardo, che l'azione del Comparto informativo si è dipanata lungo quattro precise direttrici di indirizzo: la piena sintonia con il livello politico; la "manutenzione della riforma", volta a rafforzare l'unitarietà della comunità di intelligence; il recupero di sempre più ampi margini di efficacia ed efficienza nell'utilizzo delle risorse, perseguito anche attraverso l'aggiornamento dei metodi di lavoro; la promozione di una cultura della sicurezza condivisa con i cittadini, con le imprese e con il mondo accademico e della ricerca.

L'impianto espositivo della Relazione compone il quadro dei prioritari ambiti di attenzione dell'intelligence aggregandoli attorno a tre macro-aree tematiche: il fenomeno jihadista, le vulnerabilità del tessuto economico e le connesse dinamiche sociali, le minacce attestate nello spazio cibernetico. In linea con la precedente edizione, chiudono la Relazione un breve capitolo sulle prospettive del rischio e l'allegato "*Documento di Sicurezza Nazionale*" che riferisce, come previsto dalla normativa vigente (art.38, comma *1-bis* della legge 124/2007), sulle attività svolte in materia di tutela delle infrastrutture critiche nonché di protezione cibernetica e sicurezza informatica.

La **I PARTE**, dal titolo ***JIHAD* GLOBALE, *JIHAD* REGIONALE,** si sofferma in primo luogo sull'evoluzione de **LA MINACCIA IN OCCIDENTE,** così come qualificata dall'affermazione dello *Stato Islamico*, dall'accresciuta effervescenza della galassia jihadista e dalla connessa, accentuata capacità di presa del messaggio radicale, affidato a forme di comunicazione sempre più efficaci e pervasive. In quest'ottica l'estremismo *homegrown*, inteso anche quale bacino di reclutamento per aspiranti combattenti, viene individuato come il principale *driver* della minaccia terroristica, riferibile tanto a lupi solitari e a cellule autonome quanto al diretto ingaggio da parte di organizzazioni strutturate operanti nei teatri di *jihad*.

pagg. 25 – 32

Segue quindi il capitolo sugli **SCENARI AFRICANI E MEDIORIENTALI,** nel quale l'attivismo delle formazioni terroristiche di ispirazione jihadista rappresenta un significativo connettore tra le aree di instabilità che interessano il Nord Africa, il quadrante sahelo-sahariano e il Medio Oriente.

pagg. 33 – 43

In esordio vengono tratteggiati gli sviluppi intervenuti nel corso dell'anno in Libia, Tunisia, Marocco, Algeria ed Egitto. Si prosegue con le evoluzioni in Mali, Somalia, Kenia, Golfo di Guinea, Nigeria, Repubblica Centrafricana e Sud Sudan. Quanto alle regioni mediorientali, una sezione *ad hoc* è dedicata al conflitto in "*Syrak*", con specifico riguardo all'accresciuto protagonismo dello *Stato Islamico*, a scapito delle altre formazioni estremiste, e all'impatto della crisi in chiave umanitaria e di sicurezza sui Paesi limitrofi, quali Libano e Giordania. I passaggi successivi sono dedicati al difficile processo di stabilizzazione in atto in Yemen, alle evoluzioni del *dossier* nucleare iraniano e agli sviluppi del processo di pace israelo-palestinese.

Il focus sulle criticità regionali si sposta più ad Est, con una panoramica su **VECCHIE E NUOVE FRONTIERE DEL *JIHAD***, in relazione alla situazione sul campo in Afghanistan e Pakistan, ancora caratterizzata dal dinamismo della componente *Taliban*, all'attivismo estremista in altre realtà centro-asiatiche e al possibile incremento delle attività terroristiche nel Sub-continente indiano e nel Sud-Est asiatico. *pagg. 45 – 48*

Le minacce trattate nella **II PARTE** hanno come riferimento la **SFIDA ECO-FIN E IL *FRAMEWORK* SOCIALE.** Nella sezione concernente **LE MINACCE ALL'ECONOMIA,** muovendo dagli indicatori che attestano il persistere, nel 2014, della fase recessiva, viene evidenziata la centralità della dimensione economico-finanziaria quale ambito prioritario di attenzione dell'intelligence a presidio degli assetti strategici ed interessi nazionali secondo varie direttrici d'azione: contro lo spionaggio industriale e le pratiche lesive della concorrenza sui mercati nazionali ed internazionali; a tutela dei nostri investimenti all'estero e delle linee di approvvigionamento energetico; in direzione dei fenomeni di evasione ed elusione fiscale; a protezione della stabilità del sistema bancario e finanziario. *pagg. 51 – 63*

Si continua con il crimine organizzato**,** in primo luogo per evidenziare come le mafie, sfruttando gli effetti negativi della crisi, abbiano continuato a perseguire strategie d'infiltrazione in diversi settori dell'economia mediante il riciclaggio di capitali di provenienza illecita e l'acquisizione di realtà imprenditoriali in difficoltà. Ci si sofferma poi sugli interessi della criminalità organizzata italiana all'estero e sulla vitalità di strutturati gruppi criminali stranieri operanti in Italia.

In tema di **SPINTE ANTI-SISTEMA E MINACCIA EVERSIVA**, si dà conto dei rilevati segnali di intensificazione del disagio e delle possibili tensioni sociali alla luce dell'attivismo di formazioni antagoniste, di diversa matrice, intenzionate a radicalizzare le varie proteste sul territorio e ad innalzare il livello di contrapposizione con le Istituzioni. Sono trattati, inoltre, i profili di rischio riconducibili all'eversione anarco-insurrezionalista e all'estremismo marxista-leninista, nonché, in chiusura, i tratti distintivi e quelli più insidiosi, dell'attivismo di estrema destra. *pagg. 65 – 73*

A seguire, il capitolo **LA PRESSIONE DELLE CRISI SULLE FRONTIERE DELL'EUROPA** è dedicato al sensibile *dossier* dell'immigrazione clan- *pagg. 75 – 78*

destina, che vede i Servizi d'informazione impegnati a contrastare sul piano informativo un fenomeno che trae origine dalle crisi regionali e viene sfruttato da organizzazioni criminali sempre più ramificate ed interconnesse. In questa chiave si fa riferimento alle rotte e direttrici del traffico, ai sodalizi coinvolti ed all'impatto sul territorio nazionale.

La **III PARTE** dell'elaborato, intitolata **LA MINACCIA NEL CYBERSPAZIO,** muove dai più significativi aspetti fenomenici de **LA *CYBERTHREAT*** *pagg. 81 – 87* per tratteggiare poi le sfide future che l'intelligence dovrà fronteggiare con riguardo all'evoluzione delle modalità operative e all'ampio *range* di finalità e attori, cui corrisponde un ventaglio altrettanto diversificato nelle tipologie di rischio per la sicurezza del Sistema Paese: dagli attacchi alla sicurezza delle infrastrutture critiche nazionali allo spionaggio digitale, dall'hacktivismo contro obiettivi istituzionali al *cyberjihad*. Segue poi il Capitolo su **AZIONE PREVENTIVA E PROSPETTIVE**, *pagg. 89 – 91* centrato sulla risposta dell'intelligence e sulle possibili evoluzioni del fenomeno.

La Relazione si conclude con **SCENARI E TENDENZE: UNA SINTESI,** *pagg. 93 – 96* che riassume in chiave prospettica il composito panorama della minaccia che impegnerà l'intelligence nell'immediato futuro. Sulla base degli indicatori sin qui raccolti, è prevedibile che l'azione degli Organismi informativi debba rimanere prioritariamente focalizzata sul terrorismo di matrice jihadista e sulle minacce al sistema Paese, incluse quelle che si dispiegano nel cyberspazio.

L'allegato **DOCUMENTO DI SICUREZZA NAZIONALE,** infine, com- *pagg. 99 – 108* pendia le attività poste in essere dal Comparto – attraverso un articolato processo al quale partecipano fattivamente tutte le componenti dell'architettura *cyber* nazionale, così come delineata nel DPCM del 24 gennaio 2013 – in materia di tutela delle infrastrutture critiche materiali e immateriali, nonché di protezione cibernetica e sicurezza informatica nazionale.

Relazione sulla politica dell'informazione per la sicurezza

2014

La Relazione al Parlamento in versione digitale

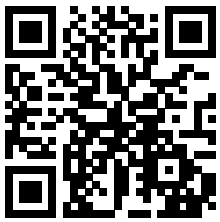
Il nuovo formato e-book

Il documento *on-line* disponibile sul sito istituzionale, oltre che nella consueta versione PDF, è ora consultabile anche in formato *e-book*, ovvero come un libro digitale da sfogliare su *tablet*, *smartphone* e sugli appositi lettori elettronici (*e-reader*). Tale opzione consente di personalizzare le opzioni di lettura, quali ad esempio le dimensioni del carattere e lo sfondo, e di compiere operazioni nel testo (evidenziare, ricercare parole, spostarsi agevolmente all'interno del documento).

Le istruzioni per il *download* della Relazione in formato *e-book* sono riportate sul sito istituzionale alla pagina www.sicurezzanazionale.gov.it/relazione-2014, che è possibile raggiungere anche utilizzando il *QR Code* riportato in basso.

Cos'è il QR Code?

Il *QR-Code* (*Quick-Response Code*) è un codice a barre bidimensionale che consente di collegarsi ad un sito utilizzando la fotocamera del proprio *tablet* o *smartphone*. Nel caso in cui l'applicazione per la lettura del *QR Code* non fosse già disponibile sul dispositivo, è necessario effettuare il *download* di una delle tante applicazioni gratuite disponibili in rete, da selezionare in base al proprio sistema operativo. Avviata l'applicazione, si posizionerà la fotocamera del dispositivo davanti al seguente *QR Code* e in pochi secondi sarà visualizzata la pagina della Relazione annuale 2014.



Dato alle stampe il 13 febbraio 2015

INDICE

PREMESSA

Rispondere alle sfide con la forza della normalità. La semplice sintesi di questo imperativo definisce plasticamente l'orizzonte verso il quale è stato indirizzato il percorso di riforma del Comparto intelligence: presidio vitale per il Paese rispetto al novero di minacce antiche e nuove, sempre più asimmetriche, poliformi ed ibride, strumento certo "non convenzionale", ma anche istituzione moderna e trasparente al servizio dello Stato, dei cittadini e delle imprese secondo un modello ridistributivo della informazione strategica come bene collettivo per la sicurezza nazionale.

Una traversata compiuta

Segno manifestamente tangibile, di altissimo valore non solo simbolico, di come i "Servizi segreti" abbiano in questi anni saputo compiere la traversata loro richiesta dall'incalzante cambiamento dello scenario globale ed interno è stata la partecipazione, per la prima volta in assoluto, del Capo dello Stato all'inaugurazione dell'Anno Accademico della Scuola di formazione del Comparto. Si è trattato del momento essenziale di una fisiologia consolidata nel modo di essere e di operare dell'intelligence. Ed anche del passaggio, oramai manifesto, dall'istintiva diffidenza di un tempo all'odierno consapevole riconoscimento sia di una centralità di "ruolo" nella protezione degli interessi fondamentali della Nazione, che di una "funzione" indispensabile in ogni democrazia, dispiegata ed ora anche percepita quale utile alla società, al benessere ed alla sicurezza dei cittadini, delle imprese, delle istituzioni.

Merita, al riguardo, sottolineare un duplice ordine di circostanze.

L'integrazione nei meccanismi decisionali

Da una parte, l'applicazione coerente, costante ed al contempo fortemente innovativa di una riforma ambiziosa e lungimi-

rante, coniugata a sua volta con il meritorio sforzo di apertura compiuto negli ultimi anni, ha consentito al Governo di avvalersi dello strumento intelligence, che è e deve rimanere giustappunto uno strumento "non convenzionale", in una modalità pienamente integrata nel *decision making* nazionale: nella politica di sicurezza, nella politica estera e di difesa, nella politica economica.

La "rivoluzione delle aspettative crescenti"

Dall'altra, la coscienza non soltanto nell'Esecutivo e nella Pubblica Amministrazione, ma anche presso le istanze politico-parlamentari e, più in generale, presso la pubblica opinione, della fruibilità sociale dei Servizi di informazione, ha ingenerato una salutare "rivoluzione delle aspettative crescenti", tale da implicare un'incessante verifica di efficacia.

Sempre più l'intelligence è chiamata ad essere, anche dimostrando di essere, all'altezza dei tempi, ossia di sapere dedicarsi, nel rigore e nell'assoluto rispetto delle regole, dei limiti e dei vincoli stabiliti dalla normativa, alla lettura ed alla prevenzione di problemi sempre più articolati, sovente di portata tale da ipotecare, ove rimanessero aperti, la sicurezza del sistema Paese nel suo complesso. Gli Organismi nel loro agire quotidiano si sono connotati come una "struttura di servizio", alla quale è affidata la missione di lavorare in una modalità sommersa e non convenzionale per far sì che il Governo assuma, in maniera informata e consapevole, decisioni fondamentali volte a garantire l'intangibilità delle componenti costitutive dello Stato e dei valori fondanti dell'ordinamento costituzionale, ed esprima la capacità di perseguire interessi statali primari, in un panorama composito di minacce endogene ed internazionali.

Avvisare, predire, prevenire

Si tratta di una responsabilità nella quale si fondono tre azioni imperative: avvisare, predire, prevenire.

Avvisare: una capillare e quanto più affidabile raccolta informativa sul campo è presupposto per segnalare al decisore politico in tempo utile, e con il necessario livello di accuratezza, attendibilità e dettaglio, l'insorgere di criticità, evenienze, dinamiche o condotte potenzialmente lesive per gli interessi nazionali. È un'attività imprescindibile, che tuttavia non esaurisce la ragion d'essere dei Servizi.

Predire: negli attuali scenari interni e globali caratterizzati da rischi multiformi, l'accresciuta volatilità strategica e la sempre maggiore complessità dei modelli sociali richiedono uno "sguardo lungo" da parte delle classi dirigenti, vale a dire la capacità di guardare oltre le contingenze, al di là delle emergenze del momento, a tutela dell'interesse nazionale e dei segmenti cruciali dell'economia. La gestione delle complesse evoluzioni socio-economiche e delle grandi questioni geopolitiche necessita, in altri termini, di un'elevata capacità predittiva da parte degli apparati di sicurezza, allo scopo di assicurare, anche in presenza di fatti

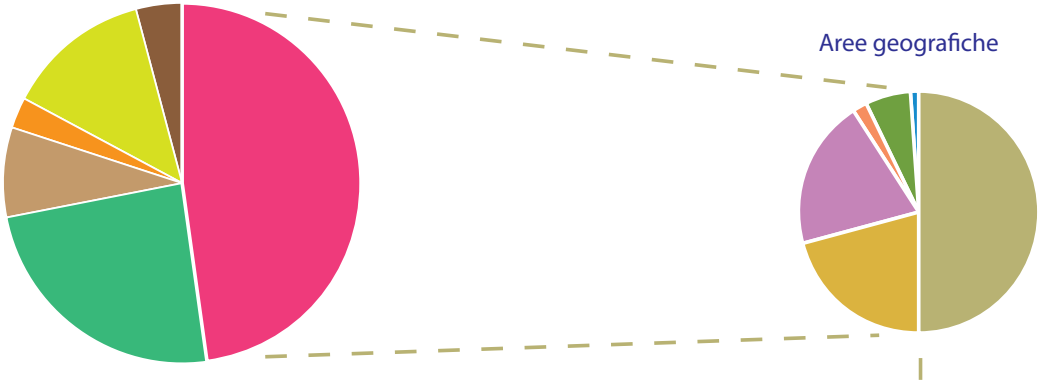
imprevisti ed eccezionali, la necessaria ed immediata continuità della vita delle organizzazioni pubbliche e private e delle attività economiche e produttive.

Da qui l'esigenza, per l'intelligence, di fornire alla committenza politica non solo informazioni contestualizzate, ma anche lavori concettuali di alto livello, prodotti analitici sofisticati per impianto e tecniche di elaborazione che incentivino la riflessione ed in tal modo contribuiscano a ricomporre in una immagine il più possibile nitida e decifrabile i tanti frammenti sparsi di un mondo in continua trasformazione (*vedi grafici sulla produzione di AISE ed AISI).*

Prevenire, infine: dispiegare una capacità di influenza strategica ad ampio spettro, tanto sotto il profilo della dissuasione rispetto a eventi temuti in relazione al loro impatto sulla sicurezza del Paese, quanto in termini di promozione e supporto agli interessi nazionali. È, peraltro, indice di raggiunta maturità che

AISE

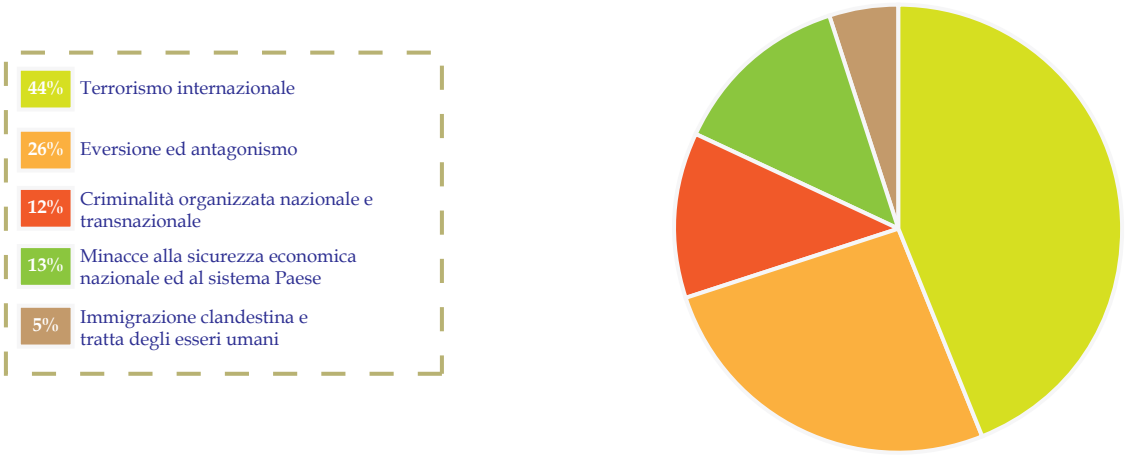
INFORMATIVE/ANALISI INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA ANNO 2014



- 48% Aree geografiche
- 24% Terrorismo internazionale
- 8% Immigrazione clandestina e tratta degli esseri umani
- 3% Proliferazione delle armi di distruzione di massa e dei relativi vettori
- 13% Minacce alla sicurezza economica nazionale ed al sistema Paese
- 4% Criminalità organizzata transnazionale

- 50% Asia
- 21% Africa
- 20% Medio Oriente e Penisola Araba
- 2% Balcani ed Europa orientale
- 6% Comunità Stati Indipendenti
- 1% America meridionale

AISI
INFORMATIVE/ANALISI INVIATE A ENTI ISTITUZIONALI E FORZE DI POLIZIA ANNO 2014



l'intelligence sia stata, nei mesi scorsi, coralmente investita anche di tale compito peculiare.

Un'inedita verifica di efficacia

In effetti, nelle difficili stagioni del 2014, la verifica di efficacia è stata svolta in termini per molti versi inediti, e si è potuta testare l'attitudine del Sistema di informazione per la sicurezza della Repubblica a misurarsi con un contesto di aspettative crescenti.

Ciò perché il Governo, sempre più chiamato a definire, ponderare ed attuare linee di indirizzo politico in una dimensione strategica, ha effettivamente trovato, nel contributo sistematico dei Servizi di informazione, un *asset* di fondamentale importanza, che gli ha permesso, nell'assumere decisioni relative alla sicurezza interna come nello svolgere azioni di politica estera, di distinguere i rischi dalle opportunità, di scorgere i contorni delle minacce, di saggiare col dovuto realismo i margini di manovra concretamente disponibili.

Le minacce "classiche" e le sfide contingenti

Sono infatti venute riproponendosi, nell'ultimo anno, minacce in qualche modo "classiche", verso le quali AISE ed AISI hanno potuto far valere il loro consolidato bagaglio di preparazione ed esperienza, come lo spionaggio, le ingerenze ostili, la proliferazione delle armi di distruzione di massa e dei relativi vettori.

Sono stati parimenti posti in gioco gli approvvigionamenti energetici, la stabilità della nostra area geopolitica e di numerose regioni del mondo, persino gli stessi valori che riteniamo debbano informare la Comunità internazionale. Sfide che hanno richiesto la messa in campo di capacità informative, analitiche e tecnologiche sempre più sofisticate, cui si è risposto nella triplice cornice dell'Unione Europea, a più forte ragione nell'esercizio della presidenza semestrale, della NATO e delle Nazioni Unite, in piena collaborazione con i Servizi dei Paesi amici ed alleati.

Allo stesso tempo, il persistere di indicatori negativi del contesto macroeconomico ha generato conseguenze assai rilevanti: i consumatori hanno rimodulato la struttura delle loro spese a causa delle ridotte prospettive reddituali, molte imprese hanno ridimensionato la loro capacità produttiva e la propensione ad innovare, gli investitori nazionali ed esteri hanno dovuto sempre più tener conto dell'incertezza delle prospettive economiche, che mina la fiducia nel mercato, ed è aumentata la disoccupazione, soprattutto giovanile.

In tale congiuntura difficile, si sono registrati segnali di intensificazione del disagio e delle tensioni sociali, che hanno indotto ad effettuare un attento monitoraggio dell'attivismo di movimenti, non solo italiani, a matrice antagonista ed anarco-insurrezionalista pronti a cogliere ogni occasione per promuovere e fomentare la protesta violenta: minaccia molto insidiosa per l'ampiezza sia della gamma dei potenziali obiettivi sia dei collegamenti transnazionali, teoricamente in grado di agire da moltiplicatore dei rischi.

A trarre vantaggio dalla crisi e dalla diffusa scarsità di liquidità sono state, dal canto loro, anche le organizzazioni mafiose, concentratesi sui reati finanziari e di riciclaggio: da qui l'intensificazione dell'azione di contrasto e l'ampliamento del suo raggio di azione, grazie ad una stretta sinergia fra intelligence e Forze dell'ordine.

Le minacce integrate come cruciale banco di prova

Altro, tuttavia, è stato il motivo più rilevante per il quale l'ultimo anno ha finito con il costituire un cruciale banco di prova per il sempre maggiore affidamento che si ripone sul ruolo della comunità intelligence: l'inusitato configurarsi di vere e proprie "minacce integrate" alla sicurezza nazionale, riconducibile alla contestuale presenza sia di scenari critici internazionali direttamente impattanti sugli interessi italiani, che del continuativo riproporsi di sfide asimmetriche alla nostra sicurezza.

Le crisi ucraina e libica…

Le crisi ucraina e libica hanno coinvolto in prima linea l'Europa e l'Italia.

Gli sforzi compiuti per promuovere efficacemente una soluzione politica – l'unica possibile – ad un conflitto, quello russo-ucraino, disputato anche nell'arena mediatica, ed il cui protrarsi o "congelarsi" comporterebbe conseguenze assai negative per l'intera co-

munità euro-atlantica, hanno reso impellente la necessità di disporre di una visione chiara dell'andamento sul terreno, al fine di trarne indicazioni sulle possibili evoluzioni e soluzioni. In tale contesto, la capacità dell'intelligence di monitorare ed analizzare gli sviluppi della situazione e la postura di tutti gli attori coinvolti si è rivelata di valido orientamento per il decisore politico.

È stato, allo stesso tempo, garantito un efficace presidio informativo in Libia, teatro di assoluta importanza che vede l'Italia convintamente impegnata, a sostegno ed in armonia con l'azione delle Nazioni Unite, a scongiurarne la frammentazione ed a sostenere un processo politico di transizione inclusivo nel quale possano pacificamente e democraticamente riconoscersi tutte le componenti di quel popolo. Lo scenario libico può trasformarsi in una minaccia diretta per l'Italia, come fattore di destabilizzazione dell'intera regione, ma anche quale potenziale piattaforma per proiezioni terroristiche, *vulnus* per gli approvvigionamenti energetici, snodo per l'immigrazione clandestina. Per questi motivi, l'intelligence vi ha continuato a svolgere, lungo tutto il 2014, un ruolo importante, al fine di monitorare ed attenuare i rischi per la nostra presenza, ed anche di valutare i margini per contribuire ad innescarvi le auspicate dinamiche virtuose.

...le nuove dinamiche del jihadismo, sfida paradigmatica

Indiscussa centralità ha rivestito, nel lavoro svolto dagli Organismi informativi, la determinazione nel fronteggiare la sfida emergente costituita dalla formazione dello *Stato Islamico* (IS). In essa si saldano in maniera paradigmatica una minaccia militare simmetrica – per combattere la quale l'Italia non ha fatto mancare il suo contributo allo sforzo internazionale – ed una asimmetrica, rappresentando l'IS una base di reclutamento, addestramento, sviluppo e finanziamento per progettualità terroristiche verso tutto l'Occidente, che è stato quindi chiamato a rispondere con iniziative adeguate, a partire dal monitoraggio e dall'inibizione dei viaggi degli aspiranti combattenti per il *jihad*.

Allo stesso tempo, la scelta strategica del qaidismo come dell'IS di ispirare il volontarismo individuale in funzione antioccidentale ha accresciuto le difficoltà nell'attività di contrasto e ha moltiplicato i soggetti a rischio. I drammatici eventi verificatisi in Francia ed in Belgio nel gennaio 2015 hanno dolorosamente dimostrato quanto sia elevata e concreta la minaccia che promana da tale evoluzione delle modalità operative di individui e gruppi estremisti che si riconducono alle diverse declinazioni del jihadismo.

Assoluta priorità per il Sistema di informazione per la sicurezza della Repubblica, in costante dialogo e scambio informativo con i Servizi dei Paesi amici ed alleati, è stato pertanto il rischio che operino nel nostro Paese cellule terroristiche autonome composte da soggetti radicalizzati di varia estrazione e provenienza, intenzionati ad impiantare filiere radicali o a condurre attacchi in Europa.

Sono massimi il livello di guardia e la collaborazione internazionale intelligence. Ciò anche se non si ha, ad oggi, cognizione di specifiche progettualità contro il nostro Paese dove, tuttavia, la minaccia terroristica di matrice jihadista rimane collegata, nella sua dimensione domestica, al cd. *jihad* individuale. Tanto in relazione all'eventualità di un'autonoma attivazione – specie sulla spinta della propaganda *on-line* – di elementi isolati o microgruppi motivati a colpire la società occidentale dall'interno, come pure nel caso di cellule dormienti che si riattivino in esito ad indicazioni esterne.

Le minacce asimmetriche al sistema

Hanno, inoltre, continuato a manifestarsi con crescente intensità minacce asimmetriche che sono certamente meno "visibili" delle cruente gesta dei terroristi. Benché, anche per tale motivo, creino minore allarme nella generale percezione, esse testano più e meglio di qualsiasi altra la capacità dei Servizi di informazione di stare al passo con il rapidissimo evolversi di sfide sempre più insidiose.

La minaccia cibernetica e quella economico-finanziaria puntano, infatti, non solo a bersagli militari o politici, ma altresì a colpire gli anelli deboli dei nostri assetti industriali, finanziari, scientifici, tecnologici. Esse impongono, perciò, la capacità di fare sistema a nostra volta e, decisivo vantaggio strategico del difensore, di "fare squadra" come sistema Paese, tra attore pubblico e mondo imprenditoriale, con la finalità di scongiurare il rischio di un vero e proprio declassamento strutturale del Paese.

Questa coerenza d'azione ed unità di intenti risulta essenziale per affrontare un contesto di mercato e di sicurezza in cui dinamiche globali si intrecciano con minacce ed eventi locali. Il dialogo sempre più intenso e frequente tra intelligence e mondo delle imprese si informa a scelte di indirizzo politico fissate dall'Esecutivo attraverso il Comparto informativo, cui la legge di riforma del 2007 ha affidato anche il compito di tutelare la sicurezza economica.

Dalla dimensione analogica a quella digitale…

L'estensione delle diverse tipologie di minaccia (spionaggio, terrorismo, antagonismo, criminalità) dalla dimensione tradizionale, "analogica", a quella digitale, diluendo spesso a dismisura i tempi di percezione ed alimentando un "falso senso di sicurezza", può comportare pericoli molto gravi e concreti in primo luogo per le nostre infrastrutture critiche. Attraverso attacchi cibernetici, anche con finalità di spionaggio, il *know-how* tecnologico ed industriale delle nostre aziende e dei nostri centri di ricerca può altresì essere derubato da attori stranieri o da organizzazioni criminali. Dalla sicurezza delle reti informatiche, inoltre, dipende sempre più il fondamentale diritto dei cittadini di comunicare liberamente e nel pieno rispetto della *privacy*.

L'intelligence ha, di conseguenza, proseguito il suo impegno nel potenziare le

difese, in stretto e necessario raccordo con i *partner* internazionali, nonché coordinando gli sforzi degli innumerevoli *stakeholder* pubblici e privati, poiché ogni vulnerabilità, nei sistemi interconnessi, può riverberarsi sulla tenuta della sicurezza collettiva.

