ATTI PARLAMENTARI

XVII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **XXXIII**
n. **4**

RELAZIONE
SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA
(Anno 2016)

(Articolo 38 della legge 3 agosto 2007, n. 124)

Presentata dal Presidente del Consiglio dei ministri

(GENTILONI SILVERI)

Trasmessa alla Presidenza il 24 febbraio 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2016

EXECUTIVE SUMMARY

Con la presente Relazione, il Governo riferisce al Parlamento sulla politica dell'informazione per la sicurezza e sui risultati ottenuti nel corso del 2016, ai sensi dell'art. 38 della Legge n. 124 del 2007.

La **PREMESSA** delinea, in uno scenario aperto, fluido e interconnesso, caratterizzato da importanti fattori di discontinuità negli equilibri geopolitici e strategici, le rilevanti sfide con cui l'intelligence è chiamata a confrontarsi nello svolgimento della propria missione di tutela della sicurezza nazionale, condotta coerentemente con la pianificazione strategica degli obiettivi informativi indicati dall'Autorità di Governo. Rispetto a tali obiettivi vengono quindi declinate, integrando sviluppi d'area e fenomeni di minaccia, le linee dell'azione intelligence nel corso del 2016.

pagg. 5 – 21

Il terrorismo internazionale di matrice jihadista, minaccia destrutturata, pervasiva e proiettata ormai su un teatro globale, determina la necessità di forme sempre più evolute di cooperazione internazionale alle quali il nostro Paese è in grado di fornire un contributo di rilievo, potendo contare su un dispositivo basato – in modo più accentuato rispetto a quanto avviene per molti altri Paesi – sullo scambio informativo e sulla costante sinergia tra Forze dell'ordine e Istituzioni che concorrono alla sicurezza nazionale; fattori, questi, che trovano il momento di massima sintesi nel Comitato di Analisi Strategica Antiterrorismo (CASA).

L'attività informativa in direzione del fenomeno migratorio, svolta in costante coordinamento interistituzionale, viene delineata in relazione al monitoraggio delle cause del fenomeno, tra cui rileva anche la scarsità delle risorse imputabile alla deriva climatica globale, e delle sue implicazioni securitarie, con specifico riferimento sia ai contesti di instabilità dai quali gli stessi originano, sia al rischio di infiltrazioni o contaminazioni terroristiche.

A seguire, sono enucleati i diversi piani sui quali si sviluppa il presidio intelligence del sistema Paese, realizzato secondo un accresciuto dialogo tra intelligence e operatori economici nazionali, anche per elevarne il grado di consapevolezza, con specifica attenzione per i gestori di infrastrutture critiche (reti di comunicazione, di distribuzione dell'energia e di trasporto) e di altri *asset* strategici.

Con riguardo alla dimensione cibernetica della minaccia, in grado di produrre effetti di estrema gravità fino alla paralisi di settori vitali del Paese, il coinvolgimen-

to dell'intelligence è declinato su più livelli di intervento, dalla raccolta e analisi di informazioni all'attività di supporto manutentivo dell'architettura nazionale cibernetica di reti e sistemi pubblici e privati.

Nel prosieguo, il richiamo all'evoluzione del ruolo dell'intelligence vale a tratteggiare i progressi raggiunti in direzione di un sistema integrato per la sicurezza del Paese che passa, tra l'altro, per il consolidamento della *partnership* pubblico-privato e per l'affinamento delle *policy* di reclutamento, con particolare accento sul potenziamento degli assetti preposti a settori peculiari tra cui *l'Information & Communication Technology* –ICT.

Attengono alla valenza strategica del rapporto tra intelligence e Università i riferimenti alla costituzione, nell'ambito della collaborazione con il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), di un laboratorio di studio in materia di *cybersecurity* per lo sviluppo di progetti di ricerca e formazione nello specifico settore. Analogo peso specifico è attribuito alla conclusione di Protocolli d'Intesa con il Ministero per l'Istruzione, l'Università e la Ricerca e con la Conferenza dei Rettori delle Università Italiane (CRUI). È ancora il mondo universitario il destinatario, nell'ambito dell'attività per la diffusione della cultura per la sicurezza, delle ulteriori 6 tappe del *roadshow* "*Intelligence live*" effettuate presso Atenei e centri di eccellenza nel corso del 2016, che vanno ad aggiungersi alle 21 già realizzate in precedenza.

Chiudono il capitolo introduttivo le positive linee di consuntivo dell'azione svolta nel 2016 ed il tratteggio degli impegni a venire, a cominciare dai risvolti securitari degli importanti appuntamenti del 2017: la celebrazione dei 60 anni dell'Unione Europea (25 marzo) e le riunioni del G7 (*in primis* l'appuntamento italiano a Taormina, 26-27 maggio).

L'esposizione cede quindi il passo al corpo centrale del documento, strutturato per offrire un quadro delle attività svolte rispetto alle tematiche alla prioritaria attenzione.

Il primo capitolo è dedicato alla **DERIVA JIHADISTA** e delinea in esordio i *trend* della minaccia nel 2016, che testimoniano, da un lato, un significativo arretramento territoriale di DAESH nei quadranti di riferimento determinato dall'intervento militare della Coalizione, dall'altro, un'accentuazione della risposta asimmetrica al di fuori dei territori di elezione mediante un'intensa campagna di attentati terroristici, in Europa e in altri importanti teatri. Sul tema della comunicazione strategica delle principali formazioni jihadiste, è delineato un nesso tra le prime sconfitte di DAESH sul terreno ed il rilevato ridimensionamento dell'apparato mediatico dell'organizzazione, quest'ultimo riflesso, sul piano dei contenuti, in una progressiva attenuazione dei richiami alle conquiste territoriali. *pagg. 23 – 29*

Occupa uno specifico paragrafo, dal titolo **IL JIHAD IN EUROPA**, il tema dell'esposizione del Vecchio Continente alla minaccia terroristica, testimoniata, oltre che dagli attacchi occorsi nel 2016, anche dalle numerose pianificazioni sventate o fallite e dall'incremento delle segnalazioni concernenti progettualità offensive. Per quanto attiene in particolare al rischio di attentati in territorio italiano, si conferma come i principali profili di criticità continuino a provenire dalla possibile attivazione di *lone wolves* e *self-starters*, ovvero da elementi auto-radicalizzati. *pagg. 30 – 33*

L'attivismo delle principali formazioni terroristiche nelle aree di instabilità rappresenta l'asse portante del paragrafo su **GLI SCENARI REGIONALI**, che in primo luogo illustra la presenza di DAESH in Africa, con specifico *focus* sul ruolo acquisito dall'organizzazione nel contesto libico e sulla sua espansione nel resto del Maghreb, specie in Algeria, tradizionale feudo d'elezione di *al Qaida nel Maghreb Islamico* (AQMI). A seguire sono enucleate le evoluzioni del fenomeno in altre aree del Continente africano. L'attenzione si sposta poi al Medio Oriente per appuntarsi innanzitutto sull'evoluzione nel contesto siro-iracheno, epicentro della minaccia simmetrica rappresentata da DAESH, e soffermarsi quindi sulle capacità dell'organizzazione di proiettare la propria azione all'esterno del *Syrak*, emblematicamente espresse dalla campagna terroristica contro la Turchia, dagli attentati realizzati nella Capitale egiziana e nella Penisola del Sinai, dall'espansione nello Yemen, dalla rafforzata presenza nella regione Afghanistan-Pakistan e nel Sud-Est asiatico. *pagg. 33 – 42*

LA FINANZA DEL TERRORISMO conclude il tema del *jihad* tracciando la sempre più accentuata tendenza di quei circuiti alla diversificazione, sia per quanto attiene a fonti e canali di approvvigionamento, sia in merito agli strumenti impiegati per il trasferimento dei fondi. *pagg. 42 – 43*

Il secondo capitolo è riservato al **FENOMENO MIGRATORIO NELLA PROSPETTIVA INTELLIGENCE** e ne illustra la geografia dei flussi e gli attori coinvolti, evidenziandone inoltre la connotazione sempre più strutturale e l'ampiezza delle dimensioni. La trattazione si sofferma in particolare sul ruolo preminente della rotta libica, specie per il trasferimento dei migranti provenienti dal Corno d'Africa e dal Golfo di Guinea. Sono evidenziate, inoltre, le conseguenze della chiusura della cd. *rotta balcanica* e le dinamiche che interessano le aree secondarie di imbarco lungo la direttrice del Mediterraneo orientale. Né mancano riferimenti ai rischi di infiltrazioni terroristiche nei flussi clandestini e al fenomeno del falso documentale, crescente ambito di contiguità tra circuiti criminali e *network* terroristici. *pagg. 45 – 52*

Alla **TUTELA DEL SISTEMA PAESE** è dedicato il capitolo successivo, che esordisce con il monitoraggio informativo degli interessi stranieri volti all'acquisizione di *know-how* altamente specializzato in settori strategici per l'Italia con lo scopo di offrire supporto al decisore politico nell'applicazione del cd. *golden power*. La trattazione prosegue evidenziando, con riferimento alla tutela del sistema bancario e finanziario, le direttrici lungo le quali si è mossa la ricerca informativa di AISE e AISI: in primo luogo le dinamiche dei mercati finanziari internazionali per individuare tempestivamente eventuali fattori di rischio; in secondo luogo, al fine di intercettare profili di criticità per gli interessi nazionali, le strategie dei grandi fondi d'investimento e delle istituzioni finanziarie internazionali. Specifico interesse è attribuito, altresì, alle dinamiche relative ai crediti deteriorati in relazione ai possibili rischi per la stabilità del nostro sistema creditizio. *pagg. 53 – 66*

Viene richiamata inoltre l'azione intelligence a salvaguardia del *know-how* industriale e commerciale italiano e a tutela del nostro tessuto imprenditoriale, in cui prevalgono le piccole e medie imprese, da investimenti esteri a carattere speculativo o non strettamente economico, anche in relazione alle possibili ricadute occupazionali e al rischio di trasferimento all'estero di *asset* strategici. È fatto riferi-

mento, altresì, al supporto offerto dall'intelligence all'internazionalizzazione delle imprese nazionali.

Un passaggio sulla tutela degli approvvigionamenti energetici illustra le variabili che hanno condizionato nel corso dell'anno il mercato mondiale degli idrocarburi, ponendo l'accento sull'instabilità della Libia e sulle strategie economico-commerciali di primari operatori esteri suscettibili di incidere significativamente sulla sicurezza energetica del Paese.