Con l'adozione del Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e del conseguente Piano Nazionale per la protezione cibernetica e la sicurezza informatica, l'Italia si è dotata di una strategia coerente con il *framework* internazionale, attorno alla quale le Pubbliche Amministrazioni ed i soggetti privati operano insieme, nella misura del possibile, per organizzare un sistema di difesa condiviso contro una minaccia per sua natura improvvisa, fulminea, sfuggente. A beneficio di chi è chiamato a fronteggiarla, compito della comunità intelligence è stato e continuerà ad essere anzitutto quello di diminuire il *gap* informativo, di dare corpo, nelle sfere più strategiche ed esposte, alle opportune sinergie tra istituzioni ed aziende nazionali rilevanti nel settore della sicurezza, tese a prevenire e contrastare attacchi informatici, e ad assicurare la protezione delle reti e dei contenuti che vi transitano.

… alla minaccia eco-fin

Allo stesso tempo, nelle nuove forme e dimensioni della competizione globale possono annidarsi minacce per gli interessi economici, scientifici e industriali dello Stato.

Si è così confermata, nell'anno trascorso, la centralità della dimensione economico-finanziaria per la tutela della sicurezza nazionale e, dunque, per l'attività di ricerca informativa svolta dagli Organismi: dallo spionaggio industriale in tutte le sue forme alle pratiche lesive della concorrenza sui mercati nazionali ed internazionali, dal riciclaggio di capitali di provenienza illecita alle infiltrazioni del grande crimine organizzato in molti settori dell'economia, dalla tutela dei nostri investimenti all'estero a quella delle linee di approvvigionamento energetico.

In tale ambito, si è inoltre confermato come indispensabile, in analogia a quanto accade negli altri Paesi, l'utilizzo della leva intelligence a protezione del patrimonio scientifico e tecnologico: decisivo fattore di competitività, detenuto dalle realtà produttive della nostra Italia.

Sul punto, nota la struttura granulare del tessuto industriale nazionale, vale evidenziare come le imprese medio-piccole registrino – a valle di una prolungata fase recessiva – una crescente vulnerabilità soprattutto dal punto di vista finanziario, data la carenza di capitali freschi attingibili dai circuiti ordinari.

Si è dunque trattato di un settore dell'attività del Comparto perimetrato, quanto a spazi di intervento, dalla duplice esigenza di non interferire nel libero svolgersi delle vicende economiche e di perseguire, contestualmente, l'obiettivo, fondamentale per l'azione di rilancio del Paese, di apertura massima agli investimenti esteri.

Si è nondimeno rilevato come questi ultimi possano essere, in singole, specifiche contingenze, finalizzati a sottrarre conoscenze ed a pregiudicare le possibilità di sviluppo e le prospettive occupazionali. In siffatte circostanze, gli *asset* strategici nazionali vanno efficacemente protetti, facendo ricorso, là dove effettivamente necessario ed opportuno, ad ogni strumento previsto dalle normative vigenti. In tal senso, l'attività di intelligence si è posta a salvaguardia di quelle dinamiche di mercato che favoriscono l'efficienza produttiva ed allocativa, incentivano l'impiego ottimale delle risorse, incoraggiano l'innovazione e la crescita della produttività, stimolano la penetrazione delle aziende nei mercati esteri.

Come superare la "prova del nove": quattro direttrici di indirizzo

È, in ultima analisi, proprio per la loro singolare complicazione e criticità che le minacce asimmetriche hanno rappresentato la "prova del nove" per l'apporto conoscitivo fornito all'Esecutivo dal Sistema di informazione e hanno sottoposto quest'ultimo a sollecitazioni intense e costanti, mettendone sotto quotidiano esame il quoziente di flessibilità ed adattabilità al cambiamento e l'attitudine ad innovarsi, ad adeguarsi alla mutevolezza ed al polimorfismo degli scenari. Hanno verificato, in altri termini, il valore aggiunto dell'intelligence, il suo grado di osmosi con le articolazioni ed i meccanismi del *decision making* nazionale.

Al riguardo, la riconosciuta normalità dei "Servizi segreti" ha preso forma concreta anche nella loro capacità, vieppiù corroborata nei mesi trascorsi, di corrispondere puntualmente alle richieste delle Amministrazioni. Ciò che è stato possibile nella misura in cui il loro operare si è dipanato lungo quattro precise direttrici d'indirizzo.

1. *Sintonia*

La prima, quale imprescindibile fonte di legittimazione ed al contempo presupposto qualificante dell'azione dell'intelligence, è stata la piena sintonia con il livello politico, tradottasi in uno scambio costante, senza soluzioni di continuità, di reciproca lealtà e di mutuo affidamento. In virtù dell'ininterrotta alimentazione di tale raccordo, il Governo ha potuto disporre di uno strumento sì, per sua natura, non convenzionale, ma, nondimeno, strettamente e rigidamente operante all'interno del perimetro giuridico nel perseguimento di obiettivi decisi dalla stessa Autorità politica.

Ciò è stato l'effetto di due fattori. Da un lato, il crescente ruolo del CISR, che riunisce attorno al medesimo tavolo i titolari delle responsabilità politiche riguardanti gli interessi nazionali di natura politica, militare, economica, scientifica ed industriale che costituiscono l'oggetto della missione intelligence. Il CISR è progressivamente evoluto in un "Gabinetto classificato per la sicurezza nazionale" a geometria variabile, capace di mettere a frutto, anche in virtù dell'assidua preparazione dei lavori nel suo formato al livello tecni-

co, quella visione di insieme delle minacce e dei relativi strumenti di prevenzione e contrasto senza la quale verrebbe meno la necessaria adeguatezza della risposta nazionale ai pericoli che si annidano nel contesto competitivo globale.

Per converso, tale evoluzione ha sistematicamente postulato il sempre più attivo ed incisivo coinvolgimento del Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), anzitutto sul piano dell'indispensabile verifica politica, ed altresì nel delineare la piena comunanza di intenti fra Esecutivo e Legislativo, come pure la feconda coralità d'impegno di tutte le compagini parlamentari sui temi della sicurezza nazionale, che sole permettono di combattere e vincere anche le battaglie più impegnative.

2. *La "manutenzione" della riforma*

È in forza di tali armonici rapporti tra decisori politici e vertici del sistema operativo dell'intelligence che si è potuto agevolmente continuare ad implementare nel 2014, a sviluppo dell'*acquis* ordinamentale e regolamentare consolidato negli anni precedenti, una seconda, significativa linea d'azione del settore, vale a dire la "manutenzione della riforma", attuata in una duplice direzione.

Unitarietà…

È stata in primo luogo rafforzata l'unitarietà della comunità di intelligence, armonizzando il pieno rispetto della ripartizione di competenze interna ed esterna voluta dal legislatore, forma di garanzia doverosa, con l'impulso a lavorare in maniera coerente ed integrata.

Si è rivelato ineludibile rafforzare in capo al DIS il coordinamento operativo fra le due Agenzie ed accrescere la complessiva armonia e continuità di tutto il processo informativo, dalla ricerca "sul campo", all'analisi situazionale, previsionale e strategica. Si tratta di precondizioni essenziali tanto per fronteggiare minacce nuove nella loro genesi e nella loro dinamica – emblematica, al riguardo, quella *cyber* – quanto per sviluppare con efficacia ed autorevolezza la collaborazione internazionale con i Servizi dei Paesi amici ed alleati che condividono i nostri stessi valori e perseguono i nostri stessi obiettivi: possiamo e dobbiamo contare sulla solidità della nostra rete di alleanze, al cospetto della quale sarebbe impensabile presentarsi ed agire in ordine sparso.

A tal fine, il Presidente del Consiglio dei Ministri, sentito il CISR, ha approvato il 23 luglio del 2014 una Direttiva che ha istituito all'interno del Comparto una Commissione permanente a composizione interorganismi, cui è stato affidato il compito specifico di espletare le attività necessarie e strumentali all'esercizio, da parte del DIS, dell'azione di indirizzo e di coordinamento ad essa demandata dalla legge, nelle diverse fasi in cui si articola il ciclo intelligence. Non un appesantimento dell'architettura esistente, bensì uno strumento agile, concepito con lo scopo di assicurare la sinergia e l'integrazione info-operativa fra le Agenzie, evitando *gap*, sovrapposizioni e duplicazioni.

Insediatasi già in estate, la Commissione, consolidando un formato intersettoriale già avviato, ha riservato il suo primo *focus* al fenomeno dei *foreign fighters* e al correlato capitolo dell'estremismo *homegrown*, e ha ulteriormente incoraggiato le sinergie info-operative fra AISE ed AISI. Ciò in un contesto di proficua interazione con le Forze di polizia, specie nell'ambito del Comitato di Analisi Strategica Antiterrorismo (CASA), che si è confermato quale virtuoso "modello italiano" di costante dialogo tra intelligence e *law enforcement* cui si guarda con interesse da parte di altri ordinamenti securitari europei.

…e pianificazione

L'atto di indirizzo presidenziale ha parimenti previsto – secondo una coerente progressione – la sinergia e la condivisione nella programmazione dell'attività informativa entro il perimetro ed in base alle priorità individuate dall'Esecutivo.

Con la pianificazione approvata dal CISR, le linee di ricerca sono state enucleate attorno a selezionate direttrici su cui concentrare sforzi e risorse. In questo contesto, i Servizi hanno potuto operare in maniera più incisiva negli ambiti info-operativi individuati come prioritari nonché a copertura di obiettivi – è il caso della corruzione – ora enucleati in maniera più mirata. La naturale interconnessione dei fenomeni oggetto di attività informativa esige infatti, oltre alla coerenza con il fabbisogno espresso dal Governo, anche la complementarietà fra i piani di ricerca individuati da ciascuna Agenzia, in ragione della sempre più marcata trasversalità delle minacce alla sicurezza nazionale.

3. *Risorse*

Spendere meno, spendere meglio…

Terzo binario che, con assiduità, si è continuato a percorrere anche nel 2014 per conferire vitalità, coerenza e congruità al processo di aggiornamento dell'intelligence nazionale è stato il recupero, in misura della economicità, di margini di efficacia ed efficienza nell'utilizzo delle risorse. Il settore si è autoimposto con un tasso di correzione significativo una manovra di *spending review* assai rilevante, informata a tre principi: risparmiare, razionalizzare, reinvestire in spesa produttiva.

Il "dividendo" ottenuto con tagli, revisioni e rimodulazioni di spesa è stato, in particolare, impiegato per potenziare la capacità tecnologica. A fronte degli investimenti sovente massicci compiuti da altri Stati in tale settore, ed in forza della necessità di contrastare gli attori della minaccia che ci obbligano ad interagire in tempo reale con rischi inediti e puntiformi, l'integrazione fra la componente umana, la cui valenza strategica rimane imprescindibile, e quella tecnologica è il vero *game changer* della dimensione intelligence.

Lo è nelle modalità di lavoro, nell'utilizzo costante ed adeguato di quanto la tecnologia può offrire a supporto: a tal fine, opera, in seno al Sistema di informazione, una Commissione Permanente

ICT (*Information and Communication Technology*), "cabina di regia" dinamica ed a geometria variabile, deputata ad attuare specifici progetti nel contesto del *procurement* unificato di Comparto introdotto dai nuovi regolamenti, e che ha fra l'altro animato, nel mese di novembre, un evento interno a carattere seminariale, presieduto dall'Autorità Delegata per la Sicurezza della Repubblica, inteso a fare il punto del lavoro sin qui svolto ed a tracciare, nell'ambito di apposito documento strategico, le linee guida cui uniformare gli investimenti tecnologici.

L'integrazione "uomo-tecnologia" è pure strumento di dialogo operativo con le Pubbliche Amministrazioni, gli Atenei, gli Istituti di Ricerca, i soggetti imprenditoriali: un mezzo che rende il lavoro dell'intelligence sempre più fruibile e tangibile, e con sempre maggiore velocità, da parte della società italiana.

…e modernizzare la cultura aziendale

Lo sforzo di modernizzazione non si è esaurito nello "spendere meno" e "spendere meglio". Il rinnovamento è dipeso anche dalla capacità di aggiornare la cultura istituzionale e di fare spazio alle energie più fresche.

È stata dunque portata avanti la politica di reclutamento avviata negli anni più recenti, con "campagne" realizzate attraverso procedure *on-line*, rivolte a giovani laureati e ricercatori da impiegare in segmenti che travalicano il tradizionale, e pur sempre fondamentale, ambito legato alla difesa degli interessi politico-militari del Paese. Le nuove professionalità, rappresentate da esperti di economia, finanza, matematica, ingegneria informatica, energia, sistemi complessi e reti infrastrutturali, sono state fuse con quelle provenienti dai bacini più "classici", Pubblica Amministrazione, Forze Armate e Forze di polizia. E sono state, soprattutto, formate.

L'attività della Scuola di Comparto è riassumibile nei numeri: oltre 500 tipologie di attività didattiche, tra addestramento info-operativo, area tecnologica, sicurezza fisica, competenze linguistiche, settore amministrativo-giuridico e sanità, frutto di un'articolata fase di rilevazione dei fabbisogni formativi, di pianificazione e progettazione degli interventi, in un ciclo continuo rinnovato di anno in anno sulle base delle diverse sollecitazioni provenienti dagli scenari, interni ed esterni, di interesse per la sicurezza nazionale.

Né i numeri dicono tutto. Ad essi va aggiunto, in primo luogo, l'insegnamento, nelle Aule della Scuola, non solo di competenze, ma più e prima ancora di valori istituzionali essenziali per il corretto funzionamento degli Organismi di intelligence in un ordinamento democratico.

Va aggiunta, altresì, l'apertura all'interazione con la società civile. In continuità col recente passato, sono stati ammessi alla frequenza di alcune iniziative didattiche esponenti di Pubbliche Amministrazioni con le quali sono in corso rapporti di collaborazione: è quanto è accaduto, fra gli altri, con il Ministero degli Affari Esteri

e della Cooperazione Internazionale, con cui è peraltro proseguito, per tutto l'anno, un collaudato esercizio di scambio analitico. La Scuola ha al contempo organizzato lezioni sull'intelligence riservate a studenti esterni e ha proseguito il *roadshow* inaugurato nel 2013. In una serie di incontri presso vari poli accademici della Penisola, cui ha partecipato l'Autorità Delegata per la sicurezza della Repubblica, i vertici degli Organismi hanno riscontrato ovunque interesse e disponibilità per i temi affrontati. Ad esito di tale tornata sono stati formalizzati accordi di collaborazione sia sul fronte della formazione che dell'analisi e della ricerca.

4. *Una cultura condivisa della sicurezza*

La proiezione esterna dell'ambito formativo non è stata, a sua volta, che tassello di un ben più vasto mosaico, ove si è composta la quarta, e per certi versi più qualificante, espressione di una visione moderna dell'intelligence: quella dell'*outreach* nel sistema Paese. L'obiettivo, quotidianamente ricercato, è quello di un Comparto intelligence che faccia pienamente propria la *mission* della comunicazione istituzionale e della promozione di una cultura condivisa della sicurezza. Tali attività sono indispensabili per un'intelligence aperta ed è opportuno coinvolgervi, oltre al mondo accademico e della ricerca, anche le imprese. Ciò quale ulteriore stimolo per promuovere lo sviluppo di un efficace *network* coordinato e dinamico di "sicurezza partecipata", alimentato da continue interazioni fra pubblico e privato nel pieno rispetto dei principi fondamentali dell'ordinamento democratico.

La riservatezza ed il segreto sono strumenti ineliminabili per tutelare le operazioni attuate a salvaguardia della sicurezza nazionale, da perseguire in termini di reciprocità, posto che le attività intervenute nell'ambito di accordi di collaborazione a livello internazionale debbono continuare ad essere protette dalla più stringente logica del *need to know*, nell'interesse della Nazione e dei valorosi professionisti che le svolgono.

Dalla "formula delle cinque W"…

Tuttavia, la riservatezza non deve necessariamente coprire tutto quanto viene fatto dall'intelligence, che è chiamata non solamente ad essere, ma anche a venire percepita come uno strumento normale esistente in tutti i Paesi. Non v'è motivo perché, nelle sue missioni, nelle sue regole e nelle sue metodologie, essa sfugga all'aurea "formula delle cinque W": *Who*, chi esercita la responsabilità di guidarla; *What*, cosa fa ed a cosa serve per difendere quel supremo bene collettivo che è la sicurezza nazionale; *Where*, quali sono le sue priorità e le sue sfere d'intervento; *When*, quando deve rispondere, in maniera flessibile, alle contingenze, in un *framework* strategico ed operativo profondamente incardinato nella normativa e concepito per mantenere la sua validità nel lungo periodo; *Why*, perché nel mondo d'oggi è impossibile farne a meno, men che mai in un ordinamento democratico.

…alla trasparenza come regola: il versamento agli archivi di Stato

Vale, in tutto questo, la linea dell'apertura e della conoscibilità, che i cittadini per primi si aspettano, come eloquentemente dimostrato dal massiccio afflusso di pubblico allo *stand* del Forum PA, dalle oltre 140.000 visite mensili al sito *www.sicurezzanazionale.gov.it* con più di 150 contributi alla sezione "Scrivi per noi", dalle 10.000 *mail* pervenute, dai circa 7.000 *curricula* ricevuti da persone che aspirano a lavorare nel Comparto.

Del resto, il principio che in un regime democratico la trasparenza sia la regola ed il segreto l'eccezione è l'ancoraggio costituzionale della legge di riforma. Ed è stato, nell'anno trascorso, anche il criterio ispiratore della direttiva con la quale il 22 aprile il Presidente del Consiglio ha disposto il versamento agli archivi di Stato, una cui prima *tranche* è già avvenuta in novembre, dei documenti fino ad ora classificati, non coperti da segreto di Stato, appartenenti a tutte le Amministrazioni e riguardanti alcuni dei più gravi episodi della storia repubblicana avvenuti tra il 1969 ed il 1984. Va sottolineato come, al netto dell'inevitabile dibattito che si è in qualche caso sviluppato sulla corrispondenza dei contenuti rispetto alle aspettative, vi è un dato, che va enfatizzato in tutta la sua rilevanza. E cioè che mai, nella storia repubblicana, si è proceduto ad una tale imponente opera di declassifica, coinvolgendo poco meno di quattromila fascicoli. La direttiva ha permesso di anticipare consistentemente i tempi fisiologici di versamento, di norma fissati in almeno 40 anni dalla cessazione della trattazione corrente, e ha dato concreta realizzazione ad un aspetto rilevante della legge 124 del 2007, ovvero il riconoscimento degli archivi dell'intelligence italiana come patrimonio a disposizione degli studiosi, del mondo dell'informazione e di tutti i cittadini.

L'iniziativa, riguardando uno dei periodi più complessi e dolorosi della storia repubblicana, si propone di apportare un contributo importante allo sviluppo ed al consolidamento della memoria collettiva del Paese, fornendo strumenti preziosi per la ricostruzione storico-politica di quell'epoca.

E ha, più ancora, segnato un punto di non ritorno, corroborando la visione di un'intelligence al servizio del cittadino nel segno del binomio fra trasparenza e democrazia.

Un punto di non ritorno

La logica della consuetudine con il mondo…

A venire riflessa nelle pagine che seguono è dunque l'attività di un Sistema informativo irreversibilmente modernizzato: plurale nell'articolazione ma centripeto nel *modus operandi*, selettivo negli ambiti di intervento, efficiente nell'allocazione delle risorse, trasparente nella sua ragion d'essere. Ciò non solo per forza di cose, ma anche per maturata coscienza di sé. L'intelligence sempre più si fa feconda-

mente contaminare da una visione olistica dei problemi e della loro dimensione transnazionale, col preciso scopo di adoperarsi per porre responsabilmente l'Autorità politica nella condizione di esercitare, con la necessaria avvedutezza, la sua prerogativa di decidere: cioè di scegliere, distinguendo in tempo utile ciò che fa la differenza fra l'ineludibile, generale rischiosità di un mondo complicato, ed il configurarsi di minacce reali, camaleontiche, pervasive, non sempre tangibili, rivolte all'ordinamento democratico ed ai suoi valori, alla libertà ed al benessere dei cittadini, delle famiglie e delle imprese, alla capacità di resistenza del sistema Paese.

Per precisa scelta, dunque, i capitoli che compongono la presente Relazione non contengono un'illustrazione indifferenziata e compilativa del lavoro svolto dagli Organismi. Si snodano, piuttosto, attorno ad un preciso architrave logico, costituito da quelle tre minacce integrate che hanno costituito banco di prova per il definitivo passaggio da uno "ieri" che non esiste più, e nel quale nessuno può coltivare l'illusione di vivere, ad un futuro difficilmente più rassicurante, ma sicuramente più decifrabile e forse più "gestibile" anche grazie all'impegno del Comparto.

Da qui, la suddivisione dell'elaborato in tre macrosezioni rispettivamente dedicate alla dimensione globale del jihadismo, con un accento specifico sul potenziale destabilizzante delle sue gemmazioni regionali e sui risvolti di inquietante "modernità" che caratterizzano il fenomeno *Islamic State*, califfato nell'era del *web;* alla sfida economico-finanziaria in un *framework* sociale pesantemente condizionato dai persistenti riverberi della crisi; alla minaccia nel cyberspazio, con una descrizione dettagliata della risposta nell'allegato Documento di Sicurezza Nazionale, come previsto dalla normativa.

Si è inteso restituire al lettore il senso di un'intelligence incline alla consuetudine con il mondo, adusa ad individuare e difendere l'interesse nazionale, che è costante nella sua essenza, ma viene variamente declinato nei suoi contenuti concreti al mutare delle contingenze storiche. Ciò perché la credibilità rimane una conquista quotidiana ed è requisito indispensabile per commisurare il livello di tutela della sicurezza nazionale alle dure prove che si profilano all'orizzonte.

…e la sfida sempre aperta: la fiducia

Ora sta all'intelligence preservare ed ulteriormente valorizzare il capitale sino ad oggi accumulato. È nelle piene condizioni di conseguire tali obiettivi: rafforzando ed arricchendo la sintonia con il Parlamento, ampliando gli spazi di interlocuzione con i cittadini e con la società civile, corroborando a tutti i livelli le ragioni della propria missione. Si tratta, in fin dei conti, di continuare a costruire, giorno dopo giorno, un sempre più solido rapporto di fiducia con il Paese.

Parte prima

JIHAD GLOBALE, *JIHAD* REGIONALE

LA MINACCIA IN OCCIDENTE

Linee di tendenza ed elementi di discontinuità

In Europa, la minaccia terroristica di matrice jihadista, attestata negli ultimi anni su livelli significativi ma stabili, nel 2014 ha fatto registrare un *trend* crescente, culminato, nel gennaio 2015, nell'attentato di Parigi al *Charlie Hebdo*, rivendicato da *al Qaida nella Penisola Arabica* (AQAP), e negli omicidi di Montrouge e Portes de Vincennes, compiuti in nome dello *Stato Islamico* (IS).

Gli eventi francesi valgono a ribadire i tratti, l'attualità e la concretezza di una minaccia che, come più volte evidenziato in precedenti Relazioni, trova il profilo di maggiore insidiosità nell'estremismo *homegrown,* un'area di consenso verso il *jihad* violento che spesso riflette processi di radicalizzazione individuali ed "invisibili".

Nel contempo, il rischio di nuovi attacchi in territorio europeo, e più in generale in Occidente, rimanda alle più recenti evoluzioni del quadro della minaccia, caratterizzato dalla progressiva affermazione dello *Stato Islamico* di al Baghdadi e dalla connessa, rivitalizzata effervescenza del *jihad* globale.

L'*appeal* dello *Stato Islamico*

L'IS, erede della filiale irachena di *al Qaida*, ha incarnato un paradigma di espansione nuovo e pervasivo, che ha visto il terrorismo cercare di "farsi Stato" e coniugare all'offensiva di tipo asimmetrico un confronto militare condotto con l'impiego di un esercito "regolare" e di armamento pesante finalizzato alla conquista e al controllo del territorio. Per certi versi, si tratta di un obiettivo strategico non dissimile da quello perseguito dal qaidismo "storico" e dai gruppi del jihadismo armato attivi lungo la dorsale di instabilità che si sviluppa dall'Africa occidentale sino al quadrante centro-asiatico, passando per la fascia nordafricana e subsahariana. Nel caso dello *Stato Islamico*, tuttavia, tale "progetto politico" ha trovato per la prima volta una traduzione concreta, sancita in giugno

con la "proclamazione" del califfato, sopravanzando l'organizzazione fondata da Bin Laden ed anzi innescando una dinamica di antagonismo all'interno della composita galassia qaidista.

A livello regionale, lo *Stato Islamico* si è inserito negli spazi creati dalla cronicizzata crisi siriana e dall'irrisolto *dossier* iracheno; ha sfruttato, anche sul piano militare, la mancanza di coesione degli avversari; ha ricercato alleanze all'interno delle tribù sunnite, sino ad imporsi quale riferimento "sovrano" e di amministrazione del territorio.

Nel contempo, il vantaggio competitivo guadagnato dalla formazione si è qualificato per la disponibilità di risorse finanziarie senza precedenti per un'organizzazione terroristica (derivanti soprattutto dall'azione predatoria ed estorsiva esercitata nelle aree controllate, dal contrabbando di greggio e dal commercio clandestino di reperti archeologici) capaci di assicurare, tra l'altro, compensi, logistica ed un equipaggiamento di prim'ordine alle proprie reclute.

La descritta traiettoria ascendente dell'organizzazione rinvia, altresì, ad una sofisticata strategia di comunicazione e propaganda, significativamente testimoniata da una copiosa produzione multimediale che spazia dal *magazine* al video-messaggio. A queste finalità risponde la diffusione *on-line* delle immagini che testimoniano le efferatezze compiute sul campo siro-iracheno, funzionale ad accreditare il ruolo-guida dello *Stato Islamico* contro i *miscredenti*, promuovendo ed alimentando un *jihad* combattente che associa pratiche militari a tecniche di guerriglia ed azioni suicide e che non manca di coltivare forme avanzate di cyberterrorismo.

Particolare dinamismo si è colto nel confronto – anch'esso giocato in larga misura sul piano mediatico – tra la formazione irachena e le componenti qaidiste "storiche", a partire dal nucleo centrale di *al Qaida* (cd. *al Qaida Core*). Già nei primi mesi del 2014, la cruenta contrapposizione sul campo siriano tra lo schieramento di al Baghdadi e le milizie di *Jabhat al Nusrah*, emanazione qaidista "legittimata" dal *leader* di *al Qaida* al Zawahiri a combattere in quel teatro, ha innescato su *blog* e *social forum* un acceso dibattito tra i sostenitori dei due fronti, profilando spaccature e, in qualche caso, defezioni a favore dello *Stato Islamico*.

Le chiamate all'azione

L'intervento militare internazionale in Siria ed in Iraq, avviato in settembre, ha offerto nuovi spunti alla narrativa jihadista, focalizzata sulla necessità di far convergere le forze islamiste in un'azione comune contro la coalizione degli "invasori" e sulla produzione di messaggi di natura istigatoria allo scopo di esercitare un'incalzante pressione intimidatoria nei confronti dei Paesi "nemici", specie occidentali. Significativi tra l'altro: l'appello all'unità sottoscritto a metà settembre da *al Qaida nel Maghreb Islamico* (AQMI) e da AQAP, che hanno offerto all'IS una sorta di patto di alleanza contro

la *diabolica coalizione;* il messaggio audio diffuso *on-line* il 21 settembre, nel quale il portavoce dell'IS al Adnani esorta i *mujahidin* sparsi nel mondo, soprattutto nei Paesi occidentali, a colpire *gli infedeli* con qualunque mezzo disponibile; il messaggio minatorio antioccidentale postato in rete a fine settembre dal *leader* di *Jabhat al Nusrah*, Abu Mohammad al Julani; il video diffuso in novembre dalla casa di produzione dello *Stato Islamico, al Hayat* (intitolato "*What are you waiting for?*"), nel quale tre combattenti francesi, dopo aver bruciato i propri passaporti, esortano i connazionali ad attivarsi; il numero 13, pubblicato il 24 dicembre, della rivista *Inspire*, curata da AQAP, nella quale si incitano all'azione i musulmani residenti nei Paesi europei; il numero 6 di *Dabiq*, periodico ufficiale dell'IS, diffuso il 28 dicembre, che in esordio si rivolge ai potenziali "lupi solitari" presenti in Europa.

La richiamata praticabilità di azioni terroristiche con gli strumenti offensivi più disparati (armi da fuoco e da taglio, ordigni fai-da-te, veleno, "*car jihad*", vale a dire autovetture lanciate contro il bersaglio, etc.), rappresenta di per sé un moltiplicatore del rischio, che accentua la possibilità di attivazioni e scie emulative da parte di soggetti più permeabili al messaggio radicale. In questa cornice si inscrivono gli attacchi in suolo occidentale registrati nel corso dell'anno (*vds. box n. 1*).

box 1

ATTENTATI DI MATRICE JIHADISTA COMPIUTI NEL 2014 IN PAESI OCCIDENTALI

Il **24 maggio**, a Bruxelles, il cittadino francese di origine algerina Mehdi Nemmouche, tornato dal teatro siriano, ha fatto irruzione nel museo ebraico della città, uccidendo quattro persone a colpi di arma da fuoco. Il **23 settembre**, a Melbourne (Australia), il diciottenne di origine afghana Numan Haider ha pugnalato due agenti dell'antiterrorismo in un commissariato dove si trovava per essere interrogato nell'ambito di un'indagine su attività terroristiche. Il **20 ottobre**, a St. Jean sur Richelieu (Canada), il convertito Martin Couture-Rouleau ha investito con un'automobile due soldati canadesi, uccidendone uno. Il **22 ottobre**, a Ottawa (Canada), il convertito Michael Zehaf Bibeau ha provocato la morte di un militare presso il *National War Memorial,* compiendo poi un attacco a mano armata all'interno del Parlamento. Il **23 ottobre**, a New York (USA), il convertito Zale Thompson ha ferito a colpi di accetta due poliziotti. Il **15 dicembre**, a Sidney (Australia), l'australiano sciita di origine iraniana Mohammad Hassan Manteghi, dichiaratamente convertito al sunnismo, armato di fucile ha preso in ostaggio una quarantina di persone in una cioccolateria, chiedendo una bandiera dello *Stato Islamico* da poter issare sul luogo. Il sequestro si è concluso il giorno successivo con un *blitz* delle Forze di polizia, nel corso del quale hanno perso la vita tre ostaggi e lo stesso sequestratore.

Foreign fighters e returnees

Agli sviluppi nel teatro siro-iracheno e alla crescente popolarità dello *Stato Islamico* presso l'uditorio estremista, sia del mondo arabo sia dei Paesi occidentali, ha corrisposto un significativo incremento del flusso di aspiranti combattenti determinati a servire la *causa* nelle file delle milizie jihadiste. Il fenomeno dei *foreign fighters*, ampiamente richiamato nella Relazione dello scorso anno, ha assunto nel 2014 dimensioni del tutto inedite, facendo ipotizzare che siano almeno tremila i *mujahidin* partiti dalla sola Europa, di cui oltre 500 provenienti dalla regione balcanica, dove operano diverse e strutturate filiere di instradamento dei volontari (*vds. box n. 2*).

La condivisione del *know-how* operativo acquisito sul campo, unitamente alla rafforzata rete di conoscenze e contatti, potrebbe accentuare in prospettiva il pericolo rappresentato da quella indefinibile percentuale di reduci che, sulla spinta di una forte motivazione ideologica e, in qualche caso, di *shock* emotivi subiti in combattimento, intendano concretizzare disegni offensivi in suolo occidentale, autonomamente ovvero su *input* di organizzazioni terroristiche operanti nei teatri di *jihad*. Nell'ottica di tali formazioni, i *foreign fighters* di matrice europea presentano, del resto, il profilo tatticamente più pagante grazie a: elevata capacità di mimetizzazione; facilità di spostamento all'interno dello spazio Schengen; utili contatti di base in Europa che possano fungere da *trait d'union* con i gruppi armati attivi nelle aree di crisi.

Per quanto riguarda l'Italia, la specifica minaccia deve essere valutata non solo per gli sporadici casi nazionali, ma anche e soprattutto tenendo presente l'eventualità di un ripiegamento sul nostro territorio di estremisti partiti per la Siria da altri Paesi europei, anche in ragione delle relazioni sviluppate sul campo tra militanti di varia nazionalità. A conferma della condivisa percezione del pericolo rappresentato dai combattenti stranieri impegnati nei teatri di *jihad*, in specie quello siro-iracheno, si pongono le iniziative assunte nei più qualificati consessi internazionali (*vds. box n. 3*).

box 2

L'ESTREMISMO ISLAMICO NEI BALCANI

La regione balcanica si conferma nodale per il radicalismo di matrice islamica, in virtù dell'incessante attivismo di soggetti e di gruppi estremisti di orientamento salafita, sempre più coinvolti nel reclutamento e nel trasferimento di jihadisti in territorio siriano ed iracheno. Particolarmente attivi in tal senso sono alcuni gruppi presenti in Albania, Bosnia-Erzegovina, FYROM, Kosovo, Montenegro e Serbia (area del Sangiaccato), che ruotano attorno a *leader* perlopiù bosniaci e di etnia albanese.

Specie in Kosovo, al di là dell'approccio radicale predicato da taluni *imam*, l'idea del *jihad* sembra allignare soprattutto in alcune aree meridionali del Paese, dove il diffuso disagio socio-economico accentua la permeabilità, specie tra i più giovani, all'azione di proselitismo di impronta salafita.

Nuove generazioni di jihadisti e *social media*

Le numerose operazioni di polizia condotte in Europa e il monitoraggio dell'intelligence fanno stato di come lo spazio comunitario risulti permeabile alle attività di proselitismo e reclutamento. Si moltiplicano, infatti, i segnali di cooptazione ideologica di aspiranti *mujahidin*, incoraggiati a raggiungere in massa, famiglie al seguito, la "nuova" patria per contribuire all'opera di *state building*. In particolare, è emersa la presenza di quella che potrebbe essere definita come una nuova generazione di

box 3

IL FENOMENO DEI *FOREIGN FIGHTERS* NEI PRINCIPALI CONSESSI MULTILATERALI

La Risoluzione del **Consiglio di Sicurezza ONU** 2178, approvata il 24 settembre 2014, definisce *foreign terrorist fighters* i "*soggetti che si recano in uno Stato diverso da quello di propria residenza/nazionalità al fine di perpetrare, pianificare, preparare o partecipare ad atti terroristici, ovvero fornire o ricevere addestramento terroristico, anche in connessione con conflitti armati*". Il documento evidenzia tra l'altro:

- la crescente minaccia rappresentata dai combattenti stranieri associati allo *Stato Islamico*, a *Jabhat al Nusrah* e ad altri gruppi affiliati o ispirati ad *al Qaida*;
- l'esigenza di rafforzare la cooperazione internazionale in materia di antiterrorismo, soprattutto attraverso maggiore *information sharing*;
- l'importanza del momento preventivo attraverso attività di contrasto all'estremismo violento e, in particolare, di sensibilizzazione delle comunità maggiormente esposte alla radicalizzazione ed al possibile reclutamento di nuovi combattenti da impiegare nei teatri di *jihad*.

Gli Stati membri sono chiamati, inoltre, a predisporre ed attuare specifiche normative volte ad impedire che cittadini o stranieri stabilmente presenti, ovvero in transito sul territorio dello Stato, possano: lasciare il Paese al fine di compiere atti di terrorismo; raccogliere fondi per finanziare i viaggi dei *foreign fighters*; offrire supporto logistico/organizzativo agli spostamenti dei combattenti diretti verso i teatri di crisi.

Nella medesima ottica, si pone l'accento sulla necessaria collaborazione degli Stati membri con le rispettive compagnie aeree nazionali, al fine di ottenere informazioni utili sugli spostamenti dei soggetti inclusi nella lista ONU degli individui e delle organizzazioni terroristiche.

Il *Memorandum de L'Aja – Marrakech sulle buone prassi per una risposta più efficace al fenomeno dei foreign terrorist fighters*, adottato in seno al ***Global CounterTerrorism Forum*** il 23 settembre e menzionato nella Risoluzione 2178, individua nei seguenti quattro campi d'azione i principali ambiti su cui concentrare l'attenzione a livello internazionale per rafforzare il contrasto

al fenomeno dei combattenti stranieri: estremismo violento; reclutamento e instradamento; capacità dei terroristi di viaggiare e loro *expertise* bellica; "reducismo". Al tempo stesso, il *Memorandum* sottolinea la necessità per gli Stati membri di adottare approcci integrati omnicomprensivi e di destinare maggiori sforzi in termini di *capacity building*.

A livello europeo, il **Consiglio dell'UE**, riunito nel formato Giustizia e Affari Interni il 4-5 dicembre, muovendo dal *Rapporto annuale sull'implementazione della Strategia UE antiterrorismo* predisposto dal *Coordinatore UE per la lotta al terrorismo*, in tema di *foreign fighters* si è focalizzato su due settori chiave: l'aggiornamento del quadro normativo e il rafforzamento dell'*information sharing*. Di rilievo, nel contesto, la richiamata proposta della Presidenza di turno italiana di adottare specifiche iniziative quali, ad esempio, la costituzione, in partenariato con l'Europol, di un *network* di punti di contatto sui *foreign fighters*.

In ambito **G7**, ove il contrasto al terrorismo internazionale è oggetto di costanti sforzi a livello politico e diplomatico, soprattutto per il tramite del Gruppo Roma/Lione, è intervenuta la dichiarazione congiunta dei Ministri degli Esteri a conclusione del *meeting* del 25 settembre, nella quale si è espressa particolare preoccupazione per la brutale violenza perpetrata dall'IS, da contrastare con un approccio omnicomprensivo che tenga soprattutto conto del massiccio flusso di combattenti stranieri e delle ingenti risorse finanziarie di cui lo *Stato Islamico* dispone.

jihadisti: molto giovani, spesso con scarse conoscenze sul piano dottrinale ma ben informati sulla pubblicistica d'area e con ottime competenze informatiche.

Proprio in riferimento all'uso del *web* quale strumento di propaganda e comunicazione, si è registrata la tendenza a privilegiare i *social network,* attraverso i quali, tra l'altro, i *foreign fighters* europei, per spronare i connazionali correligionari, alimentano un'informazione parallela ai comunicati "ufficiali" dei gruppi armati – peraltro sempre più spesso sottotitolati o tradotti in italiano – diffondendo immagini di guerra, eulogie dedicate ai *martiri* e testimonianze della loro esperienza accanto ai *fratelli* provenienti da tutto il mondo. In questo contesto, appare sempre più concreto il rischio che nel magmatico universo della messaggistica agiscano veri e propri centri di reclutamento per aspiranti jihadisti, in grado di intercettare la domanda di estremisti *homegrown* che, insoddisfatti da un impegno esclusivamente virtuale e del ruolo di meri divulgatori, aspirino a trasferirsi nel teatro siro-iracheno.

La "vecchia guardia"

Parallelamente, nei processi di radicalizzazione permane rilevante l'opera di *imam* estremisti stanziali o itineranti, latori di messaggi istigatori, se non veri e propri reclutatori, attivi specialmente in quei luoghi di aggregazione dove sia sedimentata l'eredità di trascorse gestioni d'impronta radicale. Si tratta di ambienti nei quali potrebbe ricrearsi un *humus* fertile per l'azione di sostegno logistico a estremisti, reduci, ex detenuti o militanti di movimenti messi al

bando nei rispettivi Paesi di origine. In questo senso, un profilo di attenzione riguarda il flusso di jihadisti che raggiungono il teatro siro-iracheno dai Paesi del Nord Africa ma che – per personali trascorsi in Europa, per collegamenti con soggetti residenti in territorio comunitario o per contatti maturati sul campo di battaglia – potrebbero decidere di raggiungere il nostro Continente. Questa prospettiva aumenterebbe significativamente il numero dei *returnees* e le potenziali criticità sul piano della prevenzione.

La minaccia

In relazione al quadro descritto, è da ritenersi crescente il rischio di attacchi in territorio europeo ad opera di varie "categorie" di attori esterni o interni ai Paesi-bersaglio: emissari addestrati e inviati dall'IS o da altri gruppi, compresi quelli che fanno tuttora riferimento ad *al Qaida*; cellule dormienti; *foreign fighters* di rientro o "pendolari" dal fronte *(commuters)*; familiari/amici di combattenti (donne incluse) attratti dall'"eroismo" dei propri cari, specie se *martiri*; "lupi solitari" e microgruppi che decidano di attivarsi autonomamente (*self starters).* Ciò sulla spinta anche di campagne istigatorie che ritengono pagante trasformare il Continente europeo in "terreno di confronto": con l'Occidente, in chiave di rivalsa, e tra le stesse componenti della galassia jihadista, nel quadro di dinamiche di competizione tutt'altro che univoche.

Sebbene ad oggi non siano emerse attività o pianificazioni ostili in territorio nazionale riconducibili allo *Stato Islamico* o ad altre formazioni del *jihad* globale, la minaccia interessa anche l'Italia, potenziale obiettivo di attacchi pure per la sua valenza simbolica di epicentro della cristianità evocata, di fatto, dai reiterati richiami alla *conquista di Roma* presenti nella propaganda jihadista.

Le frange curdo-turche in Italia

Criticità all'interno dei nostri confini potrebbero derivare, altresì, dal fermento manifestato dalla diaspora turco-curda presente in Italia e, in particolare, dal segmento di simpatizzanti del PKK turco, per le incursioni delle milizie dell'IS nei territori curdi in Iraq e Siria. La tensione emotiva sembra, infatti, destinata a crescere soprattutto a seguito dell'appello lanciato dal *leader* storico Ocalan – da tempo detenuto in un carcere di massima sicurezza turco – per una mobilitazione di massa contro lo *Stato Islamico*. In questo contesto, è all'attenzione informativa anche l'ipotesi che, in ritorsione per la resistenza opposta dai militanti curdi all'avanzata dei terroristi in Siria e in Iraq, esponenti della comunità curda nazionale possano essere esposti a estemporanee provocazioni/aggressioni da parte di simpatizzanti dell'IS.

Il finanziamento del terrorismo

Sul tema del finanziamento al terrorismo si è potuto osservare negli ultimi anni come, a fronte di un progressivo ridimensionamento dei

flussi di denaro provenienti da *sponsor* privati e, soprattutto, statali – sui quali, verosimilmente, ha inciso anche l'effetto deterrente prodotto dalle misure sanzionatorie imposte dalla Comunità internazionale – i gruppi terroristici abbiano dato un maggiore impulso alle forme di autofinanziamento, che si affiancano alle pratiche di raccolta fondi, operate con varie metodologie, incluse diverse e redditizie attività criminali.

In tale contesto, anche nel 2014 hanno assunto particolare valenza:

- la possibilità di ricorrere all'utilizzo strumentale di soggetti giuridici a vocazione caritatevole o ad altre attività economiche legali;
- la propaganda antioccidentale condotta dai terroristi sul *web* con l'obiettivo di raccogliere contributi dalle comunità musulmane;
- la partecipazione ad una vasta gamma di attività criminali che includono: traffico di sostanze stupefacenti; furti e rapine; sequestri di persona; estorsioni; falsificazione di documenti e valuta; frodi finanziarie; azioni predatorie sul territorio.

Sul piano interno, l'attenzione continua ad essere rivolta all'individuazione di possibili anomalie o aspetti di criticità connessi ai movimenti di denaro posti in essere da soggetti stranieri presenti in Italia e finalizzati a fornire sostegno ad organizzazioni di stampo terroristico.

A tale scopo sono stati monitorati selettivamente i sistemi di trasferimento di valuta dei circuiti internazionali ufficiali e quelli paralleli (*hawala*), le movimentazioni transfrontaliere di fondi, nonché i pagamenti internazionali effettuati nell'ambito delle attività economiche esercitate in Italia da alcuni cittadini stranieri.

In generale, appare confermata la tendenza delle organizzazioni terroristiche ad evitare l'utilizzo dei circuiti bancari convenzionali – peraltro tuttora impiegati con il ricorso a prestanome – al chiaro fine di non incorrere nel sistema dei controlli previsti dalle normative antiriciclaggio. Per quanto riguarda i sistemi alternativi di trasferimento di fondi, specifiche criticità si rilevano non soltanto in quelli operanti al di fuori dei circuiti regolamentati, ma anche nei *money transfer* regolarmente autorizzati. Tuttora utilizzato è, inoltre, il ricorso ai "corrieri di denaro", secondo modalità variabili dirette a schermare i flussi ed i soggetti coinvolti.

GLI SCENARI AFRICANI E MEDIORIENTALI

Il vasto arco di crisi che abbraccia il Nord Africa, il quadrante sahelo-sahariano e il Golfo Persico si è caratterizzato, quanto alla minaccia jihadista, per la compresenza, da un lato, di accentuati fattori di discontinuità e, dall'altro, dal protrarsi delle situazioni di instabilità già illustrate nella Relazione del 2013. L'area è stata oggetto di un articolato impegno informativo anche nell'anno trascorso, in ragione delle evoluzioni nelle singole realtà nazionali e delle relative, potenziali interazioni con variabili emergenti, quale il crollo del prezzo del petrolio intervenuto nella seconda metà del 2014.

I principali fattori di discontinuità sono da ascriversi al teatro siro-iracheno, dove, come evidenziato nel precedente paragrafo, l'autoproclamazione dello *Stato Islamico* ha conferito al terrorismo jihadista una inedita dimensione politico-statuale.

Gli elementi di continuità, sebbene relativi a scenari fra loro assai diversi per complessità e grado di impatto sulla sicurezza nazionale, sono invece riconducibili agli scacchieri nordafricano e sahelo-sahariano. Le principali organizzazioni terroristiche attive in tale vasta area (*al Qaida nel Maghreb Islamico* – AQMI, *Ansar al Shariah* – AaS, *Movimento per l'Unicità ed il Jihad in Africa Occidentale* – MUJAO, *al Mourabitoun* – AM, *al Shabaab* – AS e *Boko Haram* – BH) hanno infatti continuato a ricercare spazi di agibilità nella diffusa precarietà delle condizioni socio-economiche e di sicurezza nonché nelle difficoltà delle Autorità locali ad assicurare il controllo del territorio.

Il panorama jihadista nella sponda Sud del Mediterraneo. Le formazioni dell'area sahelo-sahariana e le crisi nell'Africa sub-sahariana

A fronte delle iniziative di contrasto, anche internazionali (si vedano i casi di Mali e Somalia), le formazioni terroristiche africane hanno affinato le proprie capacità tattiche, cercando di evitare lo scontro diret-

to con le Forze governative. Inoltre, incoraggiate dal "modello" dello *Stato Islamico* a perseguire l'obiettivo di costituire vere e proprie entità statuali – governate sulla base dei dettami coranici ed improntate alla gestione della giustizia secondo i principi della *shariah* – hanno incrementato la collaborazione interregionale anche con formazioni mediorientali, *in primis* l'egiziana *Ansar Bayt al Maqdis* (ABM) e la yemenita *al Qaida nella Penisola Arabica*. Per altro verso, si sono distinti i *leader* dell'organizzazione terroristica algerina AQMI, impegnati nella creazione di un fronte islamico comune nel Nord Africa. Quest'ultimo progetto è apparso già *in fieri* in ragione degli accordi emersi tra AQMI e AaS in Libia (AaSL) e Tunisia (AaST), organizzazioni che hanno rilanciato il *jihad* nei Paesi di origine e in quelli limitrofi e sono apparse attive nell'addestramento e nell'instradamento di combattenti verso il teatro siriano.

Tra le numerose milizie islamiche che continuano a contendersi il controllo della Libia, i gruppi terroristici riconducibili ad AaSL hanno un ruolo di rilievo. Originariamente operanti in prevalenza nel Nord del Paese (Tripolitania e Cirenaica), si sono gradualmente spinti anche in altre zone del territorio, in particolare nella regione sud-occidentale del Fezzan, che rappresenta attualmente un vero e proprio *safe haven*. In tale area, oltre ad AaSL, sono attive altre milizie a spiccata connotazione jihadista, dotate di proprie basi, strutture logistiche e campi di addestramento.

Altre due sigle hanno evidenziato una crescente proiezione offensiva verso gli Stati confinanti: la nigeriana BH, in direzione di Ciad, Niger e Camerun, e la somala AS, verso il resto del Corno d'Africa, specialmente in Kenya. La prima si è resa protagonista di un'*escalation* di violenza terroristica, culminata nell'offensiva compiuta nel gennaio 2015 nell'area di Baga (Stato di Borno), che avrebbe provocato circa duemila vittime. Nel contempo, il confronto sul terreno tra le Forze regolari nigeriane e la formazione jihadista ha portato quest'ultima a controllare una vasta porzione del Nord della Nigeria. *Al Shabaab*, dal canto suo, ha reagito alle offensive dei Contingenti internazionali ripiegando sulle aree settentrionali del Paese e a Mogadiscio, nel tentativo di riconquistare i territori perduti. Nemmeno il decesso (settembre) del suo *leader,* Mukhtar Abu Zubair, *alias* Godane, avvenuto a seguito di un'operazione antiterrorismo USA, ha indebolito il gruppo.

Infine, le formazioni africane hanno risentito dello scontro ideologico tra IS e *al Qaida Core* che, come detto, ha portato a defezioni individuali e/o di intere cellule in favore del primo, anche con forme di contagio delle cruente modalità operative adottate e pubblicizzate dal *Califfato*: in questo senso possono leggersi il rapimento e la barbara uccisione in settembre, in Cabilia, dell'escursionista francese Hervè Gourdel da parte di una frangia scissionista di AQMI denominatasi *Jund al Khilafah* (*I soldati del Califfato*).

In tale quadro di riferimento, il monitoraggio informativo ha pertanto riservato specifica attenzione alle dinamiche interne ai vari Paesi dell'area suscettibili di accrescere la portata della minaccia jihadista e di innalzare il rischio di riverberi sugli interessi nazionali.

Prioritario rilievo intelligence ha assunto la complessa situazione in **Libia**, dove il difficile processo di "*institution building*" è arretrato a causa delle profonde divisioni politiche e dell'aperta conflittualità tra le milizie riconducibili agli opposti schieramenti, soprattutto nelle aree di Tripoli e di Bengasi. Lo svolgimento di elezioni politiche (25 giugno) non ha avviato la stabilizzazione dello scenario interno, innescando, al contrario, la contrapposizione tra la nuova Camera dei Rappresentanti, insediatasi a Tobruk, e l'uscente Congresso Nazionale Generale (eletto nel 2012), con sede a Tripoli. Entrambi gli organismi istituzionali hanno rivendicato la propria legittimità ad operare, dando origine a due Esecutivi paralleli. Ad accentuare le criticità politico-istituzionali è inoltre intervenuta la sentenza della Corte Suprema Costituzionale (6 novembre) contro la legittimità della Camera dei Rappresentanti di Tobruk, che ha reso più complessa l'azione di riconciliazione promossa dall'Alto Rappresentante dell'ONU per la Libia, nonché responsabile di UNSMIL (*United Nations Support Mission in Libya*).

Assai diverso lo scenario nei Paesi vicini alla Libia. In **Tunisia**, dopo circa tre anni di tensioni interne, la fase di transizione del "dopo Ben Ali" ha registrato un significativo punto di svolta. A seguito dell'approvazione a larghissima maggioranza (26 gennaio 2014), da parte dell'Assemblea Nazionale Costituente, di una nuova Costituzione, il dialogo nazionale tra le forze politiche si è tradotto in un accordo per la formazione di un governo tecnico. Ciò nell'ottica di preparare dapprima le elezioni politiche (26 ottobre) e poi le presidenziali (23 novembre), che hanno decretato l'affermazione del partito laico *Nidaa Tounes* e del suo *leader*.

In **Marocco**, l'attenzione è stata appuntata in direzione dei fattori che hanno inciso negativamente sulla locale cornice di sicurezza, in particolare le tensioni nelle province meridionali e, soprattutto, la minaccia terroristica, alla luce anche delle numerose operazioni di polizia condotte nel Paese che hanno portato, tra l'altro, allo scompaginamento di cellule dedite al reclutamento e all'instradamento di volontari per il teatro siro-iracheno. Sono state, inoltre, monitorate le problematiche determinate dal flusso di migranti clandestini e dal traffico di stupefacenti in direzione dell'Europa.

In **Algeria**, specifico monitoraggio è stato rivolto verso i gruppi terroristici AQMI e *al Mourabitoun*, attivi nel Sud dell'Algeria, nel Nord del Mali e nel Sud-Est della Libia, da dove potrebbero mettere in atto iniziative ostili contro siti energetici ed assetti nazionali o internazionali.

In **Egitto**, è proseguita la fase di transizione con l'approvazione della nuova Costituzione, a seguito di *referendum* popolare, e la successiva modifica della legge elettorale,

propedeutica allo svolgimento delle elezioni politiche (previste nella primavera del 2015). Le consultazioni presidenziali, vinte da Abdel Fattah al Sisi con un consenso plebiscitario, hanno registrato una bassa affluenza alle urne, su cui ha inciso una diffusa disaffezione, specie delle fasce popolari più disagiate e di quelle giovanili, maggiormente colpite dagli effetti della prolungata crisi socio-economica.

Per fare fronte alla situazione, il nuovo Governo ha accelerato il piano di riforme strutturali per il rilancio dell'economia nazionale, sia attraverso il taglio dei sussidi statali sia avviando interventi nei settori delle grandi opere e dell'edilizia popolare.

Nel contempo, si è evidenziata la fermezza nei confronti della Fratellanza Musulmana (FM, già dichiarata organizzazione terroristica nel dicembre 2013), che ha comportato l'azzeramento dei suoi vertici e l'arresto di migliaia tra membri e simpatizzanti. Ciò anche in ragione dell'incremento della minaccia terroristica, riconducibile alla migrazione di affiliati della FM verso formazioni jihadiste attive specie nel Sinai, che mostrano crescenti capacità offensive, come ABM, che ha espresso adesione allo *Stato Islamico*.

L'azione di mediazione condotta da Il Cairo nella crisi israelo-palestinese, culminata nel raggiungimento del cessate il fuoco tra Israele e *Hamas* (26 agosto), rientra nel più ampio novero delle risalenti ambizioni egiziane a rivestire un ruolo primario nella regione in grado di incidere sulle dinamiche del quadrante. Nel contesto africano, si è del pari evidenziata la volontà egiziana di svolgere un ruolo più incisivo nel *dossier* relativo allo sfruttamento delle acque del Nilo, specie a seguito dell'accelerazione impressa dall'Etiopia al progetto "Grande Diga della Rinascita" lungo il tracciato del Nilo Azzurro. L'evoluzione della crisi in Libia è seguita con particolare attenzione dalle Autorità egiziane per i possibili riflessi negativi sul piano della sicurezza. Il Cairo, a tal proposito, ha espresso il proprio convinto sostegno alla Camera dei Rappresentanti riunita a Tobruk, senza interrompere, comunque, la mediazione diplomatica volta a promuovere una posizione comune fra tutti i Paesi confinanti con la Libia.

In merito alle crisi in atto nell'**Africa sub-sahariana**, sono stati oggetto di monitoraggio gli sviluppi del processo negoziale in Mali, il percorso di stabilizzazione della Somalia, l'evoluzione della situazione nel Golfo di Guinea e nella Repubblica Centrafricana, il conflitto civile in Sud Sudan e le dinamiche in Kenya.

Riguardo al **Mali**, sono proseguiti i negoziati di pace, ad Algeri, tra le Autorità di Bamako ed i diversi movimenti politico-militari separatisti delle regioni settentrionali dell'Azawad. Nonostante gli auspici iniziali, le posizioni del Governo e dei separatisti sono rimaste distanti, in quanto il primo si è dichiarato disponibile a concedere solo un maggior "decentramento" amministrativo, mentre i secondi rivendicano uno Stato dell'Azawad "federato" con il Sud Mali.

Relativamente al Corno d'Africa, in **Somalia** il Presidente, Hassan Sheikh Mohamud, è apparso determinato a riaffermare

la propria *leadership* al fine di raggiungere gli ambiziosi obiettivi fissati dal piano di ricostruzione e di riforme (la cd. *Vision 2016*), vale a dire la realizzazione dello Stato federale, la revisione costituzionale e le elezioni generali nel prossimo anno, progetto auspicato e sostenuto dalla Comunità internazionale. Le diatribe inter e intra-claniche continuano tuttavia a generare contenziosi territoriali che, interessando gran parte del territorio, ostacolano la complessa opera di riorganizzazione del Paese su base federale.

Sotto il profilo della lotta all'estremismo islamico, è rimasta elevata l'attenzione dell'intelligence nei confronti dell'organizzazione *al Shabaab*, che ha affiancato all'attivismo sul suolo somalo una intensa operatività in Kenya. All'interno della formazione è sembrata in ascesa la componente dei *foreign fighters* provenienti soprattutto dai Paesi dell'Africa Orientale, in particolare da Uganda, Tanzania e Kenya. Primario *target* informativo hanno continuato a costituire, inoltre, le dinamiche di finanziamento di *al Shabaab*, a livello sia locale che internazionale.

Anche in quest'ottica è stato oggetto di monitoraggio il fenomeno della pirateria: nonostante nel corso del 2014 sia proseguito il suo ridimensionamento, sul piano intelligence hanno mantenuto rilievo i legami diretti tra i gruppi di pirati ed *al Shabaab*, anche in considerazione dell'elevato peso economico dell'intenso traffico di navi commerciali nello stretto di Aden.

L'intensificazione delle missioni internazionali con l'impiego di unità navali nel Golfo di Aden, nell'Oceano Indiano e lungo le coste della Somalia ha comunque impedito la recrudescenza del fenomeno, rendendo spesso inefficaci gli atti di pirateria (*vds. box n.* 4).

In **Kenya**, si è assistito alla progressiva polarizzazione dei rapporti tra la maggioranza e lo schieramento dell'opposizione, in un contesto segnato dall'incremento

box 4

IL FENOMENO DELLA PIRATERIA

Nel corso del 2014 non si sono registrate catture di mercantili da parte dei pirati somali. Risultano, tuttavia, ancora sotto sequestro circa una trentina di marittimi di varie nazionalità. In maggio, undici membri dell'equipaggio della nave malese "Albedo" sono riusciti a rientrare in patria. Il 23 settembre si è conclusa positivamente anche la vicenda del giornalista statunitense Michael Scott Moore, rapito dai pirati somali a Galkayo nel gennaio 2012.

Per quanto concerne i rapporti tra i pirati ed il gruppo terroristico somalo *al Shabaab* (AS), sono stati segnalati contatti finalizzati a condurre rapimenti a scopo di estorsione ai danni di cittadini occidentali presenti a vario titolo in Somalia e nei Paesi vicini.