L'esposizione prosegue con le economie illegali, in particolare evasione ed elusione fiscale e riciclaggio di denaro, che hanno richiamato l'attenzione informativa specie in relazione alle condotte tese a schivare gli effetti della cd. *voluntary disclosure*. A seguire, sono declinati i settori dell'economia legale sui quali si concentra l'interesse della criminalità organizzata, nonché l'attenzione di quegli ambienti per i flussi di migranti clandestini quali bacini di reclutamento per fini di manovalanza e di sfruttamento sessuale. È dato poi rilievo ai caratteri distintivi dei diversi sodalizi criminali stranieri attivi sul territorio nazionale.

Ai profili di rischio correlati alle **SPINTE EVERSIVE ED ANTI-SISTEMA** è dedicato il terzo capitolo. L'attenzione è rivolta *in primis* alla minaccia di segno anarco-insurrezionalista, confermandone l'attualità, e all'estremismo marxista-leninista, del quale sono illustrati dinamiche ed ambiti di attività. Sono poi annoverati i temi più ricorrenti della protesta, di segno antagonista, centrata nel 2016 sul contrasto alle politiche economiche del Governo e alle misure richieste dall'UE nonché, nell'ultima parte dell'anno, sul referendum costituzionale, percepito come opportunità per coagulare le varie istanze sociali anti-governative. Volgendo lo sguardo alle dinamiche della destra radicale, l'accento cade sulle persistenti divisioni interne e le dinamiche competitive.

pagg. 67 – 78

Come da prassi consolidata, il capitolo **SCENARI E TENDENZE: UNA SINTESI** rappresenta il momento di passaggio tra l'azione svolta, in un 2016 costellato di rilevanti evoluzioni ed accelerazioni geopolitiche, economiche e securitarie, e le grandi sfide, complesse e interconnesse, con cui l'intelligence dovrà misurarsi nell'immediato futuro, nell'arco di un 2017 che si prospetta denso di opportunità ma anche di grandi incertezze, con dinamiche passibili di alterare nel tempo, in modo anche significativo, lo scenario internazionale ed interno conosciuto negli ultimi anni.

pagg. 79 – 85

L'allegato **DOCUMENTO DI SICUREZZA NAZIONALE** fa stato del ruolo svolto dall'intelligence rispetto alle principali iniziative architetturali volte a potenziare le capacità cibernetiche del nostro Paese e concretizzatesi nella revisione del Quadro Strategico Nazionale e del Piano Nazionale. Un passaggio è dedicato all'adozione, a livello europeo, della Direttiva in materia di sicurezza di *Network and Information System* (NIS), che ha costituito un'occasione per l'assunzione di più mirate azioni di manutenzione delle strutture a presidio dello spazio cibernetico. Non mancano riferimenti all'ampliata sinergia interistituzionale, coordinata attraverso il Tavolo Tecnico *Cyber*-TTC, e al rafforzamento del Partnerariato Pubblico Privato nell'ambito del Tavolo Tecnico Imprese-TTI. La trattazione si sposta quindi sulla dimensione fenomenologica del *cyberthreat* per illustrare, in linea con l'approccio redazionale già adottato nell'edizione 2015, anche lo stato della minaccia cibernetica in Italia e le sue possibili evoluzioni, declinandone direttrici e paradigmi comportamentali.

pagg. 1 – 33

RELAZIONE SULLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA 2016

La Relazione al Parlamento in versione digitale

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

È possibile visualizzare e scaricare il documento accedendo al seguente *link*: *http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione2016.html* oppure utilizzando il *QR Code* riportato in basso.

Dato alle stampe il 20 febbraio 2017

relazione sulla politica dell'informazione per la sicurezza

INDICE

PREMESSA

Continuità nella eccezionalità

In apparente paradosso, il dato di continuità che lega il 2016 agli anni precedenti è quello di una prolungata discontinuità, ovvero del verificarsi di eventi così rilevanti da far preconizzare conseguenze di ampia portata.

Sviluppi...

Il 2016 ha fatto registrare due sviluppi in grado di influire sugli equilibri geopolitici su scala mondiale e cioè il voto referendario, in Gran Bretagna, a sostegno della *Brexit* e l'affermazione, negli USA, di un'Amministrazione con un'agenda fortemente innovativa nel segno di un profondo cambiamento.

Molti analisti, sullo sfondo di tali risultati, hanno evocato il tema di una graduale erosione del ruolo e dello stile di vita delle classi medie rispetto a un processo di globalizzazione percepito da segmenti delle società economicamente più avanzate come causa di disuguaglianze e, conseguentemente, di una dilatata base di disagio, disoccupazione e povertà.

...tendenze...

La tendenza ad un progressivo ripiegamento sulla dimensione interna – declinatasi, a livello europeo, anche in una strisciante disaffezione verso il progetto di integrazione politica – si è accompagnata, più in generale, a segnali di un accresciuto protagonismo degli Stati-nazione in termini di reciproca, intensificata competizione, di assertività sulla scena internazionale e di emancipazione rispetto all'influenza delle istituzioni sovranazionali.

È andata inoltre consolidandosi la percezione di una insufficiente incisività della Comunità internazionale a fronte delle perduranti situazioni di conflitto in numerose aree del mondo e soprattutto nella regione mediterranea.

..e sfide

Nel contempo, tre sfide rilevanti e tutt'altro che inedite, vale a dire il contrasto al terrorismo jihadista, la sicurezza delle frontiere e la crescita economica, hanno confermato, con sempre più plastica e drammatica evidenza, il loro carattere di priorità ed urgenza nelle agende politiche di numerosi Governi. Si tratta di sfide che per natura e incidenza sulla dimensione domestica postulano un'azione strutturata in grado, a livello statuale, di coniugare al meglio politiche interna ed estera e, sul piano multilaterale – specie in organizzazioni più integrate come quella europea – di sollecitare una strategia di maggior coesione ed unità d'intenti. Ciò per corrispondere più efficacemente alle aspettative delle opinioni pubbliche correlate ad un avvertito senso di vulnerabilità per la sempre più pervasiva violenza terroristica, all'impatto divisivo dei flussi migratori di massa, alle istanze di revisione del sistema di *governance* degli squilibri indotti a livello locale dalla mondializzazione degli scambi.

L'Europa che verrà

Nell'incertezza e nella fluidità degli scenari, un dato certo è che le vicende che hanno attraversato il 2016 e, soprattutto, le interconnessioni dinamiche tra sviluppi politici, linee di tendenza e sfide securitarie trovano nel continente europeo un significativo catalizzatore sul piano strategico.

La presa d'atto di una realtà complessa e in rapido mutamento ha concorso ad animare il dibattito sull'Europa: ci attende una stagione di riflessione e confronto – peraltro in concomitanza con tornate elettorali in Paesi fondatori della UE – su correttivi, rimodulazioni e rinnovate architetture funzionali a imprimere reiterato impulso al percorso di integrazione europea.

L'appuntamento della celebrazione, a Roma, del 60° anniversario della firma dei Trattati europei fornirà l'occasione per verificare orientamenti, opportunità e linee di convergenza.

L'orizzonte geopolitico e securitario dell'Italia

Il nostro Paese guarda alle evoluzioni in atto con una duplice consapevolezza: da un lato, la pronunciata esposizione dell'Italia alle sfide rappresentate dal terrorismo jihadista, dai massicci flussi migratori irregolari e da una non ancora piena ripresa economica e, dall'altro, la necessità di perseverare nelle tradizionali linee di politica estera, fondate sul solido rapporto transatlantico, sulla convinta adesione al progetto europeo e sulla tradizionale funzione di cerniera geostrategica tra Nord e Sud del Mediterraneo.

Il rafforzamento dell'Unione Europea – con gli opportuni ribilanciamenti che tengano in debito conto le peculiarità degli Stati membri – rappresenta un obiettivo ineludibile, non solo perché nell'attuale contesto globalizzato la dimensione europea di un mercato unico di circa 500 milioni di consumatori assicura potere negoziale, massa critica, attrattiva per gli investimenti e capacità di resilienza, ma anche e soprattutto per i riflessi sul piano della sicurezza.

In coerenza con la visione di un'Europa "sostenibile" – e di un interesse nazionale a mantenere aperti mercati di sbocco per le nostre esportazioni – resta centrale la vocazione mediterranea del nostro Paese, con una crescente attenzione all'Africa quale retroterra strategico le cui dinamiche sempre più si intersecano con quelle del *Mare Nostrum*.

Il valore aggiunto dell'intelligence

In uno scenario aperto ed interconnesso, la capacità di lettura anticipata dei segnali di discontinuità rappresenta l'elemento cruciale per conseguire e mantenere un vantaggio strategico.

Tale assioma, declinato nella società dell'informazione, pone in evidenza il valore "sovrano" della conoscenza anche per quel che attiene alle modalità di accesso, di elaborazione e, soprattutto, di aggiornamento, visto che la rapidità di evoluzione degli scenari si riflette sulla stessa obsolescenza dei saperi.

È messa, pertanto, in risalto la necessità di conseguire la più ampia integrazione fra i diversi produttori e consumatori di informazione, di arricchire capacità e competenze, di costituire reti di condivisione informativa per favorire la crescita del sistema Paese, la sua resilienza e competitività.

Si tratta di una visione rispetto alla quale il nostro Comparto informativo, grazie al lungo e continuo processo di ammodernamento di strutture e metodologie avviato con la riforma del Sistema di informazione per la sicurezza del 2007, continua ad operare per assicurare il più ampio presidio in termini di sicurezza nazionale e di protezione degli interessi supremi del Paese.

Ciò nel quadro di un rapporto di piena inclusione dell'attività di intelligence nelle politiche nazionali che scaturisce dall'allineamento delle pianificazioni operative dei Servizi rispetto alle linee di fabbisogno individuate dal Governo.

Gli indirizzi di Governo e il controllo parlamentare

Centrale, nella prospettiva nazionale della politica di informazione per la sicurezza, è, quindi, il rapporto sintonico tra committenza politica e Agenzie d'intelligence, la cui attività operativa e di analisi, nel 2016, è stata indirizzata verso gli obiettivi indicati dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR) nel contesto di una pianificazione strategica di respiro triennale (2015-2017).

Il sistematico raccordo tra Organismi informativi e Autorità di Governo, rafforzato dalle attività del cd. CISR tecnico, "cinghia di trasmissione" utile ad assicurare anche una stabile concertazione tra le Amministrazioni interessate, si è accompagnato alla consolidata e cooperativa interlocuzione con il Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), testimonianza della convergenza e dell'*idem sentire* tra Esecutivo e Parlamento sui rilevanti temi della sicurezza nazionale. Ne sono emblematico ritorno le 5 audizioni tenute dall'Autorità Delegata, oltre a quelle di Vertici e di alti Dirigenti degli Organismi informativi (5 per il DIS, 7 per l'AISE e 4 per l'AISI).