La Nigeria si è confermata significativamente interessata dal fenomeno. I pirati hanno preferito scegliere come obiettivo le imbarcazioni utilizzate a supporto dell'attività estrattiva petrolifera *off-shore*, abbordandole con natanti di piccole dimensioni. In tale quadro, spicca l'attacco, avvenuto nelle acque angolane nel mese di gennaio 2014, ai danni della nave "Kerala", indicativo della raggiunta capacità di pianificare e realizzare azioni ad elevata distanza dalle basi, ricorrendo a tal fine all'impiego di "navi madre".

delle azioni terroristiche, di matrice sia interna che esterna, a fronte della vasta azione di prevenzione e contrasto avviata dalle Autorità keniote a seguito dell'attacco al *Westgate* di Nairobi (21 settembre 2013), rivendicato da *al Shabaab*.

Il monitoraggio informativo si è focalizzato sulle attività terroristiche della formazione somala, specie nella Capitale keniota e lungo le coste, che negli ultimi mesi dell'anno hanno interessato strutture turistiche e progetti infrastrutturali.

Anche l'area del Golfo di Guinea è stata oggetto di un mirato esercizio di intelligence incentrato sui riflessi, soprattutto economici e di ordine pubblico, dell'epidemia di febbre emorragica Ebola nei Paesi maggiormente colpiti. In particolare, l'elevata diffusione del contagio, oltre ad avere messo a dura prova i sistemi sanitari nazionali in **Guinea**, **Liberia** e **Sierra Leone**, ha anche condotto all'adozione di misure di emergenza, quali la chiusura delle frontiere e le limitazioni ai viaggi aerei e marittimi, che a loro volta hanno prodotto serie ripercussioni sulle economie locali.

In **Burkina Faso** sono stati seguiti gli esiti dell'insurrezione armata dello scorso ottobre, che hanno comportato le dimissioni del Presidente Blaise Campaorè e l'avvio di un'Amministrazione provvisoria, inizialmente guidata dai militari e, successivamente, da Autorità civili, nel quadro della vigente Costituzione e della "Carta di transizione".

La situazione interna in **Nigeria** ha risentito del deterioramento della situazione di sicurezza nel Nord conseguente al menzionato attivismo di *Boko Haram*, responsabile, oltre che di cruenti attentati, di sequestri di persona, effettuati anche al di fuori del territorio nigeriano: in Camerun, nell'aprile 2014 sono stati rapiti due religiosi italiani, rilasciati due mesi dopo. Il movimento, pronunciatosi a favore dell'IS dichiarando, tuttavia, di sostenere anche *al Qaida* e i *Taliban*, sta evidenziando una crescente connotazione transnazionale: dalle risultanze intelligence emerge infatti che intrattiene più assidui contatti con i principali gruppi radicali islamici operanti nel Sahel, tra cui AQMI. Ciò in un contesto politico del Paese particolarmente sensibile, correlato con le dinamiche afferenti alle elezioni presidenziali (calendarizzate per il 28 marzo 2015).

Nella **Repubblica Centrafricana** è proseguito il sanguinoso conflitto tra milizie musulmane e cristiane, mentre i tentativi di avviare un processo di riconciliazione nazionale non hanno prodotto apprezzabili risultati. Per contro, sono emerse spinte autonomiste ed indipendentiste promosse dalla componente musulmana, che propugna la divisione del Paese in due entità statuali, una delle quali, quella del Nord, da porre sotto la sovranità della fazione islamica. In tale quadro, la situazione di sicurezza, nonostante timidi segnali di miglioramento, ha continuato ad evidenziare significative criticità, a fronte delle quali le missioni di *peace-keeping/peace-enforcing* presenti in area hanno profuso un importante impegno. Estremamente sensibile risulta, inoltre, la situazione umanitaria, anche in ragione dell'ingente mas-

sa di rifugiati e sfollati in fuga dalle aree teatro degli scontri.

Particolare attenzione è stata dedicata alle evoluzioni in atto nella **Repubblica del Sud Sudan** dove, grazie all'impegno della Comunità internazionale ed in particolare dell'*Intergovernmental Authority for Development* (IGAD), si sono almeno in parte attenuate le tensioni interetniche che avevano caratterizzato gli ultimi mesi del 2013 e l'inizio del 2014.

Il conflitto in "*Syrak*" e i riflessi nella regione

Per quanto riguarda la situazione in **Siria**, l'apparato di difesa e sicurezza di Damasco ha continuato a dimostrare capacità operative superiori a quelle dell'insorgenza, la cui azione ha risentito di divisioni interne, nell'ambito di un articolato scenario che ha visto lo *Stato Islamico* imporsi fra gli attori chiave della crisi. La presenza di numerosi *foreign fighters* nelle file di tale entità ha contribuito ad accrescere il livello della violenza, specie nel Nord (area di Aleppo), nella valle dell'Eufrate, nonché nel Nord-Est e nell'Est del Paese, aree dove maggiormente si è registrato l'attivismo dell'IS a discapito delle altre formazioni insorgenti, sebbene gli effetti di tale dinamismo siano stati comunque contenuti dall'azione della Coalizione internazionale. In generale, le fazioni dell'insorgenza "moderate" o comunque non ostili all'Occidente non hanno potuto incidere in maniera determinante sugli sviluppi sul terreno, nei confronti tanto delle Forze lealiste quanto dello *Stato Islamico*.

La crisi ha causato inoltre gravi implicazioni sul piano umanitario, testimoniate dalle stime delle Nazioni Unite, secondo cui sarebbero 11 milioni le persone che in Siria necessitano di aiuti.

Il regime non ha mostrato segnali di sfaldamento, rinnovando peraltro tentativi funzionali a ripristinare forme di accreditamento sul piano internazionale. Assad, dopo la riconferma alle elezioni presidenziali del 3 giugno, ha reiterato la propria disponibilità a collaborare con Stati Uniti, Regno Unito e Arabia Saudita nell'azione di contrasto all'IS. La Comunità internazionale, e in particolare l'Unione Europea, ha sostenuto dal canto suo l'iniziativa dell'ONU volta a promuovere la "de-escalation" della crisi siriana.

Relativamente al **Libano**, si è osservata una complessa dialettica fra le principali *leadership* clanico-settarie locali, divise sull'approccio agli eventi in Siria, oltre che dai problemi interni.

Uno sviluppo senz'altro positivo è rappresentato dalla formazione dell'Esecutivo, benché non sia stato possibile procedere all'elezione del Presidente della Repubblica (carica vacante dal 25 maggio 2014) e al rinnovo del Parlamento (decaduto nel giugno 2013). Al contempo, nonostante l'impegno degli attori regionali e internazionali per promuovere la sicurezza del Libano, l'involuzione della crisi siriana ha comportato un incremento della minaccia jihadista.

Permangono inoltre ulteriori rischi correlati al perdurante conflitto siriano, quali: lo *spillover* dei combattimenti; la questione

dei rifugiati siriani (circa 1,2 milioni); le difficoltà dell'economia, privata del *partner* "naturale" siriano; le infiltrazioni di elementi ed organizzazioni radicali; il contrabbando di armi ed equipaggiamenti.

Su tale sfondo si è innescata una lunga serie di attentati, taluni particolarmente efferati, perpetrati da formazioni jihadiste, perlopiù contro obiettivi militari e sciiti nella Capitale e nelle regioni orientali e settentrionali del Paese.

Sempre in Libano, la ricerca informativa è stata incentrata anche sulla raccolta di indicatori utili a monitorare la nascita e l'evoluzione di nuovi gruppi estremisti collegati a IS, in particolare nel Nord del Paese e nei campi profughi palestinesi di al Beddawi (Tripoli) ed Ayn el Helweh (Sidone).

L'attività intelligence si è inoltre sviluppata a fini di tutela del Contingente nazionale inquadrato in UNIFIL.

In **Giordania**, sebbene la monarchia mantenga il sostanziale controllo del Paese, permangono sensibilità per la precaria situazione economica nonché per i gravi riflessi delle crisi siriana ed irachena attestate, tra l'altro, dall'elevato numero di rifugiati e dall'attivismo, lungo la fascia frontaliera, di formazioni armate affiliate all'insorgenza anti-Assad, tra le quali agguerrite componenti jihadiste. Sul piano della politica interna, hanno continuato ad evidenziarsi forme di contrapposizione tra il Governo e il "Fronte di Azione Islamica" (FAI), locale espressione della Fratellanza Musulmana.

La situazione in **Iraq** si è caratterizzata per la recrudescenza delle violenze e, soprattutto, per il progressivo radicamento dello *Stato Islamico*, agevolato da varie componenti sunnite (tribali, baathiste e nazionaliste), insofferenti nei confronti della politica del *Premier* sciita al Maliki. L'organizzazione è stata in grado, dapprima, di conquistare porzioni di territorio nella Provincia occidentale di al Anbar e, successivamente, di condurre un'offensiva che ne ha esteso l'area operativa sino alla periferia di Baghdad.

Benché l'intervento della Coalizione internazionale abbia frenato l'espansione di IS, gli sviluppi dell'anno trascorso hanno esasperato le preesistenti criticità in un tessuto sociale già duramente provato, sia per la drammatica situazione umanitaria ingeneratasi a seguito degli scontri armati, sia per il diffuso senso d'insicurezza, accresciuto anche dall'incontrollata circolazione di armi tra la popolazione e dalla costituzione di gruppi armati sciiti per contrastare l'avanzata sunnita.

In tale quadro, un segnale incoraggiante sul piano politico è stata la formazione (8 settembre) del nuovo Governo, guidato dal *Premier* sciita Haider al Abadi.

Quanto allo **Yemen**, è stato monitorato il difficile processo di stabilizzazione del Paese, dove sono emerse con evidenza le perduranti criticità politico-istituzionali e di sicurezza. Le iniziative del Presidente Hadi per la pacificazione interna – che hanno dovuto misurarsi anche con le continue interferenze dell'ex Presidente Saleh – non sono riuscite a superare le resistenze dei gruppi separatisti presenti nel Sud e, soprattutto, della componente sciita-zaydita degli Houthi nel Nord, determinata ad ottenere una maggiore rap-

presentatività nella ripartizione del potere. Gli Houthi, avvalendosi di proprie milizie armate, hanno animato un teso confronto con le istituzioni, scandito da picchi di conflittualità e sfociato, nel gennaio 2015, nell'assedio di infrastrutture governative e dello stesso palazzo presidenziale.

Il gruppo terroristico AQAP continua a rappresentare nel Paese la primaria fonte di minaccia per gli interessi occidentali. Tale formazione, radicata specie nelle province meridionali, nonostante le rilevanti perdite subite in conseguenza dell'intensificazione delle operazioni militari antiterrorismo condotte dalle Forze di sicurezza yemenite nel corso dell'anno, ha continuato a dare prova di un significativo attivismo, sia attraverso la realizzazione di attacchi in danno di obiettivi governativi di Sanaa e contro gli Houthi, sia assicurando sostegno logistico e finanziario a gruppi jihadisti che operano in altri teatri di crisi, tra cui, in primo luogo, quello siriano.

In questa cornice si inscrive l'azione terroristica – riconducibile ad AQAP – perpetrata nella capitale yemenita, in prossimità dell'Accademia di Polizia (almeno 40 vittime e altre decine di feriti), lo stesso giorno dell'attentato di Parigi contro la sede di *Charlie Hebdo*, di cui, come già detto, AQAP si è successivamente attribuita la responsabilità.

Gli assetti interni al CCG

In merito ai Paesi membri del **Consiglio di Cooperazione del Golfo (CCG)**, l'attività informativa è stata rivolta al monitoraggio delle dinamiche interne a tale ambito, condizionate dalle crisi regionali in atto. Particolare rilievo hanno acquisito le frizioni tra Doha, da una parte, e Riyadh, Abu Dhabi e Manama dall'altra, culminate con il ritiro (5 marzo) dei rispettivi Ambasciatori dalle sedi diplomatiche presenti in Qatar e superate in novembre al delinearsi di rinnovate convergenze fra quei Governi. Questo sviluppo è parso indotto anche dal comune interesse di tutti i Paesi del Consiglio a mostrare sufficiente coesione di fronte alla potenziale minaccia rappresentata da IS. Nella medesima ottica è maturata la decisione di aderire, pur a diverso titolo, alla Coalizione internazionale contro le forze jihadiste attive nel teatro siro-iracheno.

La postura di Teheran

Per quanto concerne l'**Iran**, che potrebbe giocare un ruolo di sempre maggiore rilievo nel difficile contesto mediorientale, è emersa la complessità delle dinamiche interne connesse alle aspettative di promozione sociale nutrite da significativi settori dell'elettorato, alle persistenti fragilità dell'economia ed alla dialettica tra le varie componenti dell'*establishment*. In tale scenario, l'attività info-valutativa ha confermato la correlazione tra la proiezione internazionale di Teheran e le evoluzioni politiche interne, con particolare riguardo ai negoziati sul nucleare, alle crisi in Siria ed in Iraq, nonché al processo di transizione in Afghanistan.

Quanto al *dossier* nucleare, le trattative con i "5+1" finalizzate a raggiungere un

accordo definitivo nell'ambito del "Piano d'Azione congiunto" siglato nel novembre 2013 non hanno condotto alla soluzione dei punti più controversi in discussione, a partire da quello relativo alla capacità di arricchimento dell'uranio da garantire all'Iran (*vds. box n. 5*). Il termine dell'*interim deal*, fissato prima a giugno e poi a novembre 2014, è stato quindi prorogato sino alla metà del 2015.

box 5

IL *DOSSIER* NUCLEARE IRANIANO

Le trattative, dopo un promettente avvio, si sono arenate per la distanza delle posizioni su specifici aspetti del negoziato tra la Comunità internazionale e la Repubblica Islamica, quest'ultima comunque interessata a non compromettere lo sviluppo del proprio programma nucleare per usi civili. La proroga dei negoziati concordata dalle parti ha articolato il negoziato in due fasi. La prima, con scadenza fissata al 1° marzo 2015, prevede il raggiungimento di un accordo politico e la predisposizione di un *draft* consuntivo dei principali punti concordati. Entro il 30 giugno dovranno invece essere stabiliti i dettagli tecnici dell'accordo. Nel frattempo, fermo restando l'impianto sanzionatorio generale, Teheran riceverà il trasferimento rateizzato di 4,9 miliardi di dollari attualmente congelati all'estero.

I punti più controversi che sinora hanno impedito il raggiungimento di un accordo riguardano la capacità di arricchimento dell'uranio da garantire all'Iran e la revisione dell'impianto sanzionatorio da parte della Comunità internazionale. Rispetto al primo punto, il dibattito si è prevalentemente concentrato sulla quantità e tipologia delle centrifughe, sullo stoccaggio dell'uranio arricchito, sulla destinazione del reattore di Arak e dell'impianto di Fordow, nonché sulla durata dell'accordo e sul futuro della ricerca iraniana nel settore nucleare. L'obiettivo della Comunità internazionale è di rendere "innocuo" sotto il punto di vista militare il programma nucleare sviluppato sinora da Teheran, garantendone anche per il futuro la destinazione pacifica. Con riferimento al secondo aspetto, rimangono sul piatto negoziale le modalità e la tempistica relative alla revisione del regime sanzionatorio in corrispondenza dell'accettazione da parte iraniana delle limitazioni al programma nucleare.

È probabile che sull'andamento dei negoziati tra i "5+1" e l'Iran possa influire anche il difficoltoso sviluppo nelle trattative con l'Agenzia Internazionale per l'Energia Atomica (AIEA) in merito alla *Possible Military Dimension* (PMD) del programma nucleare iraniano. I colloqui sul tema, infatti, erano stati temporaneamente sospesi nel maggio 2014 a seguito della pubblicazione di un Rapporto dell'Agenzia di Vienna, in cui, pur non avendo evidenze su una possibile deriva militare del programma nucleare, si imputava a Teheran scarsa collaborazione per sciogliere i relativi dubbi. I successivi rapporti dell'Agenzia internazionale (5 settembre, 7 novembre 2014) hanno confermato la perdurante esistenza di criticità per quanto riguarda le informazioni/spiegazioni relative alla citata PMD. L'Iran, da parte sua, nega ogni addebito, definendo "totalmente infondate" le informazioni, in possesso dell'AIEA, su presunte attività di "weaponizzazione" svolte in passato.

La questione palestinese

Per quanto riguarda **Israele** e i **Territori Palestinesi** (Cisgiordania/*West Bank* e Striscia di Gaza), il 2014 ha visto un'ennesima battuta d'arresto del processo di pace e nuove spirali di violenza.

Le parti hanno dimostrato perduranti divergenze sulle questioni relative agli insediamenti israeliani nei Territori, al riconoscimento dei confini pre-1967 e al rilascio dei prigionieri palestinesi detenuti prima degli Accordi di Oslo del settembre 1993. Oltre a ciò, sui rapporti tra Tel Aviv e l'Autorità Nazionale Palestinese ha inciso la costituzione (2 giugno) del Governo di Unità Nazionale palestinese, formato da personalità "tecniche" e sostenuto sia da *Fatah* sia da *Hamas*.

Gli sviluppi politici si sono innestati su una precaria cornice di sicurezza e su un quadro socio-economico particolarmente critico tanto per la Cisgiordania quanto per la Striscia di Gaza. In particolare, nelle aree più sensibili della *West Bank* (Gerusalemme Est, Betlemme, Hebron, Jenin, Nablus, Tulkarem) si sono susseguiti scontri tra palestinesi e Forze di sicurezza israeliane, mentre è proseguita l'espansione di insediamenti approvati dal Governo Netanyahu. Nel contempo, non è venuto meno l'attivismo nella Striscia di Gaza sia dell'ala militare di *Hamas* (*Brigate Ezzedin al Qassam*), sia quello delle formazioni armate jihadiste-salafite contigue alla *Jihad Islamica Palestinese,* concretizzatosi nel reiterato lancio di razzi verso il territorio israeliano, che hanno provocato la reazione militare di Tel Aviv. La situazione si è aggravata quando elementi palestinesi hanno rapito (12 giugno) e ucciso tre giovani coloni israeliani, i cui cadaveri sono stati poi rinvenuti (30 giugno) nell'area di Hebron. L'evento ha contribuito ad alimentare il clima di tensione, sfociato in numerose sortite aeree israeliane contro obiettivi mirati ubicati a Gaza e in una vasta operazione antiterrorismo estesa a tutti i Territori, cui ha fatto seguito l'operazione militare *Protective Edge* (8 luglio – 26 agosto). Inoltre, a partire dal mese di ottobre, permane uno stato di elevatissima tensione per l'intensificazione delle violenze tra israeliani e palestinesi, specie a Gerusalemme Est, area a maggioranza araba.

Sino alla fine del 2014 le Forze di sicurezza israeliane hanno mantenuto un'attenzione elevata non solo verso Gaza, ma anche verso il Sinai egiziano, il Sud del Libano e la fascia confinaria con la Siria (Alture del Golan). Ciò in considerazione dell'estrema instabilità regionale e dell'accresciuta presenza nell'area di micro-formazioni contigue all'ideologia qaidista e sunno-salafita, in larga parte connesse con l'insorgenza siriana.

VECCHIE E NUOVE FRONTIERE DEL *JIHAD*

La regione "*Af-Pak*": *al Qaida Core*, realtà talebane e istanze etnico-tribali

La matrice *Taliban* ha continuato a contrassegnare l'attività insorgente sia in **Afghanistan** sia in **Pakistan**, tentando di trarre massimo profitto dalla rimodulazione della missione ISAF.

In Afghanistan, l'ala oltranzista del movimento ha prevalso su quella più disponibile al dialogo, determinando la sostituzione di tutti i comandanti dissidenti. La cornice di sicurezza afghana è stata dunque indebolita dall'incessante offensiva *Taliban*, non più limitata ad attacchi del genere "mordi e fuggi", ma apertamente orientata allo scontro diretto con le Forze di sicurezza locali per la conquista di porzioni di territorio. Queste ultime, meglio addestrate rispetto al passato, hanno assicurato con il sostegno di ISAF il presidio dei principali centri urbani.

La *leadership* del *Mullah* Akhtar Mansour della tribù Ishaqzai, nominato capo della struttura militare del movimento *Taliban* insieme al *Mullah* Hotak (fratello del *leader* storico dell'organizzazione, il *Mullah* Omar), ha trovato sostegno e legittimazione anche presso elementi di spicco di altre tribù, in particolare degli Alizai, fortemente radicati nella catena di comando e controllo delle province occidentali del Paese ed in passato apertamente in contrasto con gli Ishaqzai.

A seguito degli eventi siro-iracheni, è emerso come l'organizzazione dello *Stato Islamico* guardi anche alla regione "*Af-Pak*" quale bacino per attività di reclutamento e per la realizzazione di basi logistiche, al fine ultimo di estendere la propria influenza dal Medio Oriente all'Asia centro-meridionale.

L'azione intelligence è stata diretta alla prevenzione delle azioni ostili contro sedi diplomatiche e Forze della Coalizione internazionale, nonché a danno di simboli ed interessi occidentali, talora poste in essere da elementi infiltrati (cd. *insider attacker*). Il

5 agosto si è registrato il più grave di tali episodi, un attacco perpetrato da un elemento *Taliban* che indossava l'uniforme delle Forze di difesa e sicurezza afghane, nel quale sono rimasti uccisi 13 militari statunitensi.

Specifica attenzione è stata riservata alla cornice di sicurezza nel *Regional Command West* (RC-W), sede del Contingente nazionale, dove il livello di minaccia, con il progressivo ridimensionamento della missione internazionale denominata *Train Advise and Assist Command-West* (TAAC-West), permane elevato per la presenza di consistenti forze insorgenti ed il conseguente rischio di attacchi condotti con lancio di razzi o con l'impiego di ordigni esplosivi artigianali (IED). Nell'area, in aggiunta ai militanti *Taliban*, è emerso il rinnovato attivismo di un'altra componente "storica" dell'insorgenza rappresentata dalla cd. *rete Haqqani*, come pure di estremisti provenienti dal Pakistan. Continua altresì a registrarsi una significativa operatività di gruppi jihadisti riconducibili per lo più alla guerriglia *Taliban* e al partito radicale *pashtun Hezb-i Islami*.

Peraltro, nel 2014, la dialettica tra le principali etnie afghane (i *pashtun*, i tagiki, gli *hazara* e, in misura minore, gli uzbeki), si è sviluppata principalmente nel dibattito politico per la "corsa" dei rispettivi *leader* alla Presidenza della Repubblica e nella contrapposizione tra *power-broker* locali, intenzionati a preservare la propria influenza; ciò in uno scenario interno gravato da incognite anche sotto il profilo economico (*vds. box n. 6*).

box 6

AFGHANISTAN. PROSPETTIVE DI SOSTENIBILITÀ ECONOMICA E FISCALE

Le incertezze derivanti dall'ingresso dell'Afghanistan in una delicata fase di transizione politica e di sicurezza hanno determinato un sensibile rallentamento della *performance* economica del Paese, acuito da una crisi finanziaria che ha messo a repentaglio la copertura del fabbisogno di bilancio per il 2014. Il riordino delle procedure di raccolta fiscale (a fronte di un gettito che ha registrato nel 2014 il terzo calo annuale consecutivo) e l'allargamento della base imponibile di riferimento potrebbero invertire tale tendenza, a condizione che vi sia una ripresa della crescita economica. Per il momento le premesse di un nuovo ciclo di sviluppo rimangono fragili, essendo limitate quasi esclusivamente alla sfera dei servizi (che, allo stato, genera circa il 50% del PIL) e l'economia del Paese è destinata a restare dipendente dall'aiuto internazionale (verosimilmente per oltre il 40%).

In una prospettiva di più lungo termine, effetti virtuosi sulla dinamica del ciclo economico potranno scaturire da un'adeguata valorizzazione delle potenzialità dei comparti agricolo, minerario ed energetico.

Sono necessari, a tal fine, il consolidamento della cornice di sicurezza, l'adozione di un quadro normativo in grado di tutelare gli operatori stranieri e la sicurezza degli Investimenti Diretti Esteri (IDE), nonché, anche in una prospettiva di incremento delle aree coltivabili e arabili, iniziative volte a promuovere la riconversione delle piantagioni di oppio.

Il rischio di un repentino ritorno alla polarizzazione etnica che aveva caratteriz-

zato il conflitto civile degli anni Novanta è stato scongiurato, grazie all'accordo raggiunto alla fine di settembre per la formazione di un Governo inclusivo di rappresentanti degli opposti schieramenti.

Più in generale, risulta in aumento nel Paese l'afflusso di militanti stranieri provenienti soprattutto dal Pakistan e, in particolare, dai cd. "Territori Tribali" (*Federally Administered Tribal Areas* – F.A.T.A.), che continuano a costituire un *safe haven* per i gruppi jihadisti, essendo ancora in larga parte al di fuori del controllo delle Forze di sicurezza pakistane.

Proprio in ritorsione ad un'offensiva lanciata in quell'area sembra porsi il drammatico eccidio (16 dicembre) compiuto in una scuola pubblica di Peshawar frequentata dai figli di militari dell'Esercito pakistano, rivendicato dalla formazione *Tehreek-e-Taliban Pakistan*, che ha provocato oltre 130 vittime.

Gli equilibri in Asia Centrale

L'Asia Centrale costituisce oggetto di interesse informativo per il suo peculiare profilo geopolitico e per la considerevole disponibilità di risorse energetiche, che appare evidente alla luce della crescente competizione di vari attori internazionali interessati ad ottenere il diritto al loro sfruttamento.

Si tratta di un'area caratterizzata da diverse criticità, quali la mancata risoluzione in ambito regionale dell'annosa questione della gestione delle risorse idriche comuni, peraltro in progressiva riduzione, la presenza di contenziosi confinari (frontiere tagiko-uzbeka e uzbeko-kirghiza) che sfociano periodicamente in incidenti ed acuiscono il livello di instabilità nella regione e, infine, l'attivismo della criminalità organizzata, agevolata dalla porosità delle frontiere. La permeabilità dei confini (1.300 km) che il Tagikistan condivide con l'Afghanistan consente, inoltre, il transito nella regione di miliziani provenienti dall'area afghano-pakistana.

Si registra inoltre l'intensificazione delle attività delle organizzazioni terroristiche *Islamic Movement of Uzbekistan* (IMU), *Hizb-ut-Tahrir* (HuT), *Islamic Jihad Union* (IJU) e il *Movimento Islamico del Turkestan Orientale* (ETIM), attive prevalentemente nella Valle di Ferghana (area a prevalenza uzbeka, ma condivisa con Kirghizstan e Tagikistan).

AQIS e il *jihad* in Sud Asia

Il *leader* di *al Qaida Core*, al Zawahiri, rivolgendosi nel settembre scorso alle popolazioni musulmane del subcontinente indiano e del Sud-Est asiatico, ha richiamato le locali comunità islamiche all'unità ed annunciato la costituzione di una nuova branca dell'organizzazione da lui diretta, denominata *al Qaida in Indian Subcontinent* (AQIS).

L'iniziativa va ricollegata al richiamato interesse manifestato dallo *Stato Islamico* per la regione asiatica centro-meridionale ed alla concreta possibilità che componenti di rilievo dell'insorgenza afghana sviluppino una progressiva gravitazione in direzione dell'IS, mettendo così in discussione l'azione di *patronage* tradizionalmente eser-

citata da *al Qaida* sulle organizzazioni jihadiste del quadrante "*Af-Pak*".

Analogo dinamismo si coglie nei Paesi del Sud-Est asiatico, dove accanto a formazioni jihadiste storiche, di ispirazione salafita e tradizionalmente riconducibili all'ideologia qaidista quali *Abu Sayyaf*, sono andati emergendo – soprattutto in Indonesia e Malesia – gruppi sensibili ai richiami dell'IS.

Malgrado ciò, al pari di altri contesti jihadisti, l'unitarietà nella *battaglia contro l'Occidente* sembrerebbe prevalere anche qui sulla logica di competizione, profilando un innalzamento della minaccia terroristica nell'intero quadrante asiatico.

Parte seconda

LA SFIDA ECO-FIN E IL *FRAMEWORK* SOCIALE

LE MINACCE ALL'ECONOMIA

La congiuntura

L'attività informativa si è sviluppata in uno scenario caratterizzato dal perdurare della fase recessiva e da un andamento del livello medio generale dei prezzi che è arrivato a presentare segnali deflattivi. In particolare, nel terzo trimestre 2014 il Prodotto Interno Lordo (PIL) è diminuito dello 0,1% rispetto al trimestre precedente. In agosto, settembre e dicembre 2014 l'inflazione è divenuta negativa, anche se la variazione dei prezzi sui dodici mesi è rimasta complessivamente positiva, seppur in maniera estremamente contenuta (*vds. Banca d'Italia, Bollettino economico n. 1 gennaio 2015 – ISTAT, Conti nazionali*).

Nel terzo trimestre 2014, e rispetto allo stesso periodo del 2013, i consumi interni sono aumentati dello 0,4%, mentre gli investimenti fissi lordi sono scesi del 3,1%; le importazioni sono diminuite dello 0,7%, mentre le esportazioni sono aumentate dell'1,3%. La produzione industriale, nella media dei primi dieci mesi dell'anno, è scesa dello 0,8% rispetto allo stesso periodo dell'anno precedente. È rimasto elevato il tasso di disoccupazione che, ad ottobre 2014, era pari al 13,2%, contro il 10% medio dell'Unione Europea a 28 (*vds. ISTAT, Rilevazione sulle forze di lavoro*). Particolarmente colpita è la fascia di età compresa tra i 15 e i 24 anni, che registra un tasso di disoccupazione pari al 43,3% (in aumento dell'1,9% rispetto al 2013).

Parimenti, la debolezza congiunturale ha condotto ad una revisione del profilo temporale del riequilibrio dei conti pubblici, con il posticipo al 2017 del raggiungimento del pareggio di bilancio in termini strutturali. Il rapporto debito/PIL, prossimo al 132% nel 2014, il rapporto deficit/PIL al 3% e l'oneroso piano di ammortamento del debito hanno dunque lasciato il Paese esposto alle turbolenze dei mercati finanziari. Ciò pur

nella sostanziale tenuta del differenziale del valore dei titoli del debito rispetto a quello di riferimento in Europa.

Gli investimenti esteri: depotenziare i rischi e cogliere le opportunità. Strumenti normativi ed attività informativa

A fronte di una diffusa incertezza sull'andamento della domanda interna, la capacità di attrarre investimenti esteri si è confermata come una importante leva di crescita, soprattutto per un Paese quale l'Italia, che presenta ampie opportunità di investimento. L'afflusso di capitali stranieri rappresenta, infatti, un fattore moltiplicatore per la competitività delle imprese nei mercati internazionali (*vds. box n. 7*), specie quando si coniuga con competenze e soluzioni tecnologiche innovative.

Nel corso del 2014, l'attività degli Organismi informativi, in coerenza con la linea d'azione illustrata nelle Relazioni degli scorsi anni, ha mirato a garantire il supporto intelligence utile alla salvaguardia di quelle dinamiche di mercato che favoriscono l'efficienza produttiva e allocativa. Ciò al fine di assicurare continuità alla tutela degli assetti strategici nazionali nei confronti di manovre acquisitive che sottendono a finalità sostanzialmente predatorie, con l'obiettivo di sottrarre tecnologie e *know-how* industriale e commerciale, essenziali per la competitività del sistema Italia, a detrimento delle prospettive di sviluppo e dei livelli occupazionali delle im-

box 7

LA CONCORRENZA FISCALE INTERNAZIONALE E PAESI DI PROSSIMA ADESIONE ALL'UE

I flussi di IDE in Italia, promossi da recenti misure normative nazionali, potrebbero risentire, peraltro, della concorrenza fiscale di quei Paesi interessati ad aderire all'Unione e particolarmente impegnati nell'attrazione di capitali mediorientali ed asiatici. Mentre nel caso di Stati già membri dell'UE la Commissione Europea dispone di leve di intervento (politico ed amministrativo) per evitare l'adozione di normative fiscali non in linea con il Diritto Comunitario Europeo, negli Stati extracomunitari sussistono regimi fiscali che, se da un lato possono agevolare le rispettive economie nel conseguire, nel tempo, i requisiti economici necessari per l'accesso nell'UE, dall'altro possono, nell'immediato, fornire alle stesse realtà nazionali vantaggi competitivi per promuovere rapporti di favore con attori economici di Medio Oriente ed Asia.

prese italiane *target*, per lo più PMI colpite dal lungo ciclo recessivo.

In una logica di supporto informativo ai fini dell'adozione di strumenti interdittivi, disciplinati dalla legge 11 maggio 2012, n. 56 sul cd. *golden power* (integrata nel 2014 con diversi provvedimenti sulle attività da tutelare e sulle relative procedure, *vds. box n. 8*), l'azione intelligence è stata principalmente indirizzata al monitoraggio di:

- partecipazioni al capitale sociale di società nazionali, con particolare riguardo ai mutamenti nei rapporti di *governance* e nelle linee di politica aziendale suscettibili di arrecare pregiudizio agli interessi nazionali;
- acquisizioni da parte di compagini societarie estere poco trasparenti, tali da implicare possibili forme di condizionamento o destabilizzazione della normale gestione aziendale;
- trasferimenti oltre confine dei centri decisionali di imprese italiane, nonché delocalizzazioni totali o parziali della produzione, con i connessi riflessi occupazionali e di deindustrializzazione del tessuto economico.

Sono stati in particolare, oggetto di attività informativa:

- l'interesse da parte di gruppi economici stranieri verso i comparti della meccanica e dei materiali plastici utilizzati nelle filiere dell'elettronica industriale; della logistica portuale, con finalità di controllo dei flussi commerciali; dell'agroalimentare, con possibile impatto sui

box 8

APPLICAZIONE DELLA *GOLDEN POWER*

Per quel che concerne la normativa attuativa della legge 56/2012, si evidenzia che sono stati emanati/adottati:

- il DPCM 108/2014, afferente alle attività di rilevanza strategica ed alle attività strategiche chiave nei settori della difesa e della sicurezza di competenza del Ministero della Difesa e del Ministero dell'Interno;
- il DPR 35/2014, che stabilisce le procedure per l'esercizio dei poteri speciali nei settori della difesa e della sicurezza;
- il DPR 85/2014, concernente gli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni;
- il DPR 86/2014, che individua le procedure per l'attivazione dei poteri speciali nei settori dell'energia, dei trasporti e delle comunicazioni.

canali di approvvigionamento delle materie prime;

- gli investimenti esteri verso i segmenti delle infrastrutture (energetiche, trasporti e telecomunicazioni), dell'industria aerospaziale, del *real estate* e finanziario, relativamente ad operazioni di soggetti mediorientali ed asiatici (inclusi taluni Fondi Sovrani) orientati a diversificare il proprio portafoglio di investimenti;
- le dinamiche competitive sui mercati emergenti di rilevanza strategica di America Latina ed Africa, nei quali si confrontano primari investitori istituzionali esteri – anzitutto Fondi Sovrani e società di Stato – ed attori nazionali tradizionalmente presenti in quei contesti;
- le *joint venture* finalizzate ad attuare investimenti congiunti all'estero in settori ad alta tecnologia – in particolare nei segmenti dell'energia e delle comunicazioni – suscettibili di comportare la perdita di *know-how* a beneficio del socio straniero, agevolandolo nell'accesso ai mercati.

L'attività intelligence a tutela degli assetti strategici nazionali si è sviluppata, altresì, sul terreno del controspionaggio, in relazione ai tentativi di indebita ingerenza a fini informativi in settori sensibili del sistema produttivo nazionale, specie nel settore scientifico (*vds. box n. 9*).

box 9

LO SPIONAGGIO INDUSTRIALE

L'attività occulta tesa all'acquisizione di segreti industriali e di proprietà intellettuale è un fenomeno in forte espansione in tutto il mondo e, come si dirà più avanti, sempre più frequentemente condotto nello spazio cibernetico. Considerata l'intensa competizione in atto tra i sistemi Paese per il controllo di tecnologie chiave, questa minaccia è suscettibile di insidiare la supremazia degli Stati ad economia più avanzata e, tra questi, certamente anche l'Italia.

Diversi sono gli attori, statuali e non, che possono rendersi autori di pratiche di spionaggio industriale: si spazia dalle imprese interessate ad acquisire il *know-how* dei propri *competitor*, spesso avvalendosi di impiegati infedeli e/o insoddisfatti (cd. fenomeno dell'*insider threat*), alle strutture private dedite a un vero e proprio "commercio di informazioni".

Rilevante è il ruolo svolto da Servizi d'intelligence stranieri, che mirano ad acquisire segreti industriali e scientifici al fine di rendere maggiormente competitive le realtà produttive dei Paesi di riferimento sui mercati, risparmiando sulle ingenti risorse pubbliche necessarie a finanziare le attività di ricerca e sviluppo (R&S). Per tale motivo, non sorprende il fatto che taluni Organismi informativi abbiano nel tempo implementato le attività per l'acquisizione di segreti ed informazioni sensibili attraverso metodologie operative quali manovre di selezione, avvicinamento, coltivazione e reclutamento di fonti umane, nonché di intercettazione e di intrusioni telematiche.

Da non trascurare, infine, il ruolo di esperti informatici che possono agire autonomamente o al servizio di uno o più degli attori citati.

Gli obiettivi delle attività di spionaggio industriale sono normalmente strutture pubbliche e private coinvolte in costose attività di R&S, ovvero che operano in settori strategici e *high-tech*. Costituiscono *target* privilegiato le tecnologie dell'informazione e delle telecomunicazioni, quelle militari (aerospaziali, aeronautiche e dei sistemi marittimi), energetiche (soluzioni a bassa emissione di anidride carbonica), dei nuovi materiali (tecnologie manifatturiere e nanotecnologie), biomedicali e farmaceutiche, di ingegneria genetica.

La sicurezza energetica quale presupposto della crescita: diversificazione delle fonti di approvvigionamento e tutela delle infrastrutture nazionali

In una realtà, quale quella italiana, caratterizzata da dipendenza energetica, l'impegno dell'intelligence si è proposto di assicurare il necessario supporto informativo e valutativo alle linee d'azione governative volte a garantire la continuità e l'economicità dei flussi di idrocarburi. Requisiti, questi, imprescindibili per promuovere competitività, crescita economica ed occupazione.

In tale contesto, la ricerca informativa delle Agenzie si è concentrata sulle possibili minacce ai principali canali d'approvvigionamento di idrocarburi, con particolare riguardo ai flussi provenienti dal Nord Africa, dal Medio Oriente e dalla Federazione Russa, via Ucraina. Anche sotto questa visuale si è sviluppato il monitoraggio intelligence della crisi ucraina (*vds. box n. 10*).

box 10

LA CRISI UCRAINA

Sviluppatasi a partire dal novembre 2013 con la decisione dell'ex Presidente Yanukovich di non sottoscrivere gli accordi politico-economici con l'Unione Europea, la crisi ucraina ha rappresentato, dopo quella georgiana del 2008, il più serio confronto tra Russia ed Occidente sul terreno europeo dai tempi della guerra fredda.

Dopo la destituzione (22 febbraio) di Yanukovich e l'insediamento di un Esecutivo di transizione, guidato dal *leader* dell'opposizione, Arseniy Yatsenyuk, un ulteriore fronte si è aperto nella Penisola di Crimea, dove la popolazione, con un *referendum* (16 marzo), ha espresso, a larga maggioranza, la volontà di adesione alla Federazione Russa. All'esito di ciò, il 18 marzo, Vladimir Putin ha firmato il decreto che ha reso la Crimea un nuovo soggetto della Federazione. A partire da aprile, per contrastare i focolai di scontro diffusisi nelle regioni orientali del Paese, le Forze di sicurezza ucraine hanno avviato un'operazione militare contro i separatisti filorussi di Luhansk e di Donetsk, non riuscendo, tuttavia, a riportare sotto il controllo di Kiev molte località del bacino del Donbass. L'elezione, con il 54% dei suffragi, di un nuovo Presidente della Repubblica, l'imprenditore Petro Poroshenko (insediatosi il 7 giugno), ha aperto nei rapporti tra Mosca e Kiev una nuova fase, caratterizzata dall'avvio di colloqui di pace, cui hanno partecipato rappresentanti di Russia, Ucraina, OSCE e del separatismo ucraino, e sfociata nell'accordo di *cessate-il-fuoco* siglato tra le parti il 5 settembre a Minsk (che prevede la demarcazione di una "linea di contatto" e di una "zona cuscinetto").

Gli ulteriori sviluppi politici ucraini hanno visto la celebrazione (26 ottobre) delle elezioni parlamentari anticipate – cui non hanno preso parte le regioni separatiste – vinte dai due partiti di Governo (filoeuropeisti e antirussi) guidati dagli alleati Petro Poroshenko e Arseniy Yatsenyuk. Il primo ("Blocco Poroshenko") ha ottenuto il 21,82% dei voti; il secondo ("Fronte Popolare") il 22,14%. Il "Blocco delle Opposizioni", l'unico partito di opposizione, contrario alla scelta europeista dell'Esecutivo, ha sfiorato il 10% dei consensi. Alle elezioni, peraltro, ha votato solo il 52,42% degli aventi diritto, dato che rivela le profonde divisioni presenti nell'ambito del Paese.

A fronte di tale situazione, la Commissione UE ha emanato sanzioni settoriali contro la Federazione Russa che prevedono la restrizione all'esportazione di beni *dual-use* e materiali/servizi per attività di prospezione petrolifera, il divieto all'*export* di armi, restrizioni sull'accesso al mercato dei capitali e specifiche misure di congelamento sul territorio nazionale di beni/attività riferiti a soggetti/enti listati.

Gli approvvigionamenti dalla Libia

Gli effetti derivati dall'instabilità della Libia, fra i principali fornitori dell'Italia nel settore degli idrocarburi, sulla continuità dei flussi hanno continuato a sollecitare un attento presidio informativo ed un costante esercizio analitico da parte degli Organismi di intelligence.

Nel 2014, l'afflusso di gas verso il nostro Paese si è dipanato, a causa delle continue chiusure di terminali libici, nel segno della discontinuità verificatasi dopo la sollevazione del 2011.

In una fase di profonde mutazioni nel mercato globale petrolifero e del correlato impatto sotto il profilo degli equilibri geopolitici e macroeconomici, l'interesse nazionale alla continuità dei flussi libici permane prioritario. Al di là delle pur rilevanti dinamiche sviluppatesi con l'acuirsi della crisi russo-ucraina, tanto sulle forniture quanto sugli investimenti incisi dal quadro sanzionatorio, vale sottolineare come il rapporto con il Paese nordafricano rimanga centrale per la concorrenza di fattori strutturali: prossimità geografica, entità degli investimenti nazionali cui sono derivate rendite di posizione e aspettative di continuità sul piano contrattuale, operatività di dotti che collegano le nostre sponde (gasdotto *Greenstream*).

A livello europeo, anche sulla spinta della crisi ucraina, si è ulteriormente consolidata la tendenza della UE a porsi quale attore unitario nel perseguimento di politiche volte, da un lato, allo sviluppo della produzione interna di idrocarburi (Mar Mediterraneo, Mare del Nord e Mar Nero) e, dall'altro, all'ampliamento del novero dei fornitori, con particolare attenzione alle progettualità in corso in America settentrionale, in Africa, nel Caucaso meridionale ed in Australia.

Con riferimento alla tipologia dei prodotti energetici, si è valutato che, nel medio periodo, la combinazione tra l'incremento della produzione australiana e statunitense

di gas naturale e la progressiva contrazione della domanda da parte del Giappone potrebbe rendere nuovamente appetibile il mercato europeo del gas naturale liquefatto (GNL). Ciò in un quadro che deve, tuttavia, tenere conto della richiamata caduta dei corsi petroliferi, che sta incidendo negativamente sullo sviluppo del GNL.

In ogni caso, la possibilità di attingere gas naturale da un più ampio ventaglio di fornitori avrebbe un impatto positivo sul processo di interconnessione energetica europea, poiché si attenuerebbe l'attuale elevato livello di vulnerabilità sistemica e si ridurrebbe, al contempo, il differenziale di prezzo tuttora esistente tra i Paesi dell'Unione. Lo sviluppo di un *network* integrato, tra l'altro, renderebbe maggiormente strategico e vantaggioso il ruolo dei rigassificatori e, più in generale, degli stoccaggi, consentendo ai consumatori di accrescere il peso della componente "spot", valorizzata ai prezzi correnti di mercato, rispetto ai contratti di fornitura di lungo periodo, sin qui prevalentemente negoziati con la formula *take or pay*.

Le economie illegali: evasione ed elusione fiscale, occultamento e trasferimento all'estero di capitali

Negli ultimi anni sono state numerose le iniziative in ambito multilaterale (OCSE, UE, G20) volte a contrastare il trasferimento di capitali nei paradisi fiscali, a rafforzare la cooperazione amministrativa – non solo "su richiesta" da parte dell'Autorità interessata ma anche su base "spontanea" e "automatica" – e ad incrementare il livello di trasparenza tributaria. In tale quadro si è registrata, a livello internazionale, una convergente, intensificata attenzione verso il contrasto al trasferimento di profitti in Paesi a regimi privilegiati (*profit shifting*) e lo sfruttamento improprio delle asimmetrie tra le diverse legislazioni (*vds. box n. 11*).

In un contesto di più convergente pressione internazionale, le strategie sottostanti le operazioni di evasione ed elusione fiscale vanno connotandosi secondo accresciu-

box 11

COOPERAZIONE INTERNAZIONALE E DOPPIA IMPOSIZIONE

Consapevole della rilevanza strategica della cooperazione internazionale quale strumento privilegiato di contrasto alla fuga di capitali per motivi fiscali, l'Italia ha siglato nel 2012, congiuntamente a Francia, Germania, Spagna, Regno Unito e Stati Uniti, il *Foreign Account Tax Compliance Act* (FATCA), per la *compliance* fiscale internazionale automatica e l'applicazione di una legislazione concordata.

Al fine di arginare l'uso improprio della normativa tributaria, l'Italia ha inoltre recentemente ampliato la lista dei Paesi con cui ha siglato accordi bilaterali contro la doppia imposizione e a favore dello scambio di informazioni secondo lo standard OCSE (tra i firmatari si annoverano Cipro, Federazione Russa, Malta, Singapore, San Marino, Corea del Sud, Hong Kong, Lussemburgo, Messico, Bermuda, Cayman, Isole Cook, Gibilterra, Isola di Man).

ti livelli di sofisticazione. Ciò ha richiesto la ricerca di ulteriori margini di efficacia dell'azione di contrasto e di collaborazione interstatuale, così come, all'interno del Paese, fra le singole Amministrazioni preposte alla constatazione e all'accertamento delle attività fraudolente e dei proventi sottratti al gettito tributario.

Su tale aspetto, l'attività intelligence è stata prioritariamente indirizzata all'individuazione di condotte pregiudizievoli per gli interessi erariali poste in essere, o comunque destinate a svilupparsi, in tutto o in parte, in territorio estero. Si è confermata la persistenza di tali fenomeni, riconducibili nella loro fase attuativa a modalità operative attuate nel campo sia delle imposte dirette che di quelle indirette.

Peraltro, le risultanze informative evidenziano l'esigenza di continuare ad assicurare adeguato monitoraggio dei flussi da e con l'estero rilevanti ai fini doganali, rispetto ai quali hanno assunto preminente rilievo le condotte finalizzate all'introduzione fraudolenta nel territorio nazionale di merce di varia natura, specie di provenienza asiatica, con ricadute sul regolare esercizio della concorrenza, sul corretto andamento dei mercati, sulla sicurezza e sulla salute pubblica.

Le operazioni di costituzione e di trasferimento di risorse finanziarie oltre confine hanno presentato una stretta connessione con attività rilevanti sul piano fiscale, in quanto espressive di condotte evasive. Non sono tuttavia mancate fattispecie motivate da ragioni diverse da quelle tributarie, come l'interesse a poter disporre, all'estero, di capitali frutto di altri comportamenti illeciti, quale è il caso dei proventi di attività truffaldine compiute a danno di banche o fornitori. Si è potuta inoltre constatare l'introduzione di nuove tecniche per il rimpatrio e il reimpiego sul territorio nazionale di capitali di origine illecita detenuti all'estero.

Il rischio economico e la stabilità del sistema bancario e finanziario

Al di là delle implicazioni in termini di minori entrate erariali, tali operazioni determinano comunque un deflusso di liquidità che va a detrimento di un mercato già fortemente condizionato dalla stretta creditizia.

Va peraltro sottolineato che la caduta dei prestiti alle imprese nel 2014 è stata più lenta che negli anni precedenti. Ciò anche grazie al pagamento delle *tranche* di arretrati della PA, usate in parte per ridurre l'esposizione bancaria.

Dal consolidarsi di tale tendenza potrà proficuamente derivare un più pronunciato dinamismo del sistema creditizio italiano nei mercati finanziari internazionali, unitamente ad una maggiore attrattività delle nostre banche rispetto ad eventuali investitori esteri interessati ad entrare nel loro azionariato.

Riguardo a tale aspetto, persiste la necessità di salvaguardare tanto l'oggettività delle procedure di affidamento degli istituti di credito, quanto la rispondenza alle condizioni di mercato delle relazioni creditizie con le imprese partecipanti.

Nella medesima ottica di tutela, in relazione alle operazioni di ricapitalizzazione connesse all'introduzione del meccanismo di Vigilanza Unica, l'analisi intelligence si è focalizzata sulle mire espansionistiche di *player* esteri interessati a capitalizzare la vulnerabilità degli assetti azionari.

Nel corso del 2014, è altresì proseguito il monitoraggio dell'utilizzo sia delle criptovalute (*bitcoin*), in considerazione dei profili di rischio legati alla scarsa tracciabilità delle transazioni e all'opacità di alcuni operatori, sia delle cd. valute complementari (es. SARDEX). Queste, pur offrendo opportunità per lo sviluppo dei territori, sono suscettibili di profilare criticità sul piano tributario, a causa della difficile determinazione della base imponibile relativa alle operazioni di compravendita e di scambio commerciale.

Il crimine organizzato nel tessuto economico-produttivo nazionale: strategie affaristiche

Sul piano interno, il perdurare della crisi ha consentito alle organizzazioni criminali autoctone di rafforzare la propria presenza sui mercati mediante ingenti liquidità di natura illecita, favorendo l'acquisizione di attività imprenditoriali in difficoltà ed il consolidamento della *leadership* delle aziende già a guida mafiosa nei diversi settori dell'economia legale.

Per raggiungere tali obiettivi, le mafie hanno beneficiato, anche al di fuori delle aree di origine, dei convergenti interessi crimino-imprenditoriali di sempre più diffuse *lobby* costituite da una variegata gamma di attori (professionisti, intermediari, imprenditori collusi, pubblici ufficiali ed amministratori corrotti), la cui azione è finalizzata a inquinare le dinamiche del mercato e a condizionare i processi decisionali.

Tali *lobby*, per converso, anche in assenza del *player* criminale, hanno talvolta mutuato il metodo relazionale mafioso imponendo il proprio sistema corruttivo, specie nel settore delle grandi opere e dei più remunerativi appalti.

In alcune regioni del Paese, caratterizzate dalla presenza di un'ampia area grigia nel cui ambito si saldano interessi illeciti differenziati, la corruzione rappresenta il principale fattore di inquinamento utilizzato indifferentemente sia dalla criminalità organizzata, intenta a superare crisi strutturali e a preservare rendite di posizione, sia dai circuiti crimino-affaristici, interessati ad acquisire e mantenere un indebito vantaggio competitivo nei settori di riferimento.

L'ingerenza del crimine organizzato nella gestione della cosa pubblica ha trovato ulteriori conferme, oltre che in eclatanti sviluppi investigativi, nel sempre consistente numero di amministrazioni locali sciolte per mafia.

Non sono emersi significativi elementi di novità nelle dinamiche interne alle organizzazioni criminali (*vds. box n. 12*), da tempo impegnate a ricalibrare tanto le strategie di mantenimento del *welfare* mafioso, specie per il sostegno alle famiglie dei sempre più numerosi *boss* in carcere, quanto quelle di investimento.

Per quel che concerne i settori d'intervento che foraggiano le casse dei sodalizi alimentandone le capacità di inquinamento dei circuiti legali, **Cosa Nostra**, diminuita la pressione estorsiva su un tessuto imprenditoriale locale già in grave difficoltà, sta tornando ad attività tradizionali, in parte abbandonate nel recente passato, come il traffico di droga e il gioco clandestino.

Le componenti più competitive, sia per la guida esperta di *boss* recentemente scarcerati, sia per l'attitudine a permeare e condizionare taluni processi decisionali, costituiscono il volano di possibili tentativi di

box 12

LA CRIMINALITÀ ORGANIZZATA NAZIONALE: DINAMICHE ORGANIZZATIVE INTERNE

L'incisiva azione di contrasto, se da una parte ha provocato un'ormai cronica crisi di *leadership* interna a **Cosa Nostra**, dall'altra ha evidenziato la resilienza dell'organizzazione e la sua capacità di rimodellarsi continuamente. A livello provinciale, al temporaneo indebolimento della mafia palermitana, che affida le sue prospettive di recuperare prestigio al reintegro, nelle posizioni di vertice, di nomi di primo piano di *famiglie* storiche del capoluogo regionale, fanno da contraltare, da una parte, il ruolo meramente "oracolare" del *boss* latitante Matteo Messina Denaro e, dall'altra, il consueto dinamismo della *famiglia* di Catania.

La **'ndrangheta** conferma di essere un'organizzazione mafiosa in cui le sovrapposizioni di interessi fra le diverse cosche vengono armonizzate grazie all'innovativo ricorso a strutture di rappresentanza, i cui ambiti di effettività sono tuttora legati a variabili non stabilizzate.

Sul territorio, la provincia di Reggio Calabria, pur rimanendo caratterizzata dalla più qualificata presenza 'ndranghetista, sembra oggi attraversare una fase di defilamento dettata dall'esigenza di superare le conseguenze delle recenti investigazioni, mentre notevole attivismo si registra fra le cosche della fascia tirrenica (nella Piana di Gioia Tauro e, in maniera minore, nel vibonese) e jonica (nel reggino e nel crotonese).

L'esasperata conflittualità, tanto interna che esterna, rimane la cifra distintiva dei *clan* di **camorra**, soprattutto di quelli dell'area del capoluogo partenopeo e del suo *hinterland*, che conduce a vorticose alternanze nelle *leadership* e a ripetuti episodi omicidiari, questi ultimi strettamente connessi alla fluidità degli assetti e all'indebolimento del controllo del territorio da parte delle famiglie di maggior "lignaggio". Nell'area fra Napoli e Caserta, invece, i *clan* dimostrano una maggiore solidità strutturale che consente loro di continuare a coltivare l'ormai consolidata vocazione imprenditoriale.

Una prevalente anima gangsteristica e banditesca caratterizza tuttora, infine, la variegata galassia della **criminalità pugliese**, non in grado di rappresentare un livello qualificato di minaccia alla sicurezza nazionale, con l'eccezione di qualche storico potentato barese e salentino, dotato di interessi economico-imprenditoriali di rilievo, e di alcuni gruppi emergenti nel foggiano.

riorganizzazione delle strutture di vertice e il perno su cui potrà fondarsi una nuova e più dinamica realtà mafiosa.

La **'ndrangheta**, parimenti, ha confermato la storica primazia nel traffico di sostanze stupefacenti. In questo settore, grazie ai collegamenti con le aree di produzione e alla consolidata *expertise*, svolge funzioni di brokeraggio e "rifornimento" anche per altre organizzazioni criminali. I sodalizi calabresi, inoltre, hanno confermato la tendenza a diversificare gli investimenti, rafforzando la propria presenza imprenditoriale anche nella *green* e *new economy*, spaziando dall'eolico al ciclo dei rifiuti, nonché nel gioco *on-line*.

La capacità adattiva della 'ndrangheta la rende ipercompetitiva nei mercati del Nord Italia e all'estero, dove vanta un *brand* di elevata "affidabilità" nei contesti illegali e riesce ad espandersi grazie ad una fitta rete collusiva.

I ***clan*** **camorristici**, infine, soprattutto quelli della provincia napoletana connotati da spiccata vocazione imprenditoriale e potere intimidatorio, hanno consolidato, nel territorio di matrice, il proprio monopolio nel mercato del calcestruzzo e degli inerti, affinando le strategie di penetrazione nel settore della grande distribuzione e nelle diverse fasi del ciclo dei rifiuti. Nel casertano, la decapitazione del cartello dei Casalesi è parsa offrire spazio a forme ibride di criminalità economica.

Lo scarso livello strategico dell'attuale *leadership* camorrista, l'eccezionale densità di presenze gangsteristiche e la diffusa illegalità creano stati permanenti di conflittualità tra gli schieramenti criminali che, anche in prospettiva, potranno ulteriormente deteriorare la vivibilità di ampie zone campane.

Le mafie italiane all'estero

L'interconnettività di interessi sempre più globalizzati e le connaturate capacità relazionali hanno accentuato la spinta espansiva delle principali organizzazioni criminali al di fuori dei confini nazionali.

In particolare:

- in Europa, ad una politica di sommersione di Cosa Nostra, i cui interessi sono presenti principalmente ad Est, fa da contraltare un notevole e più visibile dinamismo delle 'ndrine calabresi. Pur se formalmente dipendenti dalle cosche di riferimento, le articolazioni 'ndranghetiste d'oltreconfine godono di un'ampia autonomia operativa soprattutto nel settore degli stupefacenti (anche attraverso *joint venture* con i cartelli colombiani e i trafficanti turchi) e mantengono legami funzionali con la cosca madre per il riciclaggio di capitali illeciti e come supporto logistico alla latitanza;
- in Nord America, si confermano gli storici *spin-off* di Cosa Nostra e della 'ndrangheta, diramazioni con le quali le corrispondenti *famiglie* d'origine mantengono continui e più strutturati contatti;
- in Africa, le 'ndrine, particolarmente attive in tutti i Paesi del Maghreb con

aziende operanti nel settore delle infrastrutture, dell'allevamento e della lavorazione di prodotti alimentari, oltre che nell'eolico, potrebbero sfruttare le potenzialità di nuovi mercati in crescita e con una minore sensibilità o esperienza normativa anticrimine rispetto all'Europa.