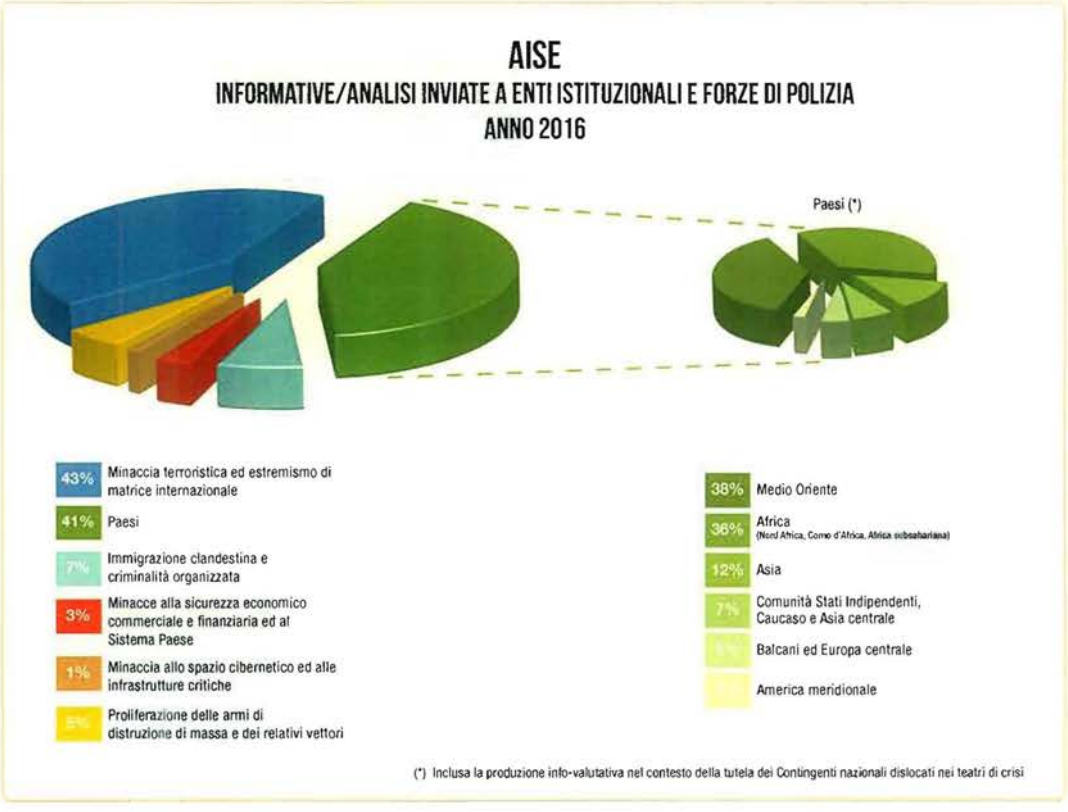
La produzione informativa e d'analisi

Come per la scorsa annualità, anche per il 2016 le priorità di intervento degli Organismi informativi hanno intrecciato, con una angolazione che integra contesto e fattori di rischio, la copertura di teatri di interesse e di minacce sistemiche per la sicurezza del Paese (*vedi grafici sulla produzione informativa di AISE ed AISI*).

Il *network* dei fattori critici e le instabilità territoriali

In coerenza con le indicazioni del Vertice politico, le interrelazioni tra sviluppi d'area e fenomeni di minaccia – che compongono il *network* dei fattori critici e che informano lo sviluppo della presente relazione – hanno costituito un principio cardine dell'attività intelligence, sviluppatasi nel segno del coordinamento, della condivisione e della multidisciplinarietà.

Significativo, in proposito, l'impegno informativo profuso a supporto dell'azione politico-diplomatica dell'Italia in direzione della sponda Sud del Mediterraneo: per la stabilizzazione della Libia e per il contenimento di ingenti flussi migratori illegali, che anche nel 2016 hanno trovato la principale via di transito in quel territorio; per la sicurezza della regione, alveo di una minac-

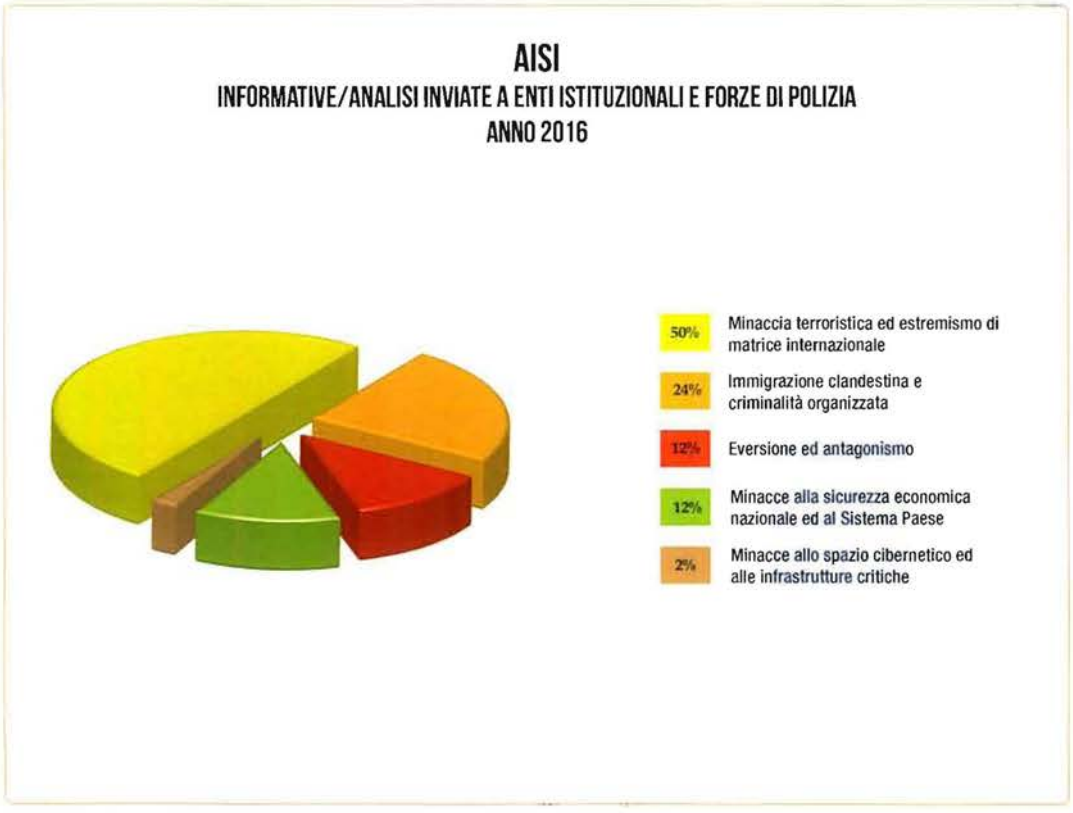


cia terroristica dalle potenziali proiezioni extracontinentali, ma anche area strategica di approvvigionamento energetico; per il sostegno – pure nell'ambito delle politiche UE – ai Governi delle popolose realtà subsahariane.

La medesima logica *multitasking* – corrispondente alle diverse declinazioni della sicurezza nazionale – ha caratterizzato lo sguardo dell'intelligence alle realtà territoriali d'interesse, passate in rassegna, nella presente relazione, secondo la prevalente, ma non esclusiva, linea narrativa del fermento jihadista e della competizione tra DAESH e *al Qaida*: dal Maghreb al Sahel, dall'Africa occidentale a quella orientale, dal teatro siro-iracheno al Sinai e a Gaza, dalla crisi yemenita all'attivismo radicale nel Golfo, dall'*Af-Pak* al Sud-Est asiatico.

Le interazioni come moltiplicatore del rischio

In varia misura, le attività di raccolta informativa, così come quella di analisi rispetto a crisi geopolitiche, dinamiche geostrategiche ed evoluzioni del quadro economico, hanno sistematicamente concorso ad integrare, nella medesima prospettiva intelligence, la valutazione ponderata su minacce



eterogenee e su altri potenziali vettori di pericolo per la sicurezza nazionale.

Non è un caso che i fenomeni più insidiosi, ovvero che hanno rappresentato le sfide più impegnative per gli Organismi informativi siano quelli che hanno evidenziato la più stretta interdipendenza rispetto a sviluppi sul terreno nei teatri di crisi ovvero una connaturata propensione a interagire con minacce di diversa matrice e persino con dinamiche di per sé "neutre" (a partire dall'evoluzione tecnologica).

Ciò vale per il terrorismo internazionale di matrice jihadista, per il fenomeno migratorio che ha continuato ad investire il Mediterraneo con cifre sempre più elevate, anche in termini di perdite di vite umane, per i fattori critici per il nostro sistema economico-finanziario e, soprattutto, per la minaccia cibernetica, a motivo della sua peculiare natura interconnessa.

Il terrorismo jihadista come "guerra nella pace"

L'offensiva del terrorismo jihadista, che aveva subìto un'accelerazione in Francia nel 2015, è proseguita durante tutto il 2016 in Europa, con i cruenti attacchi di Bruxelles, la strage sul lungomare di Nizza, l'assalto alla chiesa di Rouen, l'attentato al mercatino di Natale di Berlino. Un'offensiva con un teatro di proiezione globale – scandita, oltre lo spazio UE, dall'attentato di luglio a Dacca sino all'attacco di fine anno ad Istanbul – che ha tragicamente confermato la tendenza di DAESH ad accentuare la risposta asimmetrica per compensare gli arretramenti territoriali sul campo siro-iracheno.

Il conseguente, grave bilancio di vittime, con il coinvolgimento anche di connazionali, mostra come si sia venuta così determinando quella condizione di minaccia autorevolmente definita come "guerra nella pace".

Su un piano generale, permane, nei centri di elaborazione strategica del *global terrorism*, la capacità di pianificare attentati complessi e ad alto impatto mediatico, oltre che di sfruttare la tecnologia a fini propagandistici e per le comunicazioni tra militanti.

In parallelo a dette operazioni, che presuppongono tempi di gestazione e di preparazione più lunghi (con una maggiore permeabilità all'azione di contrasto), le organizzazioni terroristiche – DAESH, ma anche *al Qaida*, impegnate a contendersi gli spazi d'influenza in quadranti africani e asiatici – hanno concorso ad alimentare ed ispirare azioni di *jihad* individuale riferibili a gruppi ristretti o soggetti isolati disposti ad attivarsi sulla sola base di un indottrinamento, spesso assorbito via *web* o in ambiente carcerario.

Il terrorismo, atomizzato e acefalo, del *lone wolf* che si auto-innesca è più sottile e subdolo, ma non meno grave del terrorismo organizzato e "militarizzato". Se, infatti, esso non appare in grado di portare una minaccia di natura esistenziale per uno Stato o una collettività, può certamente alterare in modo anche sensibile molti aspetti della vita quotidiana della popolazione, con danni di enorme portata specie se correlati al limitato impiego di mezzi e risorse.

Ancor più grave è il fatto che la minaccia jihadista sia in grado di maturare all'interno delle società occidentali, attraverso i cd. *estremisti homegrown* (immigrati di seconda o terza generazione, nonché convertiti, nati, cresciuti o radicalizzati in suolo occidentale), pienamente integrati nel Paese di residenza e con elevata capacità di mimetizzazione, anche perché l'adesione al messaggio estremista avviene in esito a processi di radicalizzazione sempre più rapidi e silenti.

La pervasività del terrorismo jihadista, in ragione anche della sua connotazione multiforme (transnazionale ed endogeno, tecnologico, strutturato ma anche fluido e dematerializzato) ha chiamato in causa le vulnerabilità di sicurezza dentro e fuori l'Europa, sollecitando forme sempre più evolute di cooperazione internazionale e, soprattutto, l'affinamento dei moduli di scambio informativo a livello continentale. Va detto, al riguardo, che la nostra Comunità intelligence svolge in ambito di cooperazione internazionale (sul piano sia bilaterale sia multilaterale) un ruolo di impulso a favore della massima condivisione informativa, potendo anche vantare, in ambito nazionale, un modello virtuoso di cooperazione sul versante del controterrorismo (*vds. box n. 1*).

box 1

IL MODELLO ITALIANO DI RISPOSTA

È opinione condivisa che l'esperienza di controterrorismo maturata negli anni di piombo e la perdurante lotta ad una criminalità organizzata tra le più efferate e aggressive al mondo abbiano reso le nostre Istituzioni tra le più preparate, a livello internazionale, nel confronto con minacce ibride o asimmetriche, anche sotto il profilo del contrasto ai correlati flussi finanziari.

Se da un lato sono proprio il *background* e la professionalità a dare la consapevolezza delle difficoltà di prevenire sempre e in ogni caso atti ostili, anche clamorosi, dall'altro può annoverarsi tra i successi "intangibili" del dispositivo nazionale l'avvenuto, pacifico svolgimento di eventi di vasta portata internazionale e valenza simbolica.

Sul piano metodologico, possono annoverarsi tra le *best practices* della strategia nazionale di controterrorismo:

- i rodati meccanismi di interscambio che assicurano, nel pieno spirito del dettato normativo (a partire dalla legge 124/2007 che ha riformato il settore intelligence), un effettivo, costante raccordo informativo tra AISE ed AISI, con il coordinamento del DIS;

- la proficua interazione tra intelligence e Forze di polizia, inclusa l'Amministrazione penitenziaria, specie nell'ambito del Comitato Analisi Strategica Antiterrorismo - CASA, operante presso il Ministero dell'Interno. In quella sede congiunta: sono oggetto di sistematica valutazione le segnalazioni di minaccia, anche provenienti dalla collaborazione internazionale d'intelligence; viene aggiornata la "lista consolidata" dei *foreign fighters* all'attenzione; sono condivisi, tra l'altro, i provvedimenti di espulsione a carico di soggetti ritenuti pericolosi per la sicurezza. Il CASA è un punto di forza del modello italiano, un modello ultradecennale che il nostro Paese sta cercando tenacemente di promuovere in ambito europeo, nell'assunto che solo un maturo rapporto tra intelligence e Forze di polizia può tradurre la cooperazione internazionale in efficaci strumenti di prevenzione;
- le sinergie interistituzionali che hanno portato, tra l'altro, all'approvazione, nel 2015, di due importanti provvedimenti legislativi:
  - il decreto-legge 18 febbraio 2015 n. 7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43, che nel 2016 ha conosciuto una proroga della possibilità, sempre transitoria, che operatori dell'intelligence svolgano colloqui in carcere con detenuti di interesse per finalità informative;
  - il decreto-legge 30 ottobre 2015, n. 174, convertito con modificazioni dalla legge 11 dicembre 2015, n. 198, che all'art.7-bis, consente all'AISE, in situazioni di crisi all'estero che coinvolgano la sicurezza nazionale o la protezione di nostri concittadini, di avvalersi delle Forze speciali della Difesa e dei relativi assetti.

Le criticità del fenomeno migratorio

Le migrazioni di massa su scala mondiale tendono a configurarsi sempre meno come emergenze cicliche e sempre più come un fenomeno di lungo termine e portata storica, in quanto effetto di un concorso di fattori strutturali e congiunturali: gli squilibri reddituali (e di opportunità) tra diverse regioni del mondo, i grandi cambiamenti climatici (*vds. box n. 2*), le guerre e le carestie, la cronica instabilità politica di molte aree, l'aumento esponenziale della popolazione in numerosi Stati le cui economie non sono in grado di assorbire la nuova forza lavoro.

Nella prospettiva intelligence e con riguardo all'incessante ondata migratoria che ha visto lo sbarco in Italia di oltre 180 mila tra migranti economici e profughi (vedendo con ciò superata la cifra record del 2014, di poco superiore alle 170 mila unità), la connotazione "fisiologica" del fenomeno cede il passo ad una "patologia sistemica" che rimanda ad una serie di fattori altrettanto eterogenei: l'attivo coinvolgimento di *network* criminali transnazionali; le pericolose contiguità tra circuiti criminali e terroristici attivi nei Paesi di origine, transito e, in qualche caso, destinazione dei migranti, le interazioni con altri settori illeciti, quali il falso documentale e il riciclaggio; l'impatto sul territorio nazionale a partire dalla congestione delle strutture di accoglienza.

box 2

I CAMBIAMENTI CLIMATICI

Al di là della sua influenza quale fattore di spinta delle migrazioni, il cambiamento climatico globale rappresenta un pericolo per la pace e per il benessere economico e sociale del pianeta, giacché inocula germi di instabilità politica ed economico-finanziaria a livello internazionale, aumentando il rischio di conflitti (intra e internazionali) e di fallimento degli Stati. A conferma della crescente percezione delle implicazioni concrete del fenomeno si rammenta la stipula nel 2015, dopo lunghissime e sofferte trattative, dell'accordo di Parigi, formalmente ratificato dalla UE nel 2016, che definisce un piano d'azione universale volto a ridurre il riscaldamento globale "ben al di sotto dei 2°C".

Per la sua collocazione geografica nel Mediterraneo, l'Italia è chiamata a svolgere un ruolo centrale nella gestione condivisa delle politiche migratorie internazionali, contemperando le esigenze umanitarie con quelle di legalità e sicurezza, e promuovendo in ambito europeo la concreta attuazione del principio di solidarietà.

In un'ottica di supporto alle nostre Autorità di Governo e in un contesto di stretto raccordo interistituzionale, la coordinata azione dell'intelligence, primariamente focalizzata, come detto, sulla realtà libica, si è dispiegata su più fronti, riguardando, tra l'altro, gli sviluppi di situazione nei quadranti ove più potente è la spinta centrifuga, le dinamiche operative e relazionali dei sodalizi criminali implicati nel traffico, gli itinerari e le opzioni di instradamento dei flussi, le aree di connivenza specie negli snodi africani e del subcontinente indiano, i terminali logistici attestati in territorio nazionale.

Il quadro economico e i nuovi attori

Quanto alla terza sfida sul nostro assetto di sicurezza, va rilevato che il sistema economico italiano sta uscendo da un periodo di crisi che non ne ha sostanzialmente alterato le caratteristiche fondamentali, i punti di forza e quelli di debolezza. Il Paese conserva una vivace vocazione manifatturiera, elevati *standard* tecnologici e capacità di innovazione, accentuata internazionalizzazione e propensione *all'export*, e – accanto a grandi gruppi strutturati e competitivi a livello internazionale – una dinamica e vasta rete di piccole e medie imprese. Esso continua a dipendere in larga misura dall'estero per le materie prime e il settore energetico. Trattandosi quindi di economia matura, il sistema italiano basa in modo crescente la sua competitività su innovazione e ricerca tecnologica, che sono, pertanto, *asset* vitali da tutelare.

Da protagonista di un sistema globalizzato, il nostro Paese deve tenere il passo con un panorama economico e finanziario internazionale in tumultuosa evoluzione e di crescente concorrenza, che presenta straordinarie opportunità ma anche inedite sfide e minacce sistemiche. Un contesto, oggi più che mai, strettamente interconnesso con le grandi dinamiche geopolitiche e

securitarie, anche in virtù dell'effetto moltiplicatore determinato dalla tecnologia, dall'immediata circolazione dell'informazione e dalle simultanee reazioni dei mercati su scala mondiale.

In questo scenario globale si sono, inoltre, ulteriormente rafforzati nuovi attori – con sistemi di potere transnazionali e detentori di inusuali concentrazioni di ricchezza – che seguono logiche autonome ed obiettivi non necessariamente orientati alla tutela dell'interesse pubblico, del territorio e della collettività. Ciò è tanto più rilevante nel caso di gruppi la cui capitalizzazione supera di gran lunga l'entità di prodotti interni di taluni Stati.

In un *trend* riscontrabile anche in altri Paesi occidentali, si avvertono, pure sul versante della protezione degli interessi economici, rinnovate istanze per un rilancio del ruolo degli Stati a sostegno e presidio della propria comunità produttiva, con adeguati supporti nazionali di informazione e tutela. Esse originano da una acuita percezione della necessità di un rafforzato sistema di garanzie per la stabilità e la salvaguardia del tenore di vita dei cittadini, rispetto a pratiche commerciali e finanziarie pregiudizievoli; in sostanza si va affermando un'accresciuta consapevolezza della interdipendenza tra prosperità economica e sicurezza.

L'Italia a fronte di vecchie e nuove minacce sistemiche

L'Italia presenta un quadro di vulnerabilità specifiche discendenti dalla strutturazione del relativo tessuto economico, su cui si innestano fattori di rischio tipici che involgono la generalità delle democrazie con sistemi produttivi sviluppati.