Le mafie straniere in Italia

Quanto alle proiezioni dei sodalizi stranieri in territorio nazionale, il dato più ricorrente nelle evidenze intelligence rimanda all'attivismo pervasivo di articolate organizzazioni criminali che mostrano di perseguire sistematicamente il controllo delle diaspore ricorrendo a modalità prossime ai tradizionali modelli mafiosi.

Ne deriva una gestione degli interessi illeciti perseguita, da un lato, attraverso l'intimidazione e la collusione e, dall'altro, incidendo significativamente sul piano sociale e imprenditoriale.

In tal senso, evidenziano un accresciuto e competitivo profilo crimino-affaristico:

- le espressioni criminali cinesi, nel cui ambito si colgono sempre più frequenti interazioni tra gruppi di impronta banditesca e componenti a vocazione imprenditoriale. Tale connubio consente a queste ultime di sfruttare le potenzialità intimidatorie delle agguerrite bande giovanili – attive nelle grandi aree metropolitane e in contatto con omologhe strutture a livello europeo – per controllare, condizionare e, ove necessario, annientare la concorrenza commerciale di connazionali. Le organizzazioni delinquenziali cinesi mirano, al tempo stesso, ad infiltrare i livelli di vertice dell'associazionismo etnico e imprenditoriale sviluppando inediti profili economici e sociali, con il rischio di inquinare e alterare i processi di integrazione degli immigrati cinesi nella realtà nazionale;
- le reti criminali nigeriane, segnatamente i cosiddetti "gruppi cultisti", che hanno progressivamente assunto un ruolo strategico per l'elevata capacità di ingerenza nelle dinamiche sociali della diaspora ricorrendo, per il controllo delle attività illegali sul territorio nazionale, alle medesime modalità violente e intimidatorie adottate in Patria. Tali formazioni, connotate da una forte tenuta identitaria, da una marcata autonomia, da notevoli capacità relazionali e da una spiccata vocazione ai traffici internazionali, mirano anche a promuovere iniziative commerciali e finanziarie per riciclare i proventi illeciti e radicarsi nel tessuto sociale ospite;
- i sodalizi esteuropei e caucasici, dediti soprattutto a reati predatori e attività estorsive, ma coinvolti nei più remunerativi traffici illeciti. Tra le espressioni criminali più pericolose, quelle moldava e georgiana, operanti talora in reciproca connessione, nonché in collegamento con le strutture mafiose attive nei rispettivi contesti di origine. Punto di forza di tali componenti, la pronunciata caratura transnazionale,

cui si correlano una costante mobilità sul territorio europeo e una capacità di rapida "rigenerazione" a fronte delle indagini e dei numerosi arresti, anche di elementi di vertice, operati nei vari Paesi UE.

Allo stato, il rapporto tra il crimine autoctono e quello straniero è contingente e finalizzato a specifici interessi illegali, sebbene si ritenga che in prospettiva possa evolversi in convergenze sempre più stringenti, specie nelle singole realtà locali.

SPINTE ANTI-SISTEMA E MINACCIA EVERSIVA

Congiuntura interna e conflittualità sociale

In un contesto macroeconomico caratterizzato da persistenti indicatori negativi, con un PIL in contrazione e un elevato tasso di disoccupazione, specie giovanile, si sono registrati segnali di un'intensificazione del disagio, non solo nell'ambito prettamente occupazionale ma anche in quella ampia area della popolazione – che le componenti antagoniste indicano come una sorta di *nuovo proletariato urbano* – in cui si collocano vari segmenti a rischio di emarginazione sociale, quali "senza casa", immigrati, famiglie in difficoltà economica e giovani senza prospettive lavorative.

Le forme di conflittualità sul territorio non hanno tuttavia prodotto nel corso dell'anno percorsi di generalizzazione ed estensione delle lotte, rimanendo sostanzialmente circoscritte alle rivendicazioni di settore volte alla tutela del posto di lavoro. Il ricorso al sistema degli ammortizzatori sociali e l'opera di mediazione dei sindacati confederali, che hanno consolidato la propria immagine di "riferimento essenziale" per la maggior parte dei contesti occupazionali, si sono ribaditi efficaci strumenti di difesa della coesione sociale. La base dei lavoratori, in linea generale, si è pertanto dimostrata sostanzialmente refrattaria ai perduranti tentativi di innalzamento del livello della protesta esperiti dalle formazioni dell'antagonismo, specie di matrice marxista-leninista, intenzionate a ricondurre le problematiche occupazionali nell'ottica ideologica del conflitto antisistema.

Nel quadro delineato, ha continuato a distinguersi il crescente fermento espresso dal comparto della logistica, le cui maestranze, in gran parte di origine extracomunitaria, sono considerate un ambito di potenziale consenso proprio da quei settori dell'antagonismo che guardano alle verten-

ze in un'ottica di *classe*. Parimenti, si profilano, in prospettiva, quali ambiti lavorativi a maggior rischio mobilitativo, tutti quelli ad "*alto tasso di precarizzazione*", caratterizzati dall'utilizzo di manodopera asseritamente sottopagata, priva di tutele e senza adeguata rappresentanza sindacale.

In termini previsionali, il protrarsi delle criticità occupazionali, correlato alla mancata soluzione delle vertenze, potrebbe originare un innalzamento del livello di protesta operaia nei contesti aziendali più colpiti dalla crisi in atto, suscettibile di estemporanee degenerazioni, anche violente.

Ulteriore fattore di rischio appare connesso alle dinamiche rivendicative del cd. *precariato esistenziale* (precari, disoccupati, giovani, immigrati, etc.) che al problema del lavoro sommano istanze relative a bisogni primari, quali il diritto alla casa, alla salute e, più in generale, alla fruizione di beni e servizi pubblici.

Nel complesso, emerge dunque uno scenario di crescente malessere acuito da sentimenti di disaffezione verso la politica e le istituzioni e destinato ad accrescere percezioni di frustrazione e insicurezza, che si diffondono specialmente tra quelle fasce della popolazione afflitte da un senso di progressiva esclusione sociale e che trovano valvola di sfogo in forme di contestazione spontanea, dal carattere di generica contrarietà alla situazione esistente. Emblematici, nel senso, gli episodi di vera e propria guerriglia urbana scoppiati soprattutto in alcune aree metropolitane ed etichettati dai media come il fenomeno delle "periferie in rivolta". Al momento, tali impeti risultano privi di connotazioni ideologiche, ma potenzialmente forieri di improvvise sortite ribellistiche specie contro la rappresentanza politica, sindacale e istituzionale.

Nella medesima ottica, non sono da sottovalutare i rischi di un possibile sviluppo di pulsioni razziste e xenofobe nei confronti delle comunità di immigrati, specie se scarsamente integrate, che già in passato hanno trovato differenti forme di innesco e che, nell'attuale sensibile congiuntura, potrebbero trovare ulteriori spunti, tra l'altro, nella percezione di una concorrenzialità sul terreno occupazionale e del *welfare*.

Dinamiche dell'antagonismo e campagne di lotta

La protesta "anticrisi" ha continuato a catalizzare l'impegno delle componenti antagoniste, determinate ad intercettare nuove disponibilità alla lotta tra le categorie considerate più esposte al disagio con l'obiettivo di favorire lo sviluppo del conflitto sociale.

Le rivendicazioni in tema di *reddito*, *diritti sociali* e *beni comuni* hanno costituito il principale ambito di intervento a livello territoriale mentre, in un'ottica più generale, la contestazione è stata indirizzata contro i provvedimenti del nuovo Governo, specie in materia di lavoro, e le *politiche d'austerity imposte dall'UE*, tematica, quest'ultima, che ha assunto rilievo centrale nel corso del semestre italiano di Presidenza UE.

Il *movimento anticrisi*, comunque, non è riuscito a consolidare il successo "politico" riscosso nelle manifestazioni romane dell'ottobre 2013, per le rinnovate divergenze e frammentazioni che ne hanno minato l'unitarietà d'intenti. A depotenziarne l'azione hanno contribuito soprattutto differenti visioni fra realtà attestate su posizioni movimentiste, orientate alla "piazza", ed espressioni più strutturate ideologicamente, interessate ad accreditarsi come "riferimento politico" sia presso gli ambienti di stampo anticapitalista sia presso le fasce popolari che non si sentono adeguatamente rappresentate.

Dopo l'annullamento del vertice europeo sulla disoccupazione giovanile in programma l'11 luglio a Torino, atteso quale importante occasione per rilanciare la protesta, il movimento antagonista ha ripreso il suo impegno in autunno, pianificando molteplici iniziative a livello territoriale funzionali alla creazione di una microconflittualità diffusa in tutto il contesto nazionale. In proposito, la scadenza di maggiore rilievo per incisività d'azione, modalità e capillarità nel territorio è stata la giornata di *sciopero sociale* del 14 novembre, tradottasi in manifestazioni in numerose città, sfociate anche in scontri con le Forze dell'ordine, blocchi stradali, picchettaggi e proteste nei contesti aziendali, specie del settore dei trasporti, scioperi, *blitz* contro sedi governative e istituzionali, banche e agenzie interinali, occupazione di edifici in disuso, iniziative davanti ai centri commerciali e ai negozi-simbolo dello "sfruttamento".

Fra i principali attori della mobilitazione *anticrisi*, i *movimenti per la casa* hanno mantenuto un ruolo centrale e trainante sotto il profilo del conflitto sociale, con l'attuazione in tutto il territorio nazionale di pratiche illegali e azioni di "disobbedienza civile", tra cui occupazioni abitative e di spazi sociali, nonché presidi "antisfratto" e inedite iniziative di "pressione" nei confronti dei Municipi.

In prospettiva, il movimento antagonista si conferma determinato a superare le contrapposizioni interne per dar vita ad una sorta di "coalizione sociale" che interpreti la percepita *diffusa voglia di tornare in piazza*. Si punterà proprio su quel *meticciato dei percorsi di lotta* che, pur nella pluralità di rivendicazioni, consente di ottenere "massa di manovra" da utilizzare e gestire per innalzare i toni ed il livello della conflittualità sociale. In tale ottica, acquisterà rilievo in particolar modo l'adesione alle proteste sia della componente migrante, portatrice di un crescente malessere, che di quella giovanile/studentesca, da sempre considerata dagli ambienti antagonisti una forza propulsiva in grado di conferire incisività e spessore alle mobilitazioni di piazza.

Significative sinergie si sono consolidate intorno all'asserita recrudescenza dell'attività repressiva, cui sono state ricondotte le iniziative giudiziarie nei confronti dei reati commessi dai militanti, nonché le misure di prevenzione di illeciti in occasione di manifestazioni, qualificate come un tentativo di frammentare e depotenziare i movimenti e la protesta sociale.

Sul versante della lotta di stampo ambientalista, è proseguito l'attivismo del *movimento No TAV*, tradottosi in iniziative diversificate in territorio valsusino in linea con la sperimentata "strategia di logoramento": attacchi al cantiere concentrati soprattutto nel corso della stagione estiva; azioni dimostrative contro imprese e strutture funzionali alla realizzazione dell'opera; gesti intimidatori nei confronti di amministratori locali e politici favorevoli al progetto; diffusione di propaganda denigratoria nei confronti dei magistrati responsabili delle inchieste sugli attivisti d'area. La mobilitazione ha ricercato nuove occasioni di visibilità a livello nazionale, specie in concomitanza con scadenze processuali relative a militanti *No TAV* che hanno offerto spunti di attivazione anche a frange di matrice anarco-insurrezionalista (*vds. box n. 13*).

Sulla scia della protesta valsusina appaiono destinati ad assumere spessore e visibilità anche gli altri fronti di lotta contro l'Alta Velocità già attivi tra Liguria e Piemonte (Terzo Valico) e in Trentino (TAV del Brennero).

box 13

GLI INSURREZIONALISTI E LA TAV

L'opposizione al progetto Alta Velocità è rimasta centrale per le componenti anarco-insurrezionaliste *movimentiste* che, propense ad integrarsi nelle lotte territoriali/sociali per radicalizzare la protesta, hanno intensificato l'impegno propagandistico a sostegno degli attivisti inquisiti, nel segno della mobilitazione permanente contro la *repressione* dello Stato. A tali ambienti, in seno ai quali sono emersi, nel corso dell'anno, segnali di insofferenza e posizioni polemiche nei confronti di una condotta giudicata troppo "appiattita" su quella del *movimento No TAV*, è altresì riconducibile una serie di attacchi a "bassa intensità" (esposizione di striscioni, blocchi temporanei della circolazione, vandalismi, lanci di bottiglie incendiarie) compiuti in solidarietà con gli indagati in varie regioni, a dimostrazione della diffusione raggiunta dalla protesta contro la *repressione*. All'area anarco-insurrezionalista appaiono attribuibili, poi, gli atti di sabotaggio ai danni delle linee dell'Alta Velocità di Milano-Torino, Milano-Firenze e Milano-Bologna, effettuati nei giorni successivi all'emissione della sentenza del Tribunale di Torino che, il 17 dicembre, ha scagionato quattro militanti dall'accusa di associazione con finalità di terrorismo, condannandoli per i soli reati specifici di porto d'armi da guerra (*molotov*), danneggiamento seguito da incendio e violenza a pubblico ufficiale, compiuti in occasione di un assalto al cantiere TAV di Chiomonte (maggio 2013). Si è trattato di azioni incendiarie realizzate con manufatti artigianali posizionati in punti nevralgici del traffico ferroviario, che hanno provocato rallentamenti e disagi alla circolazione, evidenziando l'elevata esposizione delle vie di comunicazione a tecniche di attacco anche non particolarmente sofisticate.

Un crescente rilievo mobilitativo hanno assunto nel corso dell'anno altre campagne contro le "grandi opere", ambito in cui le componenti antagoniste tentano di cavalcare il cd. effetto *NIMBY* (acronimo di *Not In My Back Yard*, letteralmente *non nel mio cortile*), che accomuna tutte le varie proteste ambientaliste promosse dai comitati popolari a livello locale, per incanalarle in un'ottica di generale opposizione alle politiche governative di *speculazione* e *devastazione ambientale*.

Importanza prioritaria, al riguardo, riveste la mobilitazione contro l'*Expo* a Milano, che individua un momento centrale nella manifestazione del 1° maggio 2015, giornata inaugurale della fiera, destinata a richiamare nel capoluogo lombardo attivisti da tutto il territorio nazionale. Il circuito antagonista lombardo, che contesta l'esposizione come *paradigma del nuovo modello di sfruttamento umano e dei territori*, si è fatto promotore di una campagna di occupazioni, specie nelle aree limitrofe all'area espositiva, con l'obiettivo di disporre di punti strategici per la gestione della protesta.

Con riguardo agli spunti mobilitativi attinti dallo scenario internazionale, rinnovato impulso ha fatto registrare la campagna a sostegno della causa palestinese, con manifestazioni di protesta e appelli al boicottaggio anche nei confronti di società italiane coinvolte a vario titolo in attività imprenditoriali con Israele.

In chiave antimilitarista, nel quadro del tradizionale attivismo contestativo contro la presenza di strutture militari sul territorio nazionale, a fronte del tono minore che ha caratterizzato l'impegno dei comitati siciliani contro il sistema satellitare *MUOS*, si è rilevato un innalzamento della tensione mobilitativa in Sardegna, ove espressioni dell'antagonismo e dell'indipendentismo sardo hanno rivitalizzato la protesta contro le esercitazioni nei poligoni e nelle installazioni militari dell'Isola, reclamando *la smilitarizzazione del territorio*.

Più in generale, la tematica appare destinata ad acquisire specifico rilievo nel corso del 2015, in cui ricorre il centenario dell'entrata in guerra dell'Italia nel primo conflitto mondiale.

L'eversione anarco-insurrezionalista

A fronte di un nuovo fermo operativo della FAI/FRI *(Federazione Anarchica Informale/Fronte Rivoluzionario Internazionale)*, tornata ad essere "silente" sul territorio nazionale dopo l'invio, nell'aprile 2013, di due plichi esplosivi a un quotidiano e a una società di investigazioni privata, si è intensificato il dibattito volto a rilanciare le progettualità d'area attraverso, in particolare, la ricerca di piani condivisi di lotta tra gli ambienti "affini" al "cartello" e quelli attestati su posizioni più ortodosse, ma comunque radicali.

In questo contesto si colloca il nuovo progetto editoriale *Croce Nera Anarchica*, diffuso anche sul *web*, avviato in aprile su *input* di anarchici detenuti, tra cui gli autori dell'attentato di Genova (maggio 2012), Alfredo Cospito e Nicola Gai. L'obiettivo è quello

di ricompattare l'area intorno alla *solidarietà rivoluzionaria* nei confronti dei compagni in carcere, prefigurando una sorta di progetto offensivo aperto e "flessibile", che prevede libertà d'azione nella scelta degli obiettivi, nel *modus operandi* e nella stessa determinazione a rivendicare o meno il gesto.

Gli attivisti sono spronati ad abbandonare gli atteggiamenti difensivi o rinunciatari – correlati all'azione di contrasto, che negli ultimi anni ha portato all'emissione di numerosi provvedimenti giudiziari – così come le pratiche di lotta *movimentiste* (presidi, cortei, etc.) considerate inefficaci.

In quest'ottica, il sostegno ai prigionieri dovrebbe tradursi nell'*azione diretta* nella sua accezione *distruttiva*. Lo sviluppo del dibattito ha fatto emergere, peraltro, la persistenza di divergenze, che sembrano destinate a incidere sulla realizzazione di un "fronte" anarco-insurrezionalista unitario (*vds. box n. 14*). Circostanza, questa, che non ridimensiona il rischio di una possibile ripresa delle azioni violente in territorio nazionale da parte sia di quelli determinati a rilanciare il logo FAI/FRI sia di quanti preferiscono l'anonimato nella pratica di opposizione radicale al *sistema*.

Gli obiettivi privilegiati rimarranno quelli appartenenti al comparto *repressivo* (Forze dell'ordine, magistratura, "carcerario"), al *dominio tecnologico* e alle *nocività*, come anche agli altri fronti di lotta dell'area, dall'antimilitarismo all'opposizione ai *poteri economico-finanziari*, ai *media di regime*.

La *solidarietà rivoluzionaria* ai compagni prigionieri continua a rappresentare un ideale connettore a livello internazionale, specie con riguardo al circuito FAI/FRI

box 14

IL CONFRONTO TRA *INFORMALI* E ORTODOSSI

La ricerca di un percorso condiviso verso una "anarchia d'azione" in cui si riconoscano tutti i militanti fortemente determinati a *distruggere l'esistente* non è apparsa tuttavia agevole. Tanto i sostenitori della FAI/FRI quanto i seguaci del filone *ortodosso*, pur accomunati dal rifiuto della cd. *linea movimentista*, accusata di confondere e sfumare l'identità anarchica in un generico antagonismo, sono parsi sostanzialmente ancorati ai rispettivi distinguo di principio e di metodo. In particolare, per gli *informali* resta centrale il valore della rivendicazione ai fini della "riproducibilità" dell'azione, mentre per gli *ortodossi* l'apertura alle *multiformi pratiche d'azione*, compresi gli interventi "non firmati", si accompagna alla necessità che ogni attacco sia preceduto da un'approfondita analisi del contesto in cui si vuole agire, al fine di individuare e colpire un obiettivo realmente *rivoluzionario*.

box 15

COLLEGAMENTI INTERNAZIONALI DELLA FAI/FRI

Internet ha rappresentato e continua a rappresentare un punto di forza dell'anarco-insurrezionalismo a marchio FAI/FRI, divenuto un *brand* di riferimento a livello globale. Nel corso del 2014 sono stati diffusi in rete almeno 40 comunicati di rivendicazione di azioni compiute in 14 Paesi, per lo più in Europa e America Latina, dedicate nella maggior parte dei casi a militanti in carcere. Al riguardo, specifica menzione meritano i rapporti privilegiati tra *informali* italiani e gli omologhi greci della *Cospirazione delle Cellule di Fuoco*, da ritenersi attualmente l'espressione FAI/FRI più "evoluta" dal punto di vista militare e di particolare spessore sotto il profilo dell'elaborazione teorica. All'organizzazione greca – che il 30 aprile ha rivendicato l'invio di un pacco bomba (inesploso, ma contenente 600 grammi di esplosivo ad alto potenziale) contro un Commissariato di polizia della Focide – si devono, del resto, il consolidamento del processo di internazionalizzazione della FAI, nonché la campagna offensiva del *Progetto Fenice*, oggetto di specifico approfondimento nella Relazione annuale 2013. In questa cornice s'inseriscono, tra l'altro, la diffusione di interventi e video-messaggi accompagnati da *slogan* antiautoritari e appelli istigatori.

(*vds. box n. 15*). In questo contesto, potranno essere presi di mira anche bersagli rappresentativi di Stati stranieri, specie di quelli considerati particolarmente attivi nella *repressione* degli anarchici, di istituzioni internazionali nel territorio italiano nonché obiettivi del nostro Paese all'estero.

L'estremismo marxista-leninista

Le realtà oltranziste d'ispirazione brigatista, tuttora contrassegnate da esiguità numerica e frammentazione interna, hanno continuato ad impegnarsi su programmi di lungo termine, volti alla formazione di nuove *forze rivoluzionarie*, in linea con l'esperienza delle organizzazioni armate degli anni '70-'80.

In questo senso, specifico rilievo assumono i perduranti legami con gli "irriducibili" del circuito carcerario, tradizionali depositari dell'ortodossia ideologica. Alcuni di essi, convinti delle favorevoli opportunità offerte dalla difficile congiuntura economica, hanno elaborato documenti teorico-propagandistici che mirano a riproporre una *lettura di classe* – incentrata sulla storica contrapposizione tra lavoro e capitale – delle più significative manifestazioni di protesta sociale in atto. L'intento è di attualizzare la proposta rivoluzionaria, favorendo il passaggio delle lotte dal piano rivendicativo a quello di radicale sovvertimento del sistema costituito.

Nel contempo, circuiti internazionali attivi nella solidarietà ai "prigionieri politici" hanno proseguito nell'attività di pubblicazione e divulgazione di interventi a favore della *lotta armata*.

Sul piano più propriamente operativo, in prospettiva, restano ipotizzabili azioni dimostrative di modesto spessore, riconducibili a elementi determinati ad orientare politicamente le istanze più radicali della protesta, nonché a stimolare fenomeni emulativi e spinte aggregative nell'area di riferimento.

La destra radicale

Le principali formazioni di matrice identitaria hanno proseguito l'impegno sulle tradizionali tematiche d'interesse, specie sul terreno delle istanze sociali. Si è confermata, tra l'altro, la propensione a strumentalizzare il disagio anche attraverso una pressante propaganda anti-immigrati.

In prospettiva, è verosimile che le compagini maggiormente rappresentative, attesa l'esigenza di incrementare visibilità e raccogliere maggior seguito, possano ricercare convergenze con altri movimenti, soprattutto a supporto di politiche migratorie restrittive e antieuropee. Allo scopo continueranno ad essere coltivate campagne di sostegno a fasce disagiate della popolazione italiana con il coinvolgimento di settori giovanili e studenteschi, particolarmente sensibili a tali tematiche. In quest'ottica, è prevedibile altresì un aumento della conflittualità con gruppi di opposta ideologia, intenzionati a circoscrivere gli spazi di agibilità politica della destra radicale.

Con riguardo alle tematiche internazionali, particolare attenzione è stata riservata a taluni sviluppi del teatro estero. In particolare, il dibattito sulla crisi ucraina ha contribuito ad acuire la frammentarietà interna dell'area, in relazione alle divergenze tra sostenitori di Kiev e attivisti filo-russi, tradottesi anche nella presenza di militanti in corpi paramilitari di entrambi gli schieramenti operanti nei luoghi del conflitto.

Sono proseguiti, inoltre, i contatti con omologhe realtà di altri Paesi europei, soprattutto dell'Est, funzionali a promuovere un'*alleanza* transnazionale di formazioni etnocentriche e tradizionaliste che, sotto l'*invocata* ègida russa, possa rappresentare un contraltare all'*imperialismo* statunitense.

La situazione ucraina ha rappresentato tema mobilitativo centrale anche per i gruppi di matrice eurasiatista, fin dall'inizio della crisi schierati a favore dei separatisti e della linea di condotta moscovita. Sul tema si sono distinte alcune realtà che hanno promosso iniziative a sostegno della popolazione russofona e inviato rappresentanti nella regione.

Ha continuato a registrarsi, inoltre, la vitalità di frange minoritarie che in alcune città hanno tratto nuovi spunti dalle rinnovate tensioni israelo-palestinesi per iniziative propagandistiche di impronta antisemita.

Nell'insieme, all'interno del frammentato ed eterogeneo panorama della destra

radicale non sono attualmente visibili dinamiche che appaiano in grado di alimentare una minaccia terroristica.

Resta ipotizzabile, comunque, che singoli individui o piccoli gruppi semiclandestini, attestati su posizioni più oltranziste, possano coltivare progettualità eversive, seppur velleitarie rispetto alle capacità e ai mezzi di cui sono in possesso.

In tal senso, significativo appare il caso – comunque finora isolato e in via di approfondimento – del sedicente gruppo neofascista *Avanguardia ordinovista*, i cui membri, arrestati il 22 dicembre, avrebbero ideato la consumazione di attacchi (anche di tipo stragista) contro obiettivi civili e personalità istituzionali, nel segno di una complessiva strategia destabilizzante.

LA PRESSIONE DELLE CRISI SULLE FRONTIERE DELL'EUROPA

Spinte centrifughe e *network* criminali

Ulteriori variabili nel complesso *dossier* migratorio sono rappresentate dalle vulnerabilità del contesto economico-sociale che, considerate nella stretta prospettiva intelligence, pongono molteplici implicazioni sul piano della sicurezza.

A fronte di un fenomeno reso ineludibile dalle crisi d'area e dalle situazioni d'instabilità politico-istituzionale nei quadranti africano e mediorientale, l'attivismo delle organizzazioni criminali nella gestione del traffico di migranti e profughi ha contribuito ad alimentare l'imponente deriva migratoria che, muovendo soprattutto dalle coste libiche, ha investito prevalentemente il Canale di Sicilia (*vds. box n. 16*).

Proprio la fragilità dello scenario libico ha trasformato quel territorio nel principale punto di confluenza e raccolta dei flussi migratori del Continente africano e di una parte di quelli provenienti dalla direttrice mediorientale. Ciò anche grazie alla complicità a livello locale di elementi appartenenti alle diverse milizie, agli apparati di sicurezza e ad altre strutture di potere.

Al contempo, in suolo libico operano gruppi criminali di varia nazionalità che fungono da terminali delle filiere attive nelle diverse tratte del traffico, a partire dalla fase di "reclutamento" dei migranti nei Paesi di origine. In questo contesto, particolare impegno informativo ha riguardato le componenti criminali nigeriane, eritree, somale, sudanesi e pakistane, con approfondimenti anche in direzione dei consistenti flussi finanziari generati dall'illecita attività.

Transita per il territorio del Paese nordafricano anche una parte significativa del flusso di profughi siriani, su particolare impulso delle reti criminali egiziane

box 16

FLUSSI REGIONALI E SPINTE CENTRIFUGHE

Per quel che concerne i numeri delle rotte via mare, secondo i dati del Ministero dell'Interno nel 2014 sono sbarcate, o sono state trasferite a terra dopo il soccorso in mare, 170.100 persone, quasi 3 volte rispetto al 2013.

Più che triplicato, inoltre, il flusso di siriani (da 11.307 a 42.323) e quello proveniente da Paesi del Corno d'Africa, segnatamente Somalia ed Eritrea (da 13.097 a 40.085).

I migranti sono risultati, in prevalenza, di giovane età (inferiore ai 36 anni) e di sesso maschile (il 70% circa del totale). Significativo il numero di minori, che è arrivato a sfiorare il 20% (di questi, il 70% circa non era accompagnato).

In generale, i migranti provengono dalle aree del Sahel, dell'Africa Occidentale e del Corno d'Africa, nonché dalla fascia asiatica che comprende il Vicino e il Medio Oriente, il Sub-Continente indiano e parte della Penisola indocinese.

La massiccia corrente migratoria che origina dal Corno d'Africa e dalla Siria investe, *in primis*, gli Stati contermini. Il prolungarsi delle crisi e le precarie condizioni di vita nei campi di accoglienza inducono il 20-35% dei profughi – spesso "convinti" dalle stesse organizzazioni criminali – a dirigersi illegalmente verso mete più favorevoli sia dal punto di vista economico che della sicurezza (Europa e Nord America).

operanti in particolare connessione con omologhe compagini turche.

Più in generale, sono emersi assidui rapporti tra sodalizi operanti lungo l'intera sponda Sud del Mediterraneo, rinnovati segnali di attivismo dalle coste meridionali della Turchia e un accentuato dinamismo di organizzazioni capaci di gestire i remunerativi traffici non solo di clandestini, ma anche di stupefacenti. In questa cornice si inseriscono le acquisizioni intelligence che hanno consentito, tra l'altro, il sequestro di imbarcazioni cariche di *hashish*, più volte utilizzate per il trasporto di migranti.

Il fenomeno migratorio ha interessato, sebbene in misura minore, anche lo scenario adriatico e i confini del Nord-Est, facendo registrare l'arrivo, attraverso la penisola balcanica, di migranti asiatici, mediorientali e africani, la cui meta ultima sono i Paesi nordeuropei.