Un primo tratto di fragilità sistemica va ravvisato, a motivo della estrema dipendenza dall'estero nella bilancia energetica, dagli effetti traslativi del rischio geopolitico sulla continuità di approvvigionamento e dalle implicazioni di costo delle importazioni in dipendenza delle fluttuazioni di mercato, ricorrenti per la comparsa di nuovi fornitori globali e per i riflessi sull'andamento dei corsi generati dalle scelte, anche di natura diplomatica, dei cartelli produttivi. In questo senso, la connotazione di cerniera della nostra Penisola, se, da un lato, accresce la superficie di esposizione alle discontinuità delle forniture, dall'altro potrebbe ottimizzare il nostro ruolo di piattaforma per gli instradamenti energetici in direzione della piazza continentale europea

Un ulteriore aspetto di criticità discende dalla ricordata conformazione puntiforme della realtà produttiva italiana, per buona parte espressa dalla piccola e media impresa detentrice di una qualificata conoscenza tecnologica ed industriale – sovente scoperta rispetto ai tentativi di indebita sottrazione cibernetica – ma insufficientemente aggregata per costituire massa critica nella serrata dinamica competitiva su scala globale.

La congiunturale fase di contrazione creditizia ha accentuato, poi, questo complesso di criticità ponendo le imprese nazionali dinanzi ad un'accresciuta sovraesposizione rispetto a manovre acquisitive estere dettate, più che da strategie di investimento,

da finalità di depotenziamento competitivo, come pure agli inserimenti tossici di matrice criminale volti a condizionare la fisiologica concorrenza in ragione di prevalenti interessi al reinvestimento di capitali di provenienza illecita. Particolarmente sensibili in questa finestra temporale, per il ruolo connettivo di sostegno della crescita economica, la integrità e la solidità del sistema bancario, bersaglio, in qualche caso, di operazioni acquisitive da parte di campioni stranieri in grado di drenare all'estero quote significative del nostro risparmio.

Il contributo dell'intelligence alla tutela del Sistema Paese

In uno scenario come quello descritto, di accresciuta complessità del commercio e della finanza internazionali, è aumentata di pari passo la necessità per le Istituzioni di un qualificato supporto informativo e di analisi.

Anche nel 2016 la pianificazione operativa delle Agenzie ha previsto l'azione di tutela del Sistema Paese e della sua internazionalizzazione rispetto alle minacce verso i settori strategici, incluso quello energetico, l'integrità del sistema bancario e finanziario, il *know-how* tecnologico e il *made in Italy*, nonché ha riguardato le dinamiche delle economie illegali, i flussi illeciti di capitali, le contiguità tra circuiti criminali e terroristici, la corruzione.

Tale azione si è espletata secondo un approccio intersettoriale e di stretta sinergia con gli altri attori istituzionali, nonché improntato a sempre maggiore attenzione verso il mondo imprenditoriale e produttivo. In particolare, le dinamiche di competizione per la catena globale del valore e di riaffermazione nell'*Industria 4.0* hanno determinato la necessità di un accresciuto dialogo tra gli Organismi informativi e gli operatori economici, anche al fine di elevarne il livello di consapevolezza, propiziarne più utili collaborazioni ed accrescerne la capacità di autotutela e prevenzione.

Ciò è valso in modo particolare per quanti sono chiamati ad assicurare la continuità delle infrastrutture critiche come reti di comunicazione, di distribuzione dell'energia e di trasporto, o banche dati anche finanziarie, che innervano la struttura economica del Paese. Nella logica di salvaguardia della stabilità del sistema si è inscritto anche il supporto necessario a fornire un più generale quadro informativo, utile all'esercizio dei poteri preordinati al mantenimento del controllo di *asset* strategici nazionali.

La dimensione *cyber* come fattore trasversale di potenziamento e di despazializzazione della minaccia

L'evolversi esponenziale delle potenzialità offerte dallo sviluppo tecnologico è stato soprattutto enfatizzato in relazione ai suoi aspetti positivi per il miglioramento della qualità di vita, come catalizzatore del benessere, dei commerci e della diffusione della conoscenza. Tuttavia, negli ultimi anni è andata parallelamente rafforzandosi la consapevolezza che anche le nuove tecnologie possono costituire – se utilizzate con finalità malevoli o ostili – uno strumento passibile di deter-

minare nuove ed inedite minacce, anche di estrema gravità, come la paralisi di settori vitali per le moderne società. Di qui, la crescente centralità della sicurezza dell'ambiente cibernetico cui è dedicato, in ossequio alla normativa vigente, un documento *ad hoc* – in appendice alla Relazione – che raccorda alle iniziative di manutenzione dell'architettura nazionale una rappresentazione analitica sulle tendenze evolutive della minaccia.

Mentre lo scenario globale resta tuttora – in una componente ormai esiziale come quella cibernetica – carente di uno strutturato quadro regolatorio, il dominio digitale si va confermando come potentissimo volano che rende più incisivi, perniciosi ed immediati fattori di rischio tradizionali ed inediti.

In un'arena attraversata da contese di matrice militare, politica, informativa, industriale e finanziaria si registrano:

- modalità nuove di attacco, come l'esfiltrazione o l'alterazione in tempi brevissimi di informazioni (anche di masse enormi delle stesse) o la distruzione e il danneggiamento di sistemi informatizzati e di dati in essi custoditi;
- un sempre più ampio novero dei possibili attori ostili, anche per la generale disponibilità ed economicità di complessi strumenti informatici. Oltre agli Stati – che vanno costantemente potenziando e accrescendo le proprie dotazioni e capacità in materia – figura una varietà di *players*: criminalità organizzata (*cybercrime*), organizzazioni terroristiche (*cyberterrorism*), gruppi privati specializzati in attività di spionaggio, sottrazione di *know-how* o di blocco di sistemi di *governance*, nonché piccole pattuglie o singoli individui con fini truffaldini, ideologici o mossi da fanatismi di vario tipo. Essi possono peraltro spesso disporre di mezzi che a volte superano per efficienza e modernità quelli degli stessi Governi o dei grandi gruppi industriali (tenuti spesso a complesse procedure amministrative per il rinnovo delle attrezzature);
- un altrettanto esteso *range* dei potenziali obiettivi: Governi, organi istituzionali, enti finanziari, imprese, infrastrutture strategiche e funzionali all'erogazione di servizi alla società civile, fino a singoli cittadini.

La variabile cibernetica come strumento di offesa sta giocando un ruolo determinante nell'evoluzione e nell'attualizzazione del cd. *conflitto ibrido*. I *target* aggrediti (in particolare gli Stati) devono in molti casi reagire con processi decisionali e procedure codificati, mentre molti attori ostili possono operare con azioni informali, discontinue, apparentemente occasionali, ma sovente inserite in vere e proprie campagne di guerra asimmetrica, persistente e coordinata, con attacchi seriali e tattiche operative che rendono difficile risalire agli aggressori. Questi ultimi possono avvalersi, altresì, di straordinari "palcoscenici mediatici", grazie anche ai *social media* e alla moltitudine di nuovi *devices* connessi alla Rete.

La risposta dell'intelligence alla *cyberthreat*

La "miniaturizzazione" e la pervasività della minaccia accrescono la necessità di un'azione più capillare ed evoluta da parte dell'intelligence, chiamata ad agire con modalità e strumenti in continua evoluzione, nel rigoroso bilanciamento fra la preservazione degli spazi di libertà e di *privacy* e le più generali esigenze di sicurezza, e, comunque, nel puntuale rispetto delle previsioni legali e nella doverosa soggezione al controllo politico-parlamentare.

Il Comparto informativo nazionale assolve in questo settore ad una missione articolata su più livelli di intervento, che accompagna l'esercizio delle prerogative sui versanti della raccolta ed analisi informative sulla minaccia e della promozione e diffusione della cultura della sicurezza alla attività di supporto manutentivo della architettura nazionale di protezione cibernetica delle reti e dei sistemi pubblici e privati, che si è tradotta, quale momento di indirizzo più qualificante, nella compilazione del Quadro Strategico Nazionale e nell'aggiornamento del relativo piano di attuazione.

Il coinvolgimento dell'intelligence sul lato "emerso" – in una logica complementare alla missione "*core*" – rimane attuale nella prospettiva, indotta anche dal recepimento della più recente produzione normativa europea, di conseguire più ottimali margini di preparazione e reattività del nostro Sistema rispetto ad eventi cibernetici condotti con finalità aggressive.

In tale campo, infatti, nessun attore statuale può agire in solitudine vista la indefettibilità del partenariato pubblico-privato e delle conseguenti sinergie con il mondo della accademia, della ricerca applicata e dell'industria di settore (*vds. box n. 3*).

box 3

PRINCIPALI INIZIATIVE DEL COMPARTO INTELLIGENCE IN MATERIA DI *CYBERSECURITY*

Tra principali iniziative intraprese nel 2016 in tema di *cybersecurity*, si ricordano:

- la revisione del Quadro Strategico Nazionale e del connesso Piano Nazionale, al fine di allineare ulteriormente il nostro sistema di sicurezza cyber agli standard internazionali;
- il consolidamento del partenariato pubblico-privato quale segmento di una più ampia direttrice d'intervento che – come si dirà più avanti – punta alla sempre maggiore interazione tra intelligence e imprese strategiche in un'ottica di tutela del Sistema Paese;
- l'organizzazione della 17^ edizione del "NATO *Cyber Defence Workshop*" tenutosi presso la Scuola di formazione del Comparto;
- la terza edizione dell'evento ICT4INTEL 2020, occasione in cui insieme alle Università e alle aziende coinvolte si è operata una riflessione congiunta sulle iniziative da mettere in atto per affinare le capacità nazionali sul versante della sfida tecnologica.

Evoluzione del ruolo degli Organismi di intelligence

La sicurezza, lungi dall'essere un valore alternativo o inconciliabile con la libertà, ne costituisce uno dei presupposti. La libertà si nutre infatti di sicurezza, giacché per potersi dispiegare deve anzitutto affrancarsi dalla violenza, dall'asservimento, dalla paura (come recita il Preambolo della Dichiarazione universale dei diritti dell'uomo del 1948) e dal bisogno economico. Il diritto alla libertà, su cui si fondano le moderne democrazie, è perciò inseparabile dal diritto alla sicurezza. E la sicurezza si nutre a sua volta di libertà.

Donne e uomini dell'intelligence agiscono a tutela della sicurezza nazionale, nell'accezione più estesa e comprensiva che questo termine può assumere – che non coincide certo con la mera "assenza di minacce e pericoli" – fronteggiando e prevenendo i possibili attacchi: alle istituzioni, ai cittadini, alle imprese. Essi assolvono a una funzione di invisibile, silenziosa difesa delle libertà che danno corpo al nostro stile di vita, di cui sono necessario presupposto.

Nel tempo, senza discostarsi dalla funzione tradizionale e primaria di offrire il supporto della "conoscenza del mondo" all'Autorità di governo, con modalità specifiche di condotta e di osservanza dei criteri di tutela informativa anche nella reciprocità della collaborazione internazionale, il Comparto è andato sempre più avvicinandosi e aprendosi alla società civile, agli operatori economici, al mondo accademico, ai centri di ricerca più avanzati, anche per potenziare gli strumenti e le conoscenze necessarie per fronteggiare, come detto, minacce sempre più complesse e tecnologiche.

L'intelligence da "apparato" a "comunità"

In questa visione, la pubblica percezione della gestione della sicurezza va evolvendosi da una visione che la vede come prerogativa esclusiva dello "Stato-apparato" a una visione di sicurezza come bene collettivo cui tutti sono interessati a concorrere e, quindi, in un'ottica di "sicurezza partecipata", che coinvolge lo "Stato-comunità". Tale processo è alla base del progressivo coinvolgimento di diversi attori pubblici e privati che, raccordati in un sistema integrato per la sicurezza del Paese, svolgono con sempre maggiore cognizione e responsabilità un ruolo attivo nella strategia comune di difesa delle istituzioni democratiche, di tutela dei diritti, di sostegno dei fattori di crescita e competitività, perseguendo i primari interessi del Paese, nel solco delle direttrici individuate dalle Autorità di Governo e sotto il controllo del Parlamento.

L'architettura dell'attuale rete securitaria si fonda, in effetti, in modo crescente sul consolidamento di moduli di *partnership* pubblico-privato, sulla diffusione di una cultura d'intelligence più consapevole non solo dei rischi ma anche delle opportunità offerte dalla competizione e dalla globalizzazione, nonché su un'attenta e avanzata cooperazione internazionale. Le attività svolte tradizionalmente dai Servizi sono, pertanto, sempre più proficuamente integrate da nuove competenze e professionalità (vds. *box n. 4*).

box 4

LA POLITICA DI RECLUTAMENTO

È, questa, la cornice nella quale si colloca la *policy* in materia di personale fatta propria dal Comparto intelligence, con investimenti crescenti sul capitale umano. Una *policy* che è necessario corollario del fatto che la Legge n. 124/2007, di riforma del Sistema di Informazione per la Sicurezza della Repubblica, ha sensibilmente ampliato gli ambiti di intervento dei Servizi informativi, ora non più circoscritti alla difesa della sicurezza, integrità e indipendenza delle istituzioni democratiche da minacce provenienti dall'interno o dall'esterno, ma ampliati anche alla tutela degli interessi strategici nazionali in campo politico, militare, economico, scientifico e industriale, nonché - in conformità con quanto previsto dalla Legge n. 133/2012 - alla protezione cibernetica e sicurezza informatica nazionale.

L'attività di reclutamento si è avvalsa sempre più di rinnovate formule di carattere selettivo, nonché della facoltà di ricorrere anche a bacini diversi da quelli tradizionali (Forze Armate, Forze di polizia, altre Amministrazioni dello Stato), e cioè Università, enti di ricerca, imprese e settore privato e altre istituzioni di interesse.

La ricerca di risorse d'eccellenza per far fronte alle sfide emergenti è proseguita, in parallelo, attraverso il sito istituzionale.

È stato così possibile individuare e assumere nuove giovani professionalità in possesso di specifiche conoscenze e competenze, specie nei campi tecnologico-informatico, linguistico, geopolitico ed economico-finanziario.

L'alleanza strategica con l'Università

In questa prospettiva, il rapporto intelligence-Università assume il valore di un'alleanza strategica per la sicurezza nazionale, in quanto stretta, con reciproco vantaggio, sull'incrocio delle rispettive conoscenze ed *expertise*.

Da un lato, l'intelligence – strumento non convenzionale, che opera sulla linea più avanzata per la difesa delle Istituzioni democratiche – attraverso la relazione con l'Accademia si pone in condizione di offrire ai decisori pubblici e agli operatori privati un prodotto informativo arricchito dal patrimonio di conoscenze elaborate in sede scientifico-accademica; dall'altro, l'Università trova nel Sistema per la sicurezza della Repubblica – a tutto vantaggio dell'interesse nazionale – un importante terminale della propria attività di ricerca, concorrendo nell'interpretazione di dinamiche sociali, culturali e politiche in continua evoluzione, e nel predisporre modelli e strategie efficaci ai fini della protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia.

L'alleanza intelligence-università è particolarmente feconda in tema di sicurezza cibernetica. Tra le numerose iniziative in corso, riveste rilievo la collaborazione strutturata con il Consorzio Interuniversitario Nazionale per l'Informatica (CINI) – cui partecipano centinaia di accademici e ricercatori appartenenti a decine di Università Italiane – che ha dato vita al Laboratorio Nazionale in tema di *cybersecurity* finalizzato allo sviluppo di progetti di ricerca e capace di erogare formazione di livello avanzato nel settore di riferimento.

Cultura della sicurezza e formazione

La *partnership* tra il Comparto e il mondo accademico ha trovato nel 2016 ulteriore suggello nella firma dei Protocolli d'intesa:

- con il Ministero dell'Istruzione, dell'Università e della Ricerca per la diffusione della cultura della sicurezza nazionale. L'intesa punta ad instaurare un rapporto di collaborazione per iniziative riguardanti attività di ricerca scientifica, didattica e di formazione, in particolare promuovendo un piano nazionale di educazione alla sicurezza rivolto agli studenti delle Scuole primarie e secondarie;
- con la Conferenza dei Rettori delle Università Italiane (CRUI). L'accordo, tra gli altri punti, prevede nel campo della sicurezza nazionale: l'individuazione di priorità e progetti; lo sviluppo di interventi congiunti di informazione, formazione professionale e alta formazione; la ricognizione dei corsi già esistenti e l'individuazione di quelli che sarebbe utile attivare; la previsione di una serie di iniziative concernenti il riconoscimento e la qualificazione degli insegnamenti.

Attraverso la sua *Scuola di formazione* – un vero e proprio *Campus* dell'intelligence – il Comparto sta consolidando i rapporti, oltre che con le università, anche con i settori di eccellenza della Pubblica Amministrazione e del mondo delle imprese.

La Scuola si candida dunque a porsi come la "Porta di accesso al mondo dell'intelligence": un centro di ricerca, un incubatore cognitivo e un ponte con il mondo esterno, ma anche uno strumento per dare profondità strategica ad un percorso che dalla conoscenza si concretizza nell'azione. Percorso che si avvale tra l'altro del sito *www.sicurezzanazionale.gov.it* quale luogo elettivo per la comunicazione con il pubblico come dimostra, a riprova dell'interesse per il Comparto, il numero di visualizzazioni (oltre 1 milione e 500mila) e di *email* pervenute (circa 7mila). L'impegno è quello di rendere possibile una contaminazione feconda, per un patrimonio comune di saperi e metodologie.

Particolare significato, nel contesto della promozione e diffusione della cultura della sicurezza, hanno assunto le 27 tappe (6 nel 2016) del *roadshow "Intelligence live"* nelle Università e nei centri di eccellenza, da Nord a Sud del Paese. Complessivamente, sono stati più di 5.000 i giovani studenti incontrati negli eventi organizzati presso

gli Atenei e con i quali l'intelligence si è confrontata sui temi della sicurezza e della difesa della democrazia. Un cammino tra le Università nazionali per far conoscere il lavoro degli Organismi informativi, sfatando miti, stereotipi e luoghi comuni ed accrescendo negli studenti la consapevolezza che essi per primi sono gli azionisti del "bene sicurezza", che è una conquista che non va mai data per scontata.

LA DERIVA JIHADISTA

PAGINA BIANCA

LEGENDA DEGLI ACRONIMI

AaIB	*Ansar al Islam Bangladesh*
ABM-WS	*Ansar Bayt al Maqdis/Wilayat Sinai*
AMISOM	*African Union Mission in Somalia*
AS	*al Shabaab*
AQ	*al Qaida*
AQ-C	*al Qaida Core*
AQIS	*al Qaida in the Indian Subcontinent*
AQMI	*al Qaida nel Maghreb Islamico*
AQPA	*al Qaida nella Penisola Arabica*
AM	*al Murabitun*
BH	*Boko Haram*
DAESH	*al Dawla al Islamiyya fi'l Iraq wa'l Sham (Stato Islamico dell'Iraq e del Levante)*[1]
ISGS	*Islamic State in Greater Sahara*
ISKP	*Islamic State in the Khorasan Province*
JCPoA	*Joint Comprehensive Plan of Action*
JMB	*Jamaat-ul-Mujahedeen Bangladesh (Gruppo Mujahidin del Bangladesh)*
LET	*Lashkar-e Toyba (Esercito del Bene)*
MINUSMA	*Multidimensional Integrated Stabilization Mission in Mali*
OPAC	*Organizzazione per la Proibizione delle Armi Chimiche*
UNIFIL	*United Nation Interim Force in Lebanon*

[1] Sulla scelta della denominazione, vds. Relazione annuale al Parlamento 2015, pag. 8, box n.1.

LA DERIVA JIHADISTA

Trend del fenomeno

In un panorama di *jihad* globale polarizzato dai *brand* di DAESH e di *al Qaida* (AQ), la scena terroristica è stata dominata, nel 2016, dalla cruenta campagna di attentati firmata dall'organizzazione di al Baghdadi anche in dichiarata risposta alla controffensiva militare della Coalizione internazionale in direzione del cd. *Califfato*.

Nel corso dell'anno si è registrato per la prima volta un significativo ridimensionamento territoriale di DAESH che, colpito nel suo tratto distintivo (il motto dell'organizzazione è "stabilirsi ed estendersi"), nel prestigio e nelle fonti di reddito, ha gradualmente rimodulato tattiche offensive e contenuti propagandistici, accentuando la risposta asimmetrica anche all'interno dei territori contesi, minimizzando, a livello mediatico, le sconfitte militari e intensificando l'attività di coordinamento di *network* per la realizzazione di attacchi al di fuori della propria area di elezione, in Occidente e non solo.

La serie ininterrotta di azioni – dal duplice attentato di Bruxelles del 22 marzo sino a quello di Istanbul del 31 dicembre – è valsa a ribadire il multiforme registro operativo di DAESH, cui hanno fatto riferimento sia cellule strutturate, formate anche da *foreign fighters* di rientro dal campo siro-iracheno, in grado di realizzare attacchi coordinati e complessi, sia lupi solitari o microgruppi auto-organizzati, ispirati o cooptati sul *web*.

Questi differenti profili di attori hanno rappresentato strumenti complementari di una strategia tesa a intimidire il *nemico*, mostrando la capacità di colpirlo dall'interno, fornendo nel contempo un'ulteriore prova di forza ai propri sostenitori, riaffermando, anche rispetto alla concorrente *al Qaida*, il ruolo guida nella battaglia globale diretta al trionfo della *vera fede* contro la miscredenza.