Quanto alle attività di favoreggiamento, l'impegno informativo ha fatto emergere, tra l'altro, l'avvenuta "specializzazione" di strutturati *network* pakistani dediti, per lo più, alla falsificazione di documenti (*vds. box n. 17*).

Come già rilevato nella Relazione 2013, permane all'attenzione dell'intelligence

box 17

FAVOREGGIAMENTO DELL'IMMIGRAZIONE CLANDESTINA E ATTIVISMO DELLE RETI PAKISTANE

Le articolate organizzazioni criminali che gestiscono i flussi migratori, vista la necessità di consentire ai migranti di attraversare molti Paesi e, spesso, di effettuare parte del viaggio in aereo, alimentano il mercato dei documenti di identità, di viaggio e di lavoro falsi.

In tal senso, è largamente riconosciuta l'abilità delle reti pakistane (o afghano-pakistane) nella contraffazione persino delle versioni più aggiornate di passaporti europei e, nel nostro Paese, sono stati individuati diversi circuiti di tale etnia coinvolti nel favoreggiamento dell'immigrazione attraverso la falsificazione documentale.

Si tratta generalmente di un numero limitato di individui che agiscono in collegamento con strutturate organizzazioni stanziate in madrepatria, dove avvengono le prime fasi del traffico (reclutamento dei migranti, contrattazione ed acquisizione del corrispettivo richiesto, partenza).

Un altro fenomeno all'attenzione, sempre sul fronte del favoreggiamento, è la stipula, dietro corrispettivo, di fittizi contratti di lavoro funzionali al rilascio/rinnovo del permesso di soggiorno. Diverse le componenti etniche evidenziatesi in questo contesto, che ha fatto emergere anche il coinvolgimento di professionisti e/o imprenditori italiani.

il rischio di infiltrazioni terroristiche nei flussi via mare, ipotesi plausibile in punto di analisi ma che sulla base delle evidenze informative disponibili non ha sinora trovato concreto riscontro. Si pongono tuttavia quale potenziale vettore di minaccia le rilevate collaborazioni e intese contingenti in estese zone del Nord Africa e della regione sahelo-sahariana tra organizzazioni di trafficanti e gruppi armati di matrice islamista, favorite talora dai legami tribali o familiari esistenti tra componenti delle diverse formazioni.

Sempre all'attenzione è poi l'eventualità che circuiti radicali di ispirazione jihadista possano ricercare, a fini di proselitismo, spazi d'influenza nei Centri di immigrazione presenti sul territorio nazionale, esposti a ricorrenti situazioni di congestione e permeabili all'azione di sodalizi criminali interessati a favorire la fuga dei migranti.

Impatto sul territorio

L'enorme afflusso di migranti sul territorio nazionale ha messo a dura prova la capacità recettiva del circuito di accoglienza. L'affollamento delle strutture e le correlate difficoltà gestionali, la promiscuità etnica,

i prolungati tempi tecnici necessari per gli accertamenti richiesti dall'istruttoria per le istanze di protezione internazionale e per il rilascio del permesso di soggiorno hanno spesso contribuito ad acuire il disagio dei migranti, innescando manifestazioni di protesta, plateali e violente.

Il frequente rifiuto dei profughi di sottoporsi alle procedure di identificazione nel timore che, una volta raggiunte le ambite mete nordeuropee, principale obiettivo finale del loro viaggio, possano essere riassegnati al primo Paese di ingresso nell'UE in applicazione del Regolamento di Dublino, incide significativamente sull'efficacia delle attività di controllo e riconoscimento.

La dispersione dei migranti sul territorio e il passaggio alla condizione di clandestinità hanno accentuato il rischio di una loro cooptazione nei circuiti delinquenziali, esponendoli altresì a diverse forme di sfruttamento, nonché a condizioni igienico-sanitarie precarie.

L'aumento esponenziale degli arrivi rischia inoltre di indebolire la tradizionale funzione di raccordo tra migranti e società ospite esercitata dalle diaspore già presenti in Italia, con possibili ricadute in termini di mancata integrazione, ampliamento dei cd. *ghetti etnici*, tendenze criminogene e processi di radicalizzazione.

Parte terza

LA MINACCIA NEL CYBERSPAZIO

LA *CYBERTHREAT*

Aspetti generali

Nel corso del 2014 la minaccia *cyber* ha continuato a rivestire elevata priorità informativa. Sono state crescenti e più mirate le attività di contrasto poste in essere dall'intelligence al fine di garantire allo spazio cibernetico – ove si sviluppa una parte significativa della crescita economica e sociale del Paese – adeguati livelli di sicurezza.

In ragione delle peculiari caratteristiche della minaccia e allo scopo di meglio inquadrarne profili tecnologici, matrici e direttrici, l'attenzione informativa si è focalizzata in modo particolare:

- sulle minacce strutturate, persistenti e pervasive gravanti, potenzialmente o di fatto, sulla sicurezza delle infrastrutture critiche nazionali;
- sulle attività di spionaggio in ambiente digitale a danno di soggetti, sia pubblici che privati, operanti in settori di rilevanza strategica per la sicurezza nazionale, specie se titolari di informazioni sensibili ovvero di conoscenze specialistiche nei settori tecnologico e del *know-how* pregiato;
- sulle campagne e sui singoli attacchi riconducibili al fenomeno dell'attivismo digitale, condotti contro *target* istituzionali;
- sull'impiego della Rete per comunicazione con finalità di propaganda, disinformazione e controinformazione, proselitismo e pianificazione di azioni terroristiche o criminali.

Lo stretto monitoraggio di tali aspetti ha contribuito alla migliore comprensione delle seguenti, principali **criticità di portata strutturale**:

- possibilità di una maggiore pianificazione e realizzazione di attività illecite mediante l'impiego di risorse digitali, ritenute "vantaggiose", in quanto rapide, efficaci e sicure;
- difficoltà a relazionare le tracce di un attacco, le risorse internet che genera-

no il flusso telematico dello stesso e la loro attestazione geografica, con parametri di riscontro univoci e oggettivi ai fini dell'attribuzione dell'evento, anche in ragione dell'impiego di tecniche di anonimizzazione;

- differenza tra modalità silenti e dissimulate del *cyber crime* e, soprattutto, del *cyber espionage,* nonché tra quelle degli attacchi di matrice hacktivista ed eversiva/terroristica, che trovano nella rivendicazione pubblica il loro momento conclusivo ed essenziale;
- agevole accesso a prodotti e strumenti innovativi che consente agli attaccanti, pur a fronte di risorse economiche limitate, di innalzare rapidamente le proprie capacità operative in corrispondenza con l'evolversi dei sistemi informatici.

La "guerra ibrida"

Dell'ampia gamma di eventi *cyber* occorsi nell'arco del 2014, ciò che ha catturato l'attenzione dell'intelligence, in misura maggiore rispetto al passato, è stato il massiccio utilizzo dello spazio cibernetico in contesti di confronto militare, circostanza, questa, che ha contribuito a connotare la natura "ibrida" di alcuni conflitti. Il ricorso al *cyberspace* – in modo combinato con strumenti convenzionali e non (pressione economica ed energetica, uso delle informazioni, impiego di forze irregolari, etc.) – ha fatto registrare un livello di complessità, intensità e sofisticazione tale da ricondurre a questo dominio un ruolo determinante, specie nell'ambito della conflittualità tra Stati. Particolarmente significativa si è rivelata la duplice modalità di utilizzo dell'ambiente cibernetico sia quale mezzo a supporto di una comunicazione rapida, efficace e praticamente senza limiti, sia come strumento, per la conduzione di attacchi a sistemi e reti critiche, complementare a quelli convenzionali ed idoneo, anzi, a determinare un effetto di moltiplicazione della forza. Ciò ha contribuito alla creazione, in altri termini, di una "dimensione digitale" della geopolitica, caratterizzata da confini "liquidi", in cui si estrinsecano equilibri di potere non sempre coincidenti con quelli della sfera fisica e della conflittualità cinetica.

Attori tecniche e finalità

A fronte di ciò, è stata confermata la tendenza ad un polimorfismo della minaccia e ad una diluizione del profilo dell'attaccante, elementi, questi, tradottisi, da un lato, nell'operatività di una vasta gamma di attori con finalità ed obiettivi diversi, operanti singolarmente o nell'ambito di organizzazioni più o meno strutturate di natura sia statuale, sia privata che criminale e, dall'altro, nella difficoltà di classificare un insieme così eterogeneo di attori, attese le difficoltà di tracciare confini precisi tra le varie categorie di attaccanti. Un soggetto appartenente ad un gruppo terrorista, ad esempio, può agire come un *hacker* o un *cracker* (*vds. box n. 18*), mentre un *insider* potrebbe operare su indicazioni

di un attore istituzionale, quale un Servizio d'intelligence estero.

Sempre più consistente, come sopra evidenziato, è risultato l'impiego del cyberspazio quale **terreno di confronto tra Stati**. In tale ambito, alcuni eventi hanno contribuito ad avvalorare le conclusioni delle principali dottrine militari, secondo cui lo spazio cibernetico costituisce la dimensione degli attuali e dei futuri conflitti: gli attacchi ai sistemi informatici dell'Estonia nel 2007, le operazioni *cyber* nel corso della crisi russo-georgiana nel 2008, l'impiego di *Stuxnet* per rallentare il programma nucleare iraniano nel 2010 e gli episodi registrati nel 2014, nel contesto della crisi ucraina. Di rilievo, nell'ambito di quest'ultima, l'impiego ancor più strutturato del *cyber* sia come fattore di innesco della conflittualità, sia, soprattutto, come elemento complementare e potenziante delle operazioni militari convenzionali. Sotto tale profilo, emblematici sono stati gli attacchi DDoS e i *web defacement* (*vds. box n. 18*), il danneggiamento fisico e tecnologico di reti di telecomunicazione e le tecniche di *information warfare,* finalizzate alla distorsione delle informazioni in vista dell'acquisizione di un vantaggio competitivo sull'avversario.

Lo spionaggio digitale

Ad una prevalente matrice statuale vanno ricondotte, poi, le più articolate attività di spionaggio digitale registrate nel corso del 2014 contro *target* nazionali operanti in settori dall'elevato ed avanzato contenuto tecnologico (*vds. box n. 9*). Nei confronti di tali soggetti l'attività di spionaggio non si è limitata solo all'esfiltrazione di informazioni sensibili relative a tecnologia, processi, programmi e prodotti futuri, ma si è posta anche in chiave strumentale rispetto alle acquisizioni di pacchetti azionari. È verosimile, cioè, che alcune operazioni finanziarie abbiano tratto beneficio da mirate offensive digitali – sotto forma di *due diligence* "clandestine" – attraverso cui sono stati acquisiti dati e notizie utili a conseguire, in fase negoziale e per effetto di una più capillare conoscenza delle aziende da acquisire, posizioni di maggiore vantaggio.

Non sono mancate, poi, attività poste in essere anche da **aziende** e ***corporation*** per finalità di spionaggio industriale e commerciale. Obiettivi privilegiati, in questo caso, sono stati il patrimonio di conoscenze tecnologiche dei concorrenti e le loro attività economiche e finanziarie, facilmente raggiungibili, specie nelle realtà piccole e medie, a causa dell'assenza di *policy* e di adeguati investimenti nel settore della sicurezza informatica.

Sotto il profilo tecnico, gli attacchi per finalità di spionaggio – che hanno fatto registrare un livello di sofisticazione più elevato rispetto al passato – hanno continuato a connotarsi per il ricorso a strumenti di estrema pervasività e persistenza, capaci di operare, altresì, mirate riconfigurazioni a fronte delle diversificate difese adottate, di volta in volta, dal *target*.

L'hacktivismo

Quanto agli *hacktivist (vds. box n. 18),* i soggetti operanti nel panorama nazionale hanno effettuato un significativo salto di qualità operativa, attestato, in modo particolare, dai seguenti fattori:

- un *trend* evolutivo delle capacità e delle tecniche di attacco;
- lo scostamento dalle iniziali spinte motivazionali basate perlopiù sulla lotta per la libertà di espressione e di informazione e sulla protesta contro ogni forma di censura e regolamentazione della Rete;
- la prospettiva di adesione di alcune frange di attivisti digitali al modello anarchico, che ha trovato principale riscontro nella conduzione di azioni ostili verso esponenti di primo piano della politica e delle istituzioni nazionali nel segno di campagne proprie dell'area libertaria;
- l'allontanamento dal *cliché* organizzativo e comportamentale originario (in base al quale l'offensiva di matrice hacktivista si palesava quale forma di attivismo indipendente rispetto ai fenomeni di piazza) e il progressivo avvicinamento, in chiave decisionale e operativa, tra le dimensioni digitale e reale dell'antagonismo. Emblematiche le convergenze rilevate in occasione di manifestazioni di piazza, rispetto alle quali sono state registrate iniziative sincrone, verosimilmente oggetto, in alcuni casi, di pianificazione preventiva.

L'hacktivismo, nella dimensione internazionale, estremamente fluida per le dinamiche organizzative dei gruppi che la compongono e trasversale quanto alle istanze ideologiche di volta in volta poste alla base delle campagne di attacco, ha confermato *Anonymous* quale punto di riferimento della maggior parte delle iniziative di antagonismo digitale, sotto la duplice veste di:

- contesto organizzativo in cui sono promosse e realizzate le campagne d'attacco, secondo un modello che vede, di norma, *target* e modalità operative scelti nell'ambito dei *forum* e delle *chat* utilizzate dai membri e simpatizzanti, in forza di un approccio *bottom-up* in cui è la base a fare le proposte e la comunità a selezionare il bersaglio e ad auto-coordinarsi per la condotta delle operazioni;
- entità "ombrello" alla quale è stata attribuita la paternità delle azioni digitali pianificate e poste in essere da altre realtà omologhe, quale efficace cassa di risonanza mediatica nella fase della rivendicazione.

Da evidenziare, in aggiunta, il persistere del supporto hacktivista alle situazioni di crisi internazionale – primavere arabe, crisi siriana e causa palestinese – ribadito, all'indomani degli attentati di Parigi, con l'avvio dell'operazione *#OpCharlieHebdo*, finalizzata a *"vendicare l'assalto inumano inferto alla libertà di espressione"* e tradottasi, successivamente, in una serie di attacchi di tipo DDoS contro decine di siti e di *account* jihadisti.

In un'ottica previsionale, alla luce delle evoluzioni che hanno caratterizzato gli attacchi di tale matrice, il livello di rischio che l'intelligence riconduce agli stessi è

ritenuto concreto, attuale e con una proiezione di medio-lungo periodo. Quale ulteriore profilo d'interesse informativo vi è quello connesso alle elevate capacità offensive acquisite dagli attivisti digitali, idonee a rendere gli stessi oggetto di potenziale manipolazione ed etero-direzione da parte di entità strutturate, per il conseguimento di obiettivi diversi dalla protesta *on-line*.

Il *cyberjihad*

Come delineato nei precedenti capitoli, è stato crescente il ricorso – specie da parte delle organizzazioni terroristiche più strutturate – alle reti, ai servizi e agli strumenti di comunicazione elettronica per finalità di proselitismo, radicalizzazione, arruolamento, addestramento, autofinanziamento e pianificazione operativa delle azioni violente. La pervasività del cyberspazio, la difficoltà di alzare barriere al suo interno e la possibilità di operare in modo anonimo hanno continuato a connotare quel dominio quale strumento ideale per lo svolgimento di attività con finalità di terrorismo.

Rilevante è apparso l'uso sempre più frequente, da parte di alcuni gruppi, di soluzioni crittografiche in grado di garantire l'anonimato delle comunicazioni. Oggetto di particolare attenzione è stata l'attività svolta dallo *Stato Islamico* , che si è concretizzata tra l'altro nella realizzazione di un dedicato sito *web*, l'*Asrar al Ghurabaa project*, atto a garantire la possibilità di comunicare in modalità "sicura" attraverso l'impiego della crittografia, quale strumento per la creazione di un ambiente assimilabile ad una sorta di "*safe haven* digitale". Quanto alle attività di propaganda, è risultato prevalente il ricorso a piattaforme di *social network*, attraverso cui sono stati gestiti centinaia di *account,* pubblicati e diffusi messaggi, immagini e video. A garanzia del "corretto" uso degli strumenti digitali, sono state altresì divulgate "raccomandazioni" per evitare, soprattutto, forme di geo-localizzazione da parte degli apparati di sicurezza. Emblematiche, nel senso, le molteplici operazioni di apertura e successiva chiusura, con cadenza periodica anche ravvicinata, dei profili sui *social media*, sovente con cambio di *nickname*, al fine di renderne ardua l'individuazione. Sebbene ad oggi non siano stati registrati attacchi di matrice terroristica contro sistemi *Infomation Technology* di rilevanza strategica, non va sottovalutato l'interesse di alcuni gruppi, così come dichiarato pubblicamente, ad effettuare attacchi *cyber* contro i sistemi e le reti di infrastrutture critiche di Stati Uniti ed Europa. Da evidenziare come la concretizzazione di tale interesse possa giovarsi della disponibilità di ingenti risorse economiche, impiegabili sia per acquisire strumenti atti a condurre azioni intrusive, sia per "assoldare" *team* di *hacker* esperti.

Al di là delle singole azioni intrusive ricondotte dai media all'IS per il tramite del *CyberCaliphate* – come quelle contro gli *account* dello *U.S. Central Command* e nei confronti di migliaia di siti francesi in rappresaglia delle azioni di *Anonymous* finalizzate a "vendicare" gli attentati in Francia – il fenomeno più significativo è dato dall'emergere di una inedita contrapposizione, destina-

ta a conoscere ulteriori sviluppi sul piano digitale, tra due attori della minaccia: l'IS ed *Anonymous*.

La criminalità informatica

Lo spazio cibernetico ha continuato a costituire terreno di operazioni anche per i **criminali informatici**, soprattutto nel settore dei cd. reati predatori, in ragione dei sempre più elevati valori economici che transitano o che sono gestiti in Rete. Il grado di rischio riconducibile al *cyber crime* è ritenuto alto, specie per la disponibilità, da parte dei relativi attori, di ingenti risorse economiche e di un discreto livello di *know-how* grazie all'arruolamento di *hacker* tecnicamente preparati e collegati tra di loro attraverso *network* di comunicazione riservati (*chat* e *forum* privati e cifrati, siti *web* inaccessibili al navigatore occasionale, etc.).

La presenza di un mercato nero del *cyber crime* sempre più strutturato, nel quale è possibile reperire strumenti e servizi utili per la commissione di illeciti nel dominio cibernetico, ha, da un lato, consentito la conduzione di attacchi sempre più sofisticati e, dall'altro, ha offerto la possibilità, anche ai tradizionali gruppi criminali organizzati (quelli che non si avvalgono della Rete), di acquisire capacità prima riservate solo ad esperti del settore.

Nel *cyber underground* (*vds. box n. 18*) sono rinvenibili diverse tipologie di programmi malevoli (*malware*) appositamente sviluppati per la loro immissione nel mercato nero.

Tra questi, oltre ai *trojan* diretti a sottrarre credenziali di accesso ai conti correnti ed alle connesse funzionalità bancarie *on-line*, sono stati registrati numerosi casi di *ransomware*, volti a criptare i *file* dei sistemi (*vds. box n. 18*). In aggiunta, si è rilevata una maggiore esposizione degli *smartphone* a tale tipologia di attacchi, attraverso varianti di *ransomware* sviluppati appositamente per la telefonia mobile.

Da evidenziare, inoltre, come le attività criminali *on-line* si siano avvalse dell'impiego di strumenti commerciali di anonimizzazione e criptazione, oltre che dell'uso di valuta virtuale.

Tra le tecniche di anonimizzazione più sfruttate si sono confermate i *Virtual Private Networks* (VPN) e la rete TOR (*vds. box n. 18*).

box 18

LE PAROLE DEL *CYBER*

Cyber underground. Con tale termine si indica generalmente quella parte del *web* (cd. *deep web* o *web* invisibile) non indicizzata dai comuni motori di ricerca ed accessibile solo attraverso specifici programmi come, ad esempio, TOR. Nel *cyber underground* si situa altresì il cd. *dark web*, così chiamato perché costituito da contenuti perlopiù illegali, intenzionalmente celati ed accessibili solo da chi è in possesso dello specifico indirizzo.

Cracker. Tale termine fu coniato dalla comunità *hacker* internazionale intorno agli inizi degli anni '90 per distinguere tale categoria dagli *hacker.* A differenza di questi ultimi, infatti, i *cracker,* pur impiegando tecniche analoghe, mirano a danneggiare volontariamente i sistemi *target* al fine di comprometterne l'integrità o causarne il malfunzionamento.

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*.

Hacker. Nella sua accezione originaria, con tale termine si indicava chi affronta sfide intellettuali, precipuamente in ambito tecnologico, per aggirare o superare alcune limitazioni intrinseche o imposte dall'esterno. Oggigiorno la declinazione, in termini negativi, di tale figura, lo identifica con il "pirata informatico", definibile come colui che si introduce abusivamente in un sistema informatico o telematico.

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*.

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.

Phishing. Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (*user-id*, *password*, numeri di carte di credito, PIN, etc.) con l'invio di false *e-mail* generiche a un gran numero di indirizzi. Le *e-mail* sono formulate in modo tale da convincere i destinatari ad aprire un allegato o ad accedere a siti *web* creati *ad hoc* dall'attaccante. Il *phisher* utilizza i dati raccolti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Ransomware. *Malware* diffuso sotto forma di allegato di posta elettronica apparentemente lecito e inoffensivo, che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione.

Spear phishing. Attacco informatico di tipo *phishing* condotto contro utenti specifici (ad es. *System Administrator*, *Program Manager*, etc.), condotto con l'invio di *e-mail* progettate per carpire informazioni sensibili dal destinatario.

TOR – The Onion Router. Rete inventata nel 1995 dalla *US Navy* per proteggere le comunicazioni governative statunitensi, oggi di pubblico dominio. Consiste in una rete di *router*, gestiti da volontari, che consentono l'anonimato e la criptazione delle comunicazioni poiché il pacchetto dati inviato, prima di giungere al *server* di destinazione, passa attraverso dei *router* intermedi che reindirizzano i dati costituendo un circuito crittografico a strati (da cui il termine *onion*). Tale strumento consente altresì di erogare "servizi nascosti", costituenti un vero e proprio mercato nero, ospitati su *server* che, facendo parte della stessa rete TOR, non sarebbero localizzabili. Essi peraltro sono accessibili solo da utenti di TOR.

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*.

VPN. Rete privata che impiega un sistema di trasmissione pubblico condiviso come, ad esempio, internet.

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.

AZIONE PREVENTIVA E PROSPETTIVE

Le reti di rilevanza strategica

Sul piano strutturale, l'attività di ricerca informativa ha mirato ad acquisire maggiore conoscenza dei **profili di criticità delle reti di rilevanza strategica per il Paese**, allo scopo di approfondirne gli aspetti gestionali e tecnologici, suscettibili di impattare sulla sicurezza e sull'integrità dello spazio cibernetico nazionale.

Le criticità emerse riguardo alle reti e alle infrastrutture per la connettività sono da ricondurre, in linea generale, a fattori tecnici nonché alla mancanza di una mappatura aggiornata dei flussi telematici nazionali. Mentre questi ultimi, sulla base di accordi economici tra i maggiori *carrier* a livello internazionale, possono attraversare il territorio di Paesi dotati di sensibilità giuridica diversa rispetto a materie quali la tutela della *privacy* e l'intercettazione delle comunicazioni, gli apparati e le tecnologie su cui si basano le citate infrastrutture potrebbero costituire, ove non dotati di adeguati livelli di protezione, un ulteriore *vulnus* per la riservatezza e l'integrità delle comunicazioni e la corretta funzionalità dei sistemi.

Le vulnerabilità dei sistemi

Quanto alla prevenzione della minaccia cibernetica, è stata incrementata l'attività di ricerca delle vulnerabilità riconducibili ai seguenti assetti:

- sistemi informatici industriali (*Supervisory Control And Data Acquisition* – SCADA), le cui principali criticità in ambito nazionale sono costituite dall'obsolescenza di impianti che, nati per operare in modo isolato, sono stati collegati e integrati nel corso del tempo a sistemi di nuova concezione per mezzo di reti aperte e non sufficientemente compartimentate. Molti sistemi SCADA, infatti, si basano su piattaforme informatiche datate e, in ra-

gione di ciò, vulnerabili a vecchi e nuovi *malware* – la cui diffusione sovente è da ricondurre a fornitori esterni – e difficilmente aggiornabili nel breve periodo per ragioni economiche e tecniche;

- piattaforme mobili (*tablet* e *smartphone*) che, caratterizzate da minori misure di sicurezza intrinseche rispetto ai *personal computer*, rappresentano un mezzo per la diffusione di codici malevoli, utili a perpetrare reati predatori, considerati gli accresciuti valori economici gestiti per mezzo di quei dispositivi;
- tecnologie di *cloud computing* (cd. *nuvola informatica*), che consentono ad una molteplicità di soggetti pubblici e privati di avvalersi di un servizio di *storage* dei dati e di elevati livelli di prestazione per la loro elaborazione, mediante un significativo contenimento degli oneri di implementazione e gestione diretta. In un'ottica di sicurezza nazionale, tuttavia, siffatte tecnologie possono presentare risvolti di criticità – laddove non accompagnate dall'adozione e dal rispetto di adeguate *policy* e misure di sicurezza – sotto il profilo della riservatezza e dell'integrità dell'informazione, con possibili ricadute in termini di violazione della *privacy*, della proprietà intellettuale e della tutela delle informazioni sensibili per il Paese. A rendere più articolato tale quadro possono intervenire, poi, i rischi connessi con la delocalizzazione dei *data center*, con conseguente memorizzazione dei dati su piattaforme dislocate all'estero, anche su più infrastrutture distribuite in località diverse per esigenze di ridondanza, a tutela della *business continuity* e del *disaster recovery*.

In ragione della rilevanza e della risonanza mondiale di ***Expo 2015***, è stata posta in essere anche una mirata azione di monitoraggio e di ricerca informativa nei confronti del primo evento nazionale *fully cloud powered*. L'elevata visibilità internazionale dell'evento potrebbe contribuire a rendere l'infrastruttura IT dello stesso un *target* appetibile per i diversi attori che operano nello spazio cibernetico.

La progressione della minaccia

Alla luce del delineato *trend*, è verosimile, per il 2015, il profilarsi di un ulteriore incremento della minaccia, a motivo sia della progressiva sofisticazione delle tecniche di attacco e di penetrazione informatica, sia dello sfruttamento di un ancora inadeguato livello di sicurezza tecnico-organizzativa e di percezione del rischio, sia, infine, per la continua espansione della "superficie di attacco", anche in ragione della crescente diffusione di applicativi per la telefonia mobile. Si valuta che gli attori ostili tenderanno a fare sempre più ricorso a tecniche di *spear phishing* (*vds. box n. 18*) e di ingegneria sociale, come il monitoraggio delle relazioni e delle abitudini di un soggetto sui *social media*, al fine di comprometterne apparati o servizi di posta elettronica per successive penetrazioni a cascata verso l'organizzazione *target* cui appartiene o cui risulti, in qualche modo, collegato. Tale scenario

è destinato a risentire anche di livelli talora non adeguati di investimenti nel settore della sicurezza ICT che, impedendo un congruo *standard* di sicurezza dei processi e dei servizi, fanno venir meno di fatto la prima, necessaria ed auspicabile misura per il contenimento della minaccia. In questo senso, le attività volte a ridurre la "superficie d'attacco" attraverso un ridimensionamento numerico dei *data center* pubblici – previsto dalla Strategia italiana per la crescita digitale (2014-2020) elaborata dalla Presidenza del Consiglio dei Ministri – risultano certamente funzionali allo scopo. Allo stesso tempo, similmente a quanto avviato da altri *partner* europei, le piccole e medie imprese nazionali potrebbero giovarsi di un ambiente *cloud* comune e sicuro, quale *driver* di crescita e protezione del proprio *know-how*. Da menzionare, infine, i rischi legati alla gestione della *supply chain* di operatori pubblici e privati, laddove una non adeguata cornice di sicurezza potrebbe esporre i prodotti e la componentistica IT a potenziali manipolazioni nei passaggi dal fornitore all'utente finale.

SCENARI E TENDENZE: UNA SINTESI

Nel corso del 2014 l'intelligence si è confrontata con uno scenario di minaccia composito, interconnesso ed in forte evoluzione, destinato a subire, anche nell'immediato futuro, l'effetto moltiplicatore di fattori altrettanto dinamici ed eterogenei, quali i riverberi della congiuntura economica, l'instabilità degli equilibri strategici internazionali e la fluidità dei modelli sociali.

Tra le sfide prioritarie figurerà ancora, trasversale quanto a genesi e ad ambito di proiezione, quella di un terrorismo jihadista in rinnovata fase ascendente tanto nella sua dimensione globale quanto nelle sue declinazioni regionali, rispetto al quale lo *Stato Islamico* continuerà ad esercitare spinta propulsiva per l'intera galassia jihadista.

Nella sua dimensione domestica, la minaccia terroristica sarà espressa soprattutto dall'estremismo *homegrown,* correlato a processi di radicalizzazione che maturano nel cuore delle società occidentali e che potranno trovare fonte di innesco e di ispirazione nell'effervescente e magmatico universo del jihadismo *on-line*: quest'ultimo per definizione in grado di mettere "in rete" individui ed organizzazioni, messaggi istigatori ed esperienze di combattimento, esecuzioni efferate e progettualità offensive. La natura liquida e ad un tempo pulviscolare della minaccia richiederà il massimo affinamento degli strumenti di prevenzione, la costante interazione tra intelligence e Forze di polizia e, soprattutto, rafforzati livelli di cooperazione internazionale utili a cogliere per tempo percorsi di radicalizzazione e segnali di allarme, nonché a monitorare gli spostamenti da e per lo spazio Schengen di militanti con cittadinanza europea. Ciò anche in relazione al flusso di aspiranti combattenti determinati a raggiungere i teatri di *jihad* e che al loro rientro in Paesi comuni-

tari potrebbero rappresentare un veicolo di minaccia terroristica. Il fenomeno dei *foreign fighters* e del connesso reducismo rappresenterà, verosimilmente, un capitolo ricorrente nell'agenda intelligence dei prossimi anni.

Anche in ragione della persistente insidiosità della minaccia jihadista e delle sue potenziali ripercussioni sulla sicurezza nazionale rivestiranno particolare rilevanza le evoluzioni nello scacchiere africano, dove le difficoltà dei processi di sviluppo e la complessità delle dinamiche politiche potranno offrire ulteriori spazi di agibilità alle organizzazioni terroristiche e alimentare il flusso di migranti clandestini in direzione dell'Europa. Specifico interesse continuerà a rivestire il Nord Africa, regione attraversata da accentuate criticità, dal particolare dinamismo delle formazioni estremiste e da diversificati processi di riassetto politico-istituzionale. Meritevoli di attenzione resteranno le evoluzioni nella fascia sahelo-sahariana, gravata da perduranti fattori di instabilità e sulla quale insistono numerose organizzazioni terroristiche. Nel contesto, assai pesanti si configurano le conseguenze dell'epidemia di febbre emorragica Ebola.

Gli sviluppi nel cd. Medio Oriente allargato – specie con riferimento alla conflittualità nel quadrante siro-iracheno, ai persistenti focolai di tensione nel contesto israelo-palestinese ed alla ridefinizione degli equilibri tra i maggiori attori dell'area – appaiono parimenti destinati ad esercitare un significativo impatto sugli interessi nazionali.

Sensibile si presenta il contesto afghano, dove la cornice securitaria potrà risentire dei tentativi dell'insorgenza di matrice *Taliban* di trarre il massimo vantaggio dalla rimodulazione della presenza internazionale, in un quadro generale che permane caratterizzato da contrapposizioni etniche e socio-economiche.

In Asia Centrale, regione di rilevanza strategica attraversata da irrisolti contenziosi ed al centro di una crescente competizione per lo sfruttamento delle ingenti risorse energetiche, l'interesse informativo sarà verosimilmente sollecitato dall'intensificazione delle attività condotte dalle locali organizzazioni jihadiste. Analoga effervescenza si coglie, altresì, nell'Asia centro-meridionale e sud-orientale, dove si profila un complessivo innalzamento della minaccia terroristica.

In linea di continuità con una tendenza già sottolineata nella precedente Relazione, la tutela del sistema Paese richiederà specifico e mirato *focus* dell'attività di ricerca ed analisi della comunità intelligence, anzitutto al fine di garantire il necessario supporto informativo all'azione di governo finalizzata all'attrazione degli investimenti esteri, preservando al contempo gli assetti strategici nazionali da operazioni acquisitive di natura predatoria suscettibili di ripercuotersi negativamente sui profili occupazionali e sulle politiche industriali di medio periodo.

Anche allo scopo di sostenere gli emergenti segnali di riavvio di un ciclo di crescita economica, seguiterà a rivestire rilie-

vo prioritario l'azione di contrasto tanto ai tentativi di sottrazione del *know-how* tecnologico, scientifico ed industriale nazionale a discapito del dinamismo del nostro sistema produttivo - sviluppati sempre più frequentemente anche nello spazio cibernetico – quanto alle minacce che possono pregiudicare la continuità ed economicità degli approvvigionamenti energetici. Queste costituiscono infatti requisiti imprescindibili per promuovere lo sviluppo economico e la competitività delle imprese nazionali. L'ottica è quella di un calibrato impegno intelligence sia a salvaguardia delle dinamiche di mercato in grado di favorire l'efficienza produttiva e allocativa, sia a presidio della solidità del sistema bancario e finanziario nazionale.

Profili di marcata insidiosità permarranno correlati alle infiltrazioni nella realtà economico-produttiva nazionale di organizzazioni criminali di stampo mafioso, che nella crisi di liquidità trovano ampi margini di manovra per operazioni acquisitive di aziende in difficoltà. Le ingerenze del crimine organizzato e di *lobby* crimino-affaristiche nella gestione della *res publica,* finalizzate a condizionare i processi decisionali, specie nel settore delle "grandi opere", saranno un ulteriore, prioritario *target* della ricerca informativa.

Sul piano delle dinamiche sociali, le criticità occupazionali protrattesi per tutto il corso del 2014 delineano per l'immediato futuro l'eventualità di un innalzamento del livello della protesta in realtà aziendali sensibili. Potranno scaturirne episodiche degenerazioni, anche violente, in un contesto che vede le componenti antagoniste interessate a strumentalizzare la protesta "anticrisi" in chiave di contrapposizione alle istituzioni. Specifico rilievo continuerà a rivestire la mobilitazione del movimento *No TAV*, alla ricerca di ulteriori occasioni di visibilità, mentre è destinata ad assumere crescente spessore la protesta contro l'*Expo 2015*.

Quanto alla minaccia eversivo-terroristica, i più rilevanti profili di rischio rimangono riferibili, nell'immediato, all'anarco-insurrezionalismo, determinato a rilanciare l'azione diretta nella sua accezione *distruttiva*, nel segno della *solidarietà rivoluzionaria*, anche internazionale, verso i militanti detenuti. Sul versante dell'estremismo marxista-leninista, è possibile che alcuni ristretti circuiti, che mantengono legami con brigatisti "irriducibili" del circuito carcerario, possano ritenere pagante il compimento di azioni dimostrative di modesto spessore intese a stimolare gesti emulativi e percorsi di riaggregazione delle *forze rivoluzionarie*.

La destra radicale dimostra, dal canto suo, un perdurante impegno mobilitativo nelle campagne sui temi tradizionali, volte a strumentalizzare il disagio sociale anche mediante iniziative di propaganda xenofoba. La crisi ucraina rappresenterà un significativo catalizzatore delle iniziative d'area, ma, al contempo, un fattore divisivo tra seguaci di Kiev e componenti filo-russe. Nei circuiti dell'ultradestra a vocazione più "militante" potrebbero trovare nuovo spazio, inoltre, spirali di conflittualità con attivisti anarchici e dell'antagonismo di sinistra.

Immanente, polimorfa e sempre più pervasiva si pone, infine, la minaccia che viaggia nel cyberspazio, espressione di progettualità ostili riferibili ad un ampio ed eterogeneo ventaglio di attori. Dallo spionaggio digitale all'hacktivismo di matrice antagonista, sino al *cyberjihad*, la minaccia cibernetica è da ritenersi concreta, attuale e con proiezione a medio-lungo periodo, in grado di impattare sulla sicurezza dei cittadini e sugli interessi politici, militari, economici, scientifici ed industriali del Paese.

In questo senso, i profili di maggior rischio saranno legati alla crescente sofisticazione delle tecniche di attacco, il cui potenziale d'incidenza sui sistemi e sulle reti risulterà tanto più rilevante in assenza di adeguati livelli di protezione e, prima ancora, di una condivisa consapevolezza della reale portata della minaccia. Al prevedibile incremento quantitativo e qualitativo degli attacchi dovrà dunque corrispondere il consolidamento dell'architettura nazionale *cyber,* imperniata sulle sinergie interistituzionali, sulla sempre più assidua interazione tra settori pubblico e privato e sull'imprescindibile rafforzamento della collaborazione internazionale, a livello sia multilaterale che bilaterale.

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

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

L'allegato alla Relazione annuale al Parlamento costituisce il "Documento di sicurezza nazionale" nel quale vengono compendiate le attività svolte dal Comparto intelligence – attraverso un articolato processo al quale partecipano fattivamente tutti i componenti dell'architettura *cyber* nazionale, così come delineata nel DPCM del 24 gennaio 2013 – in materia di protezione delle infrastrutture critiche materiali e immateriali, nonché di protezione cibernetica e sicurezza informatica nazionale.

Dopo l'adozione, nel dicembre 2013, del "Quadro Strategico Nazionale (QSN) per la sicurezza dello spazio cibernetico" e del correlato "Piano Nazionale (PN) per la protezione cibernetica e la sicurezza informatica nazionale"[1], il 2014 si è caratterizzato per una azione tesa a garantire l'ulteriore consolidamento della richiamata architettura, allo scopo di potenziare le capacità di protezione degli assetti cibernetici nazionali dai quali dipendono, sempre di più, la stabilità, la sicurezza e lo sviluppo del Paese.

Propedeutica a tale rafforzamento è stata, in primo luogo, l'implementazione delle linee d'azione previste dal PN. Nel senso, al fine di consentire all'Organismo di supporto al Comitato Interministeriale per la Sicurezza della Repubblica (il cd. CISR Tecnico, *vds. box n. 19*) la verifica dell'**attuazione degli interventi previsti nel "Piano Nazionale"**, nonché dell'efficacia delle procedure di coordinamento tra i soggetti pubblici e privati chiamati ad attuarli, il DIS – attraverso il Tavolo Tecnico *Cyber* (TTC), operante quale emanazione del CISR Tecnico – ha avviato la compilazione della "matrice di verifica", quale strumento idoneo a misurare, al termine del biennio di validità del PN (2014-2015),

[1] I documenti sono scaricabili al seguente link: *http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html*.

box 19

CISR, CISR TECNICO E TTC

Il **CISR** è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza. Il Comitato è presieduto dal Presidente del Consiglio dei Ministri ed è composto dall'Autorità Delegata e dai Ministri di Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico. Il Direttore Generale del DIS svolge al suo interno la funzione di segretario.

Il **CISR** è supportato dal cd. "**CISR Tecnico**" quale organismo collegiale permanente di coordinamento, presieduto dal Direttore Generale del DIS e composto dai Direttori di AISE ed AISI, oltre che dai Dirigenti di Vertice dei summenzionati Dicasteri.

Entrambi i consessi sono integrati dal Consigliere militare del Presidente del Consiglio, nel caso in cui gli stessi sono chiamati a trattare materie attinenti la sicurezza cibernetica.

Il **TTC**, istituito in seno al DIS il 3 aprile 2013 ed operante quale emanazione del CISR Tecnico, mira a garantire lo sviluppo dell'architettura nazionale *cyber* attraverso la "messa a sistema" delle molteplici e diversificate capacità ed esperienze in materia, nel rispetto delle competenze di ciascuna Amministrazione che lo compone.

Il Tavolo riunisce, con cadenza periodica, i PoC *cyber* dei Dicasteri CISR (Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanze e Sviluppo Economico), dell'Agenzia per l'Italia Digitale, del Nucleo per la Sicurezza Cibernetica, dell'AISE e dell'AISI.

il complessivo livello di crescita degli assetti *cyber* nazionali e la loro capacità di rispondere con efficacia alle sfide ed alle opportunità, rispettivamente, poste ed offerte dallo spazio cibernetico.

La lettura della "matrice di verifica" ha restituito, con riferimento al 2014, un quadro di situazione generale che ha visto le Amministrazioni impegnate nello svolgimento di attività finalizzate soprattutto:

- al reclutamento di personale specializzato, così da potenziare le dotazioni organiche delle strutture deputate alla sicurezza informatica;
- all'adozione di soluzioni tecnologiche per l'analisi del traffico di rete, la prevenzione della diffusione di *malware*, i servizi di investigazione degli incidenti di sicurezza e la correlazione dei relativi eventi;
- al potenziamento delle capacità di *auditing* e *penetration testing*;
- allo sviluppo delle capacità di analisi, anche attraverso l'acquisizione e la maggiore diffusione, tra le Forze di polizia, di strumenti operativi per la *digital forensic*;

- al rafforzamento dei siti di *disaster recovery* ed all'avvio di consultazioni per la realizzazione di un sito unificato di *disaster recovery* e *business continuity*;
- all'avvio di progetti per la trasformazione delle Unità Locali di Sicurezza dei singoli Ministeri in *Computer Emergency Response Team* (CERT) dicasteriali, aventi il compito di dare impulso all'attività di analisi, di valutazione delle minacce e delle vulnerabilità *(cyber situational awareness)*, nonché per consentire una valutazione sulle forniture *hardware* e *software* acquisite;
- allo sviluppo di rapporti di cooperazione internazionale a livello sia bilaterale sia multilaterale;
- al rafforzamento ed al miglioramento delle forme di partenariato con il settore privato, in particolare sulla tematica dell'individuazione di eventuali vulnerabilità di sistemi e reti;
- alla promozione del raccordo fra gli attori nazionali, specie in ambito accademico. Vale richiamare, sul punto, la creazione, frutto di una sinergia del Ministero dell'Interno con le principali Università italiane, di un "Centro studi e ricerche sul *cyber crime*". Tale Centro, che diverrà pienamente operativo nel corso del 2015, ha tra gli obiettivi l'elaborazione di metodologie e tecnologie innovative per la rilevazione e l'analisi

delle minacce e delle vulnerabilità, nonché lo sviluppo di adeguati strumenti di gestione del rischio;

- alla promozione ed alla diffusione della cultura della sicurezza informatica, attraverso attività di informazione, sensibilizzazione e formazione di base, nonché grazie alla partecipazione alla *"Cyber Europe 2014"* degli attori che compongono l'architettura nazionale *cyber* ;
- alla adesione a progetti finanziati dalla Commissione Europea. Significativo, in tale contesto, il progetto *Advanced Cyber Defence Centre*, al quale il Ministero dello Sviluppo Economico prende parte attraverso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, nel cui ambito quel Dicastero ha dato avvio alla realizzazione di un Centro Nazionale Anti-*botnet (vds. box n. 20)*, attraverso l'istituzione di un laboratorio per la raccolta e l'analisi di dati sulla loro diffusione di tali reati a livello nazionale.

Il **Tavolo Tecnico *Cyber* (TTC)** ha continuato, nel secondo anno di attività, a costituire un proficuo esercizio di coordinamento e sintesi delle iniziative poste in essere dalle diverse componenti, chiamate a fornire, oltre a punti di situazione aggiornati, apporti utili per la messa a regime di alcuni attori dell'architettura nazionale *cyber*, segnatamente del Nucleo per la Sicurezza Cibernetica (NSC), del CERT Nazionale (CERT-N) e del CERT della Pubblica Amministrazione (CERT-PA).

Per quel che concerne il **Nucleo per la Sicurezza Cibernetica**, è stato definito ed approvato lo schema per la gestione del flusso informativo *cyber* originato dalle Amministrazioni NSC e del processo da attivare in caso di crisi cibernetica. A tale schema, divenuto parte integrante della direttiva che disciplina il funzionamento del Nucleo, si è aggiunto il varo di *format* per:

- standardizzare le comunicazioni ascendenti verso il Nucleo sugli eventi rilevanti;
- favorire, su una base comunicativa omogenea, la circolarità informativa tra le varie Amministrazioni presenti nel NSC;
- identificare le piattaforme da utilizzare per lo scambio informativo in ragione della classifica ricoperta dalle segnalazioni.

box 20

LE *BOTNET*

Le cd. *botnet* sono reti di dispositivi informatici collegati ad internet ed infettati da *software* malevoli che ne consentono il controllo da remoto. Si tratta di "reti di robot", da cui deriva il nome. Le *botnet* sono normalmente impiegate per condurre attacchi di negazione di un servizio *on-line*, ovvero per l'invio di *e-mail* di *spam* o per la diffusione di *malware*.

Con riguardo al **CERT-N**, che nel mese di novembre ha reso operativo il proprio sito *web* (*www.certnazionale.it*), il Ministero dello Sviluppo Economico, allo scopo di assicurarne la piena operatività, ha attivato canali di interazione con il CERT-UE, con analoghe strutture di molteplici Paesi europei e con quello statunitense.

Una serie di incontri, inoltre, di quel Dicastero con soggetti pubblici (AgID/CERT-PA, Ministero dell'Interno/Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC e Ministero della Difesa), con Poste Italiane, con i principali operatori di telecomunicazione e con infrastrutture energetiche hanno portato alla sottoscrizione di accordi di collaborazione. Colloqui di analogo tenore sono in corso anche con altre telco, società energetiche, di trasporto e finanziarie.

All'istituzione di un Tavolo Tecnico Permanente, nel cui ambito sono state definite, tra l'altro, le procedure per la condivisione delle informazioni, si è affiancata la sperimentazione di una piattaforma, messa a disposizione dal Ministero della Difesa, al fine di agevolare l'*info-sharing* tra CERT-N e soggetti pubblici e privati.

Per quel che concerne il **CERT-PA**, nel corso della fase pilota – cui hanno partecipato, oltre a Consip, i Dicasteri degli Esteri, della Giustizia, dell'Economia e Finanze (tramite Sogei) e dello Sviluppo Economico – ha dato avvio all'emissione di bollettini e avvisi per la PA sui rischi correlati alle minacce cibernetiche. In parallelo, è stato dato impulso ad un'attività di sviluppo e di verifica della procedura di *Incident Response* della PA (IRPA), utile a supportare e coordinare le Amministrazioni nelle operazioni di prevenzione, risposta e ripristino dagli incidenti.

L'AgID, inoltre, sotto la cui egida il CERT-PA opera, ha provveduto alla redazione ed all'emanazione presso la *costituency* di riferimento (PA centrali e locali) delle Regole Tecniche di Sicurezza Informatica e delle relative Linee Guida. Per quel che concerne i rapporti con omologhe strutture sono stati siglati, nel 2014, *Memorandum of Understanding* con i CERT Nazionale dell'INAIL. Sono state avviate le attività per la sigla di un medesimo accordo con il Ministero della Difesa, ancorché, sono già in essere scambi di informazioni e collaborazione in attività inerenti il settore in argomento con il CERT Difesa.

È stato altresì messo *on-line* il portale *www.cert-pa.it*, che ospita la piattaforma di *info-sharing*, ad accesso protetto, sulla qua-

le i referenti di quei CERT acquisiscono la documentazione di sicurezza.

Tra le altre iniziative assunte dal DIS per il tramite del TTC – la maggior parte delle quali finalizzate a supportare, con prospettive diverse, la **PROMOZIONE E DIFFUSIONE DELLA CULTURA DELLA SICUREZZA CIBERNETICA** – vanno richiamate quelle con il mondo accademico e con i centri di ricerca, anche attraverso la messa a punto di progetti tesi a valorizzare, nel corso del semestre di presidenza italiana del Consiglio dell'Unione Europea, l'attenzione del nostro Paese verso la *cyber security*.

I contatti con il mondo accademico hanno conosciuto un ulteriore consolidamento con la firma, nel mese di ottobre, di un **ACCORDO DI COLLABORAZIONE** tra il DIS ed il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), volto alla creazione di un rapporto di cooperazione nel settore della sicurezza cibernetica, finalizzato allo svolgimento di attività di ricerca e sviluppo ed alla realizzazione di iniziative formative.

A valle del citato accordo, il DIS ha supportato attivamente la creazione, nell'ambito del citato Consorzio, del **LABORATORIO NAZIONALE DI *CYBER SECURITY***.

Tale struttura, che federa oltre 250 tra professori e ricercatori provenienti da 32 Università italiane, ha, quale duplice obiettivo, quello di mettere a sistema le capacità di ricerca nazionali di settore attraverso un'azione di coordinamento delle eccellenze esistenti e di dare vita ad un flusso informativo tra i membri del Laboratorio e tra questi ed il mondo esterno. Ciò, a fronte della crescente consapevolezza che l'economia reale del Paese, sempre più legata all'uso del *cyber space*, è destinata a prosperare nell'ambito di un dominio cibernetico resiliente e sicuro. Il Laboratorio, quale motore di innovazione, mira in particolare a supportare il sistema Paese di fronte alla minaccia cibernetica, attraverso:

- il miglioramento della continuità di servizio dei sistemi critici;
- l'accrescimento della consapevolezza della minaccia presso la società;
- il potenziamento delle misure di protezione da attacchi cibernetici nella PA e nelle imprese;
- il supporto ai processi di definizione di *standard* e *framework* metodologici a livello nazionale.

A cavallo tra collaborazione scientifica e *partnership* pubblico-privato si è collocata, poi, la presentazione, in dicembre, presso il Consiglio Centrale Piccola Industria di Confindustria, del rapporto, redatto dalla società di studi economici Nomisma in collaborazione con il DIS, sulla "Percezione della minaccia cibernetica nelle imprese italiane".

Lo studio, incentrato sulle PMI, in quanto catena di valore strategico del sistema economico nazionale, ha confermato come la percezione della minaccia e dei suoi possibili impatti permanga debole e poco diffusa.

Nove i settori economici sottoposti ad esame poiché ritenuti potenziali *target*: meccanica, automazione, meccatronica, nanotecnologie, ICT, *automotive*, sistemi avanzati di elettronica per la difesa ed applicazioni civili, prodotti chimici per usi industriali e tecnologie pulite (acqua, rifiuti solidi ed energie rinnovabili). Tra gli esiti più significati emersi dall'analisi vi sono:

- l'impiego del *malware* quale principale tipologia di attacco con effetti di malfunzionamento/danneggiamento di risorse informatiche e di inaccessibilità dei contenuti del sito *web* o di altre risorse informatiche;
- modesti investimenti di settore, che, a fronte della dichiarata discreta sensibilità del *top management* aziendale rispetto al tema della sicurezza *cyber*, non superano, nella maggior parte delle imprese intervistate, l'1% dei rispettivi fatturati.

Significativo e corale è stato, inoltre, l'impegno nazionale per la partecipazione alla **"*Cyber Europe 2014*"**, definita la più complessa ed estesa esercitazione mai svoltasi in ambito europeo, alla quale hanno preso parte oltre 400 esperti provenienti da più di 200 realtà pubbliche e private di 29 Stati europei.

L'esercizio – gestito dall'Agenzia Europea della Sicurezza delle Reti e delle Informazioni (ENISA) – ha previsto tre fasi:

- una tecnica, svoltasi in aprile, che ha riguardato la rilevazione, l'analisi e la mitigazione di incidenti di sicurezza informatica;

- una operativa, tenutasi nel mese di ottobre, che ha affrontato la gestione della crisi, la cooperazione, il coordinamento e lo scambio di informazioni;
- una strategica, da sviluppare nel 2015, incentrata sui processi decisionali, gli impatti politici e le pubbliche relazioni.

Per l'Italia – che ha partecipato con il CERT-N, il CERT-PA, il CERT-Difesa, il CNAIPIC, il Ministero dello Sviluppo Economico e le Unità Locali di Sicurezza (ULS) del Ministero degli Affari Esteri e di quello dell'Economia e Finanze, mentre per il settore privato con Terna, Enel, Wind e Poste Italiane – la "*Cyber Europe 2014*" ha rappresentato un'utile occasione per porre in essere un ulteriore *fine-tuning* delle procedure e dei meccanismi dello scambio informativo tra i soggetti pubblici e privati che compongono l'architettura nazionale *cyber*.

Il **SEMESTRE ITALIANO DI PRESIDENZA DELL'UNIONE EUROPEA** si è caratterizzato per una nutrita serie di eventi, alcuni dei quali oggetto di trattazione anche in seno al TTC, volti ad affrontare la specifica tematica della sicurezza cibernetica. Su tutti si evidenziano:

- *Digital Venice* (Venezia, 8 luglio) articolato in una sessione plenaria, alla quale hanno partecipato i Capi di Stato e di Governo dei 28 Paesi membri dell'UE, ed in *workshop* tematici, cui hanno preso parte oltre duecento esperti, focalizzati in particolare sull'*e-economy*, sul Mercato Digitale Unico, nonché sullo *smart-government* e sulla modernizzazione del settore pubblico. A conclusione dell'evento, destinato a rivestire periodicità annuale, è stata approvata la "Dichiarazione di Venezia" il cui punto saliente è stato il riconoscimento del paradigma della sicurezza come motore di sviluppo;
- *Workshop* tecnico, "*back to back*" con *Digital Venice*, organizzato dall'Istituto Superiore delle Telecomunicazioni del MiSE su proposta della Commissione Europea e con il supporto dell'Agenzia ENISA, finalizzato ad individuare i possibili strumenti per migliorare la cooperazione tra i CERT nazionali e governativi europei;
- Riunione, a cura del citato Istituto Superiore, del *Management Board* dell'Agenzia ENISA (11 settembre);
- Convegno su *e-Justice* (Roma, 13-14 ottobre), organizzato dal Ministero della Giustizia ed ospitato dalla Corte di Cassazione, nel quale è stato evidenziato come l'informatica contribuisca a dare ulteriore impulso alla creazione di uno spazio giuridico europeo di libertà, giustizia e sicurezza, che non può prescindere dalla soluzione di problematiche legate alla tutela dei dati personali giudiziari, alla rilevanza dei flussi informativi ed alla sicurezza dei sistemi;
- *Workshop* sulla sicurezza dei sistemi bancari *"Fighting Financial Cybercrime"* (Milano, 24 ottobre), organizzato dal Servizio di Polizia Postale e delle Comunicazioni della Polizia di Stato congiuntamente con l'Associazione Bancaria Italiana (ABI), mirante a promuovere e sviluppare una maggiore collaborazione tra settore pubblico e privato nel contrasto

ai crimini economico-finanziari *on-line*;

- Seminario *"The role of Cyber Defence to protect and sustain EU economy"* (Roma, 30 ottobre) organizzato dal Ministero della Difesa. L'agenda, il cui sviluppo è stato affidato a qualificati relatori tra cui i rappresentanti del NATO *Cooperative Cyber Defence CoE* (CCDCoE) e di alcune istituzioni europee, quali CERT-UE, ENISA ed *European Defence Agency*, ha focalizzato l'attenzione, in modo particolare, sulla cooperazione tra settore pubblico e privato e con il mondo accademico.

Per quel che concerne le attività di portata più propriamente operativa, il DIS ha continuato a potenziare la cooperazione con i Ministeri dell'Interno e della Difesa, così da rendere più sistemica la *partnership* con due attori chiamati a svolgere, ciascuno per le parti di rispettiva competenza, un ruolo di primo piano in materia di sicurezza e difesa cibernetica.

Di rilievo la definizione di un più strutturato scambio informativo del Comparto intelligence con il **Ministero dell'Interno-CNAIPIC**, nella prospettiva di favorire un ulteriore consolidamento dell'architettura nazionale e di supportare l'attività sia d'indagine a contenimento degli attacchi, sia di analisi in un'ottica più propriamente intelligence.

A tal fine, è stato redatto un protocollo d'intesa, in fase di finalizzazione, con il quale le due parti si impegnano a sviluppare un piano di collaborazione volto essenzialmente alla condivisione di informazioni idonee a prevenire ed a contrastare attacchi informatici di matrice criminale in pregiudizio delle infrastrutture critiche informatizzate di interesse nazionale, così come individuate nel Decreto del Ministro dell'Interno del 9 gennaio 2008.

Sempre nell'ottica di agevolare lo scambio informativo, specie alla luce della positiva esperienza maturata in ambito TTC, il DIS ha provveduto a realizzare un'apposita *"Piattaforma di Cyber Collaboration"* non classificata con i gestori di servizi di pubblica utilità e con gli operatori delle principali infrastrutture critiche nazionali, che consente una tempestiva condivisione di informazioni relative a potenziali minacce, offrendo altresì la possibilità agli *stakeholder* privati di acquisire dati tecnici, utili ad implementare il perimetro di sicurezza dei propri sistemi e reti.

Tali operatori, con i quali il DIS ha sottoscritto nel 2013 apposite Convenzioni, siedono al **"Tavolo Tecnico Imprese" (TTI)** che, istituito presso lo stesso DIS e riunitosi con periodicità nel 2014, ha rappresentato la sede per l'effettuazione di punti di situazione aggiornati sullo stato della minaccia *cyber* in Italia, con particolare *focus* sugli aspetti di primario interesse per il settore privato. Al fine, poi, di rendere più efficace la collaborazione tra Comparto e gestori è stato avviato un processo di condivisione di strumenti metodologici elaborati in ambito intelligence con l'obiettivo di pervenire alla definizione di un linguaggio e di un *modus operandi* comuni. In particolare, oggetto dello *sharing* sono stati un documento di *"triage"* da impiegare per la classificazione degli eventi *cyber* in base

al loro livello di rilevanza e gravità e una tassonomia, tesa alla definizione di un sistema di reportistica dei citati eventi, che contempli tutte le voci di interesse, anche ai fini dell'individuazione delle pertinenti misure di prevenzione ovvero di mitigazione e ripristino.

L'obiettivo di creare un funzionale e sistemico collegamento nazionale in materia *cyber* ha comportato, infine, lo sviluppo di una mirata attività di sensibilizzazione da parte dell'intelligence nei confronti anche di altri soggetti di rilevanza strategica per la sicurezza nazionale, come gli operatori del settore bancario-finanziario, al fine di garantire loro adeguata copertura informativa.