In quest'ottica di capitalizzazione propagandistica va letta la sistematica rivendicazione degli attentati – non solo proiezioni offensive predeterminate o eterodirette, ma anche iniziative autonome – attraverso comunicati "fotocopia" sul portale *Amaq*, riferibile a DAESH, con i quali gli autori delle azioni sono celebrati come *soldati* che hanno agito *"in risposta agli appelli lanciati per colpire i cittadini dei Paesi che fanno parte della Coalizione che combatte lo Stato Islamico"*.

Tra i *trend* del 2016 figura il sensibile decremento nel flusso di estremisti verso il teatro siro-iracheno, da ricondursi peraltro a diversi fattori, quali: una più incisiva azione di contrasto, anche con il varo di interventi normativi *ad hoc*; la diminuita attrattiva esercitata dal progetto di *Califfato* in corrispondenza con le pesanti sconfitte subìte sul piano militare; un cambiamento nelle direttive strategiche della *leadership* dell'organizzazione, verosimilmente propensa ad impiegare gli aspiranti combattenti per attivazioni terroristiche nei contesti di residenza.

La campagna terroristica in Europa

Con riguardo agli attacchi compiuti in area UE (*vds. box n. 5*), il 2016 ci consegna il preoccupante dato dell'ampliamento della casistica con riferimento non solo ai responsabili delle operazioni terroristiche, ma anche al *modus operandi* che ha ricompreso, tra l'altro, l'utilizzo di camion lanciati sulla folla – come accaduto a Nizza il 14 luglio e a Berlino il 19 dicembre – espressamente richiamato dalla pubblicistica jihadista riferibile tanto ad *al Qaida* quanto a DAESH.

box 5

PRINCIPALI ATTENTATI IN EUROPA DEL 2016

Il **22 marzo**, a Bruxelles (Belgio), tre cittadini belgi-marocchini hanno condotto un primo attacco all'aeroporto di Zaventem, mentre un altro belga-marocchino ha realizzato un secondo attentato a bordo di un vagone della metropolitana, all'altezza della fermata di Maalbeek. Entrambe le azioni sono state rivendicate da DAESH e hanno causato, complessivamente, 32 vittime, tra cui una nostra connazionale. Il **13 giugno**, a Magnanville (Francia), il cittadino franco-marocchino Laroussi Abdallah ha accoltellato a morte una coppia di poliziotti all'interno della loro abitazione prima di venire ucciso dalle Forze dell'ordine. Il soggetto aveva postato *on-line* un video nel quale giurava fedeltà a DAESH. Il **14 luglio**, a Nizza (Francia), Mohamed Lahouaiej Bouhlel, alla guida di

un camion frigorifero, si è lanciato sulla folla durante le celebrazioni della festa nazionale francese, provocando la morte di 84 persone, tra cui sei italiani, ed il ferimento di oltre 100. Bouhlel è stato ucciso nel corso dell'intervento della Polizia. Il **18 luglio**, a Würzburg (Germania), il profugo pakistano Riaz Khan Ahmadzai ha ferito a colpi di ascia i passeggeri di un treno regionale prima di essere ucciso dalla Polizia. Il **25 luglio**, ad Ansbach (Germania), il cittadino siriano Mohammad Daleel è deceduto nell'esplosione di un ordigno artigianale nascosto nel suo zaino, provocando il ferimento di molte persone. Lo stesso era in contatto con elementi di DAESH in Siria. Il **26 luglio**, a Saint-Etienne-du Rouvray vicino Rouen (Francia), all'interno di una chiesa Adel Kermiche e Abdel Malik Petitjean, cittadini francesi, hanno preso in ostaggio 5 persone, uccidendo il parroco e provocando il ferimento di alcuni presenti. I due avevano postato un video nel quale giuravano fedeltà a DAESH. Il **6 agosto,** a Charleroi (Belgio), il cittadino algerino Khaled Babouri ha aggredito due poliziotte con un machete prima di essere ucciso dalle Forze dell'ordine. Il **31 agosto**, a Copenhagen (Danimarca), Mesa Hodzic, danese di origine bosniaca, ha attaccato con un'arma da fuoco una pattuglia della Polizia nel quartiere di Christiania, ferendo due agenti ed un passante prima di essere a sua volta ferito a morte. L'aggressore aveva espresso sui *social network* la sua vicinanza ideologica a DAESH, che ha poi rivendicato l'attacco. Il **19 dicembre**, a Berlino (Germania), il tunisino Anis Amri, alla guida di un autoarticolato, ha travolto volontariamente la folla presente in un'area pedonale nella quale era allestito un mercatino di Natale provocando 12 vittime, tra cui una connazionale, e una cinquantina di feriti. Al termine dell'azione, Anis Amri è riuscito a fuggire e nella notte del 23 dicembre è deceduto a Sesto S. Giovanni (Milano) in un conflitto a fuoco con agenti della Polizia di Stato, uno dei quali è rimasto ferito.

Per quel che attiene all'ampio novero degli obiettivi colpiti (tanto bersagli istituzionali, principalmente Forze dell'ordine, quanto *soft target*, inclusi luoghi di raduno di massa), è emerso come dato inedito e di più alta preoccupazione il primo assalto in Occidente all'interno di una chiesa cattolica, compiuto il 26 luglio in Francia, a Rouen, e seguito, il 31 luglio, dalla pubblicazione del numero 15 di *Dabiq*, rivista di DAESH, dall'emblematico titolo *Break the cross* (*Distruggi la croce*).

Ricorrenze e novità nella narrazione islamico-radicale

In continuità con il *trend* rilevato nella Relazione del 2015, la propaganda e la comunicazione, combinati con lo strumento tecnologico, hanno costituito un pilastro per la strategia delle formazioni jihadiste. La diffusione del messaggio radicale, promossa sia verticalmente, attraverso le case mediatiche di riferimento delle *leadership*, sia orizzontalmente, mediante l'assiduo *networking* tra *mujahidin* anche occidentali, ha giocato un ruolo su più piani, quali il reclutamento e l'istigazione di nuovi adepti, l'intimidazione dei *nemici*, la condivisione di istruzioni tecniche e di consigli pratici per la realizzazione e la massimizzazione di atti di *jihad* individuale.

La propaganda "verticale"...

Tra gli aspetti emergenti della pubblicistica jihadista si è evidenziata una certa evoluzione nelle strategie

mediatiche di DAESH, in stretta connessione con le vicende belliche nei territori del *Califfato*.

La fase espansiva dell'organizzazione di al Baghdadi si era accompagnata alla moltiplicazione e alla diversificazione di canali, prodotti e strumenti mediatici, anche con il decentramento verso strutture locali, sia realizzando pubblicazioni in più lingue, sia dedicando intere linee di produzione ad un modulo linguistico specifico, con insistiti riferimenti al *Califfato* quale terra ideale per vivere e costruire il proprio nucleo familiare.

Alle prime, importanti sconfitte sul campo siro-iracheno è parso corrispondere un ridimensionamento quali-quantitativo dell'apparato mediatico, accompagnato, sul piano dei contenuti, da un progressivo venir meno dei richiami alle conquiste delle "Terre del Levante", a fronte di una immutata narrativa che – in analogia con quella del qaidismo storico – individua il *nemico* da combattere nei "Paesi Crociati" e nell'Occidente ("miscredenti"), nei Paesi musulmani "apostati" e nelle comunità sciite "eretiche". Può ritenersi emblematica di questo *trend* la nuova rivista di DAESH denominata *Rumiyah (vds. box n. 6)*.

DAESH ha comunque mantenuto la capacità di intervenire tempestivamente sulla scena mediatica quando ritenuto pagante sul piano propagandistico.

Anche *al Qaida* si è evoluta sul piano della comunicazione, rinnovando gli stru-

box 6

RUMIYAH

Il 5 settembre la struttura mediatica di DAESH, *al Hayat*, ha immesso *on-line* il primo numero di una nuova rivista, *Rumiyah* (lett. in arabo "Roma") seguito nell'anno da altri tre, diffusi rispettivamente il 4 ottobre, l'11 novembre e il 6 dicembre.

Riguardo alla scelta del titolo sono possibili varie ipotesi, ma in ogni caso è evidente il richiamo a Roma (intesa non solo come località geo-referenziata ma anche, in senso più ampio, come simbolo del "mondo crociato") quale meta finale dell'avanzata militare del *Califfato*.

Il *magazine* è realizzato in diverse edizioni linguistiche (inglese, francese, tedesco, russo, turco, uiguro, pashtun, bosniaco, curdo e indonesiano), tra loro non perfettamente coincidenti, essendo riscontrabili differenze in termini sia di *editing* sia di contenuto. *Rumiyah*, almeno nei suoi primi mesi

di vita, ha sostituito le riviste già esistenti, ciascuna indirizzata ad utenti ben individuati in base alle rispettive origini: *Dabiq* scritta in inglese, *Dar al Islam* in francese, *Istok* in russo e *Constantiniyye* in turco. La decisione di dar vita ad un'unica pubblicazione destinata a tutti i seguaci di al Baghdadi risponde verosimilmente alla necessità di riorganizzare l'apparato mediatico secondo una strategia di accentramento della propaganda, finalizzata a trasmettere un'immagine di maggiore forza e compattezza dell'organizzazione.

A fronte di una minore enfasi in tema di dimensione territoriale del *Califfato*, ci si sofferma sugli attacchi da compiere anche in Occidente, per i quali sono forniti suggerimenti tecnico-operativi. Ad esempio, a partire dal secondo numero, è stata inserita una sorta di rubrica dal titolo "*Just terror tactics*" in cui si indicano gli obiettivi da prediligere (strade, manifestazioni, mercati e, in generale, luoghi affollati), i diversi mezzi offensivi da utilizzare (...*se si decide di investire le vittime con un veicolo, è bene sceglierne di grandi dimensioni per massimizzare gli effetti*...) e, nel caso di azioni con armi da taglio, le parti del corpo da colpire.

menti e sperimentando nuove piattaforme, nel segno – anche qui – della continuità per quel che concerne i propri capisaldi ideologici retoricamente riferiti alla tutela dei luoghi sacri e alla vendetta nei confronti di USA ed Occidente in genere. Tra le novità, è emersa inoltre la pubblicazione – attraverso una serie speciale della rivista qaidista *Inspire* – di due documenti a firma *Lone Jihad Guide Team,* dedicati, rispettivamente, agli attacchi compiuti ad Orlando, in Florida (12 giugno) e a Nizza (14 luglio), peraltro rivendicati dalla formazione concorrente DAESH. Gli scritti propongono una sorta di *follow up* delle azioni, evidenziandone punti di forza e di debolezza, a riferimento di future operazioni da perpetrare in territorio americano ed europeo.

...e quella "orizzontale"

Per il suo impatto sui processi di radicalizzazione, ha continuato a rivestire specifico rilievo l'attivismo propagandistico di *foreign fighters* con cittadinanza o residenti nei Paesi europei, mossi non solo dall'obiettivo di cercare nuovi seguaci, ma anche dal desiderio di sentirsi ed essere considerati degli eroi da familiari e amici. Non è un caso che, appena raggiunto il teatro di conflitto, i combattenti si mostrino spesso desiderosi di condividere con il proprio circuito relazionale, e più in generale in modo aperto sui *social network*, fotografie nelle quali sono ritratti con abiti militari, in pose solenni. Un simile atteggiamento denota l'intento di suscitare ammirazione e approvazione ancor più che di alimentare un racconto glorioso a scopo di proselitismo, sebbene il semplice fatto di proporsi come modelli "virtuosi e vincenti" eserciti senza dubbio un forte richiamo emulativo su correligionari disorientati e alla ricerca di uno scopo.

IL *JIHAD* IN EUROPA

Vulnerabilità e rischi per l'Europa

Tra le criticità, sul terreno della prevenzione, si pone la circostanza che, nonostante la diffusa e consolidata consapevolezza della minaccia, permangono difficoltà oggettive da parte di singoli Stati a censire compiutamente i loro cittadini che hanno raggiunto Siria ed Iraq, condizione indispensabile per circoscriverne collegamenti nazionali ed internazionali e per individuare i circuiti relazionali che, anche sul piano logistico-finanziario, potrebbero agevolarne il ritorno nei Paesi di origine o di residenza.

Pur in assenza di univoche e convergenti indicazioni sulle dinamiche di rientro dei combattenti dal teatro siro-iracheno, non può essere esclusa l'eventualità di un loro ingresso clandestino in Europa in elusione dei controlli frontalieri.

D'altro canto, tra le "lezioni apprese" dagli eventi terroristici intervenuti nel 2016 vi è proprio la comprovata capacità, da parte di soggetti ricercati, di circolare anche per mesi nello "spazio Schengen" senza essere individuati. Aspetto, questo, che accentua il pericolo rappresentato dai *foreign fighters* e dalla possibilità che gli stessi, una volta rientrati in territorio europeo, possano ricevere linee guida ed indirizzi operativi attraverso contatti virtuali con soggetti basati nel cd. *Syrak* (quadrante siro-iracheno) o in altri Paesi.

Anche in questa specifica ottica, le evidenze intelligence hanno fatto stato della persistente centralità della regione balcanica, sperimentata sponda logistica nella direttrice di *mujahidin* in movimento tra l'Europa e il Medio Oriente (*vds. box n. 7*).

box 7

LA PRESENZA ISLAMICO-RADICALE NEI BALCANI

Il quadrante balcanico ha continuato a rappresentare una sorta di *hub* per il reclutamento di *foreign fighters* e *safe haven* per combattenti di rientro dai teatri di crisi mediorientali. Una diffusa rete di comunità musulmane radicali con forti legami con la diaspora all'estero, anche in Europa, ha agevolato l'opera di proselitismo e la partecipazione al conflitto siro-iracheno di numerosi individui di origine balcanica, nonché favorito lo sviluppo di *network* di supporto logistico, sfruttati da migliaia di combattenti in transito da Paesi europei (Italia inclusa) per raggiungere i gruppi jihadisti in Siria e Iraq. La permeabilità dell'area balcanica ad infiltrazioni terroristiche legata all'*humus* esperienziale di *ex mujahidin* del conflitto bosniaco del '92 e al dinamismo di predicatori radicali in contatto con omologhe figure attive in Europa e in Medio Oriente, ha insinuato una deriva estremista che, soprattutto in talune comunità wahhabite dell'area, ha presentato la partecipazione al *jihad* come attestazione di valore sociale e fonte di guadagno economico. Ad oggi, nonostante le costanti esortazioni di DAESH a colpire gli infedeli ovunque si trovino, richiamate anche in taluni video da jihadisti di origine balcanica, non sono state portate dirette minacce nei confronti di organismi internazionali militari e civili presenti nei Balcani. Tuttavia, la radicata presenza estremista proietta rischi concreti per la sicurezza e la stabilità dell'area, con immediate ricadute nei Paesi limitrofi ed europei, Italia inclusa.

La minaccia

Nel quadro delineato, l'esposizione dell'Europa alla minaccia terroristica è testimoniata non solo dalla richiamata serie di attentati, ma anche dalle numerose pianificazioni sventate o fallite, con arresti anche di donne e adolescenti, dall'aumento delle segnalazioni concernenti progettualità offensive da perpetrare in territorio europeo, nonché da valutazioni intelligence che – come già prospettato nella Relazione 2015 – fanno ipotizzare ulteriori, cruente campagne terroristiche in corrispondenza con gli arretramenti militari del *Califfato*. In questa chiave, nel composito contesto delle evidenze raccolte, non è da trascurare, tra i potenziali vettori di pericolo, il rinnovato attivismo in direzione dei Paesi europei da parte di soggetti ed organizzazioni radicali islamiche basate nel quadrante *Af/Pak* e sempre più coinvolte nel supporto a DAESH.

In una prospettiva di più lungo termine, è tra le ipotesi all'attenzione l'eventualità che un tracollo di DAESH in *Syrak* possa determinare non solo uno spostamento di combattenti in altri teatri di *jihad*, ma anche un rientro nei Paesi di provenienza di *mujahidin* di origine europea e delle rispettive famiglie, bambini inclusi, la cui "disintossicazione" e integrazione saranno prevedibilmente complesse (*vds. box n. 8*).

box 8

I "LEONCINI DEL CALIFFATO"

I bambini-soldato dei conflitti africani, come quelli reclutati da bin Laden nelle madrasse pakistane ci ricordano che il coinvolgimento di minori in attività terroristiche e in operazioni belliche non è una novità. Nel caso di DAESH, tuttavia, i "*leoncini del Califfato*" – espressione evocativa dei "*Leoncini jihadisti di Saddam*", gruppo estremista sunnita attivo nell'Iraq di Saddam Hussein – rappresentano un elemento chiave nell'orizzonte strategico dell'organizzazione di al Baghdadi, che nel marzo 2015, nel vivo della sua fase espansiva, pubblicava sulla rivista *Dabiq* un articolo intitolato "*I leoni di domani*", dedicato ai bambini-soldato cresciuti secondo la *sharia* nei campi di addestramento dell'organizzazione.

Nel corso del 2016, in corrispondenza con gli arretramenti territoriali di DAESH, ha assunto maggior rilievo nella propaganda il ruolo dei bambini quale garanzia di continuità del progetto califfale e della prosecuzione del *jihad* per la conquista di "*Damasco, Baghdad, Gerusalemme, Mecca, Dabiq, di Roma e dell'Andalusia*". In questo contesto si inseriscono i numerosi video che ritraggono, ad esempio, giovani seduti tra i banchi di scuola o nei campi di addestramento, ma anche mentre compiono efferate esecuzioni di *nemici dell'Islam*.

Al di là delle strumentalizzazioni mediatiche, la costante esposizione dei minori a così elevati livelli di violenza, unita al forte condizionamento ideologico subìto nella fase di formazione, concorre a delineare una minaccia di lungo periodo.

La situazione in territorio nazionale

Anche con riguardo all'Italia, è proseguita nel corso dell'anno la pressante campagna intimidatoria della pubblicistica jihadista caratterizzata da immagini allusive che ritraggono importanti monumenti nazionali e

figure di grande rilievo, tra cui il Pontefice. Tema dominante si è confermato quello dell'attesa della *conquista di Roma*, motivata anche dal ruolo assunto dal nostro Paese nella lotta internazionale al terrorismo e nella stabilizzazione delle aree di crisi, prima fra tutte la Libia.

I principali profili di criticità appaiono ancora riconducibili alla possibile attivazione di elementi "radicalizzati in casa", dediti ad attività di auto-indottrinamento e addestramento su manuali *on-line*, impegnati in attività di proselitismo a favore di DAESH e dichiaratamente intenzionati a raggiungere i territori del *Califfato*.

Al riguardo, sempre più concreto si configura il rischio che alcuni di questi soggetti decidano di non partire – a causa delle crescenti difficoltà a raggiungere il teatro siro-iracheno ovvero spinti in tal senso da "motivatori" con i quali sono in contatto sul *web* o tramite altri canali di comunicazione – determinandosi in alternativa a compiere il *jihad* direttamente in territorio italiano. È indicativo, in proposito, quanto emerso nell'ambito dell'operazione di polizia denominata "Terre vaste" che il 28 aprile ha portato all'emissione di sei ordinanze di custodia cautelare – a carico di altrettanti soggetti residenti nel nostro Paese – per il reato di partecipazione ad *associazione con finalità di terrorismo anche internazionale*. L'attività investigativa ha evidenziato, tra l'altro, il ruolo svolto da uno straniero il quale, partito dall'Italia nel 2015 con la famiglia per raggiungere il *Califfato*, ha messo in atto nei confronti di elementi presenti in territorio nazionale, su indirizzi dettati da DAESH, una sistematica attività di persuasione, esortandoli ripetutamente a non raggiungere le terre del *Califfato* ma, piuttosto, ad agire in Italia.

In prospettiva, come per altri Paesi europei, alla flessione delle partenze di *foreign fighters* dal territorio nazionale potrebbe corrispondere un aumento del rischio di attacchi "domestici" da parte di una o più persone legate da fattori di prossimità. Al riguardo, rilevano soprattutto legami familiari, rapporti amicali ed esperienze condivise di devianza negli ambienti delinquenziali e nelle strutture di detenzione.

I luoghi "fisici" della radicalizzazione

Ha continuato a destare attenzione il fenomeno della radicalizzazione all'interno degli istituti carcerari italiani, testimoniato anche dall'esultanza manifestata da diversi detenuti dopo gli attentati di Bruxelles e Nizza, indice di un risentimento potenzialmente in grado di tradursi in propositi ostili alla fine del periodo di reclusione.

Nel contempo, è parsa da non sottovalutare l'influenza negativa esercitata in alcuni centri di aggregazione da predicatori radicali o da altri personaggi dotati di una certa autorevolezza all'interno della comunità, soprattutto nei confronti di giovani privi di adeguata formazione religiosa che potrebbero essere indotti a una visione conflittuale nei confronti dell'Occidente, foriera di derive violente.

Gli aspetti collaterali

Oltre a rappresentare un potenziale *target* di attacchi diretti, il territorio nazionale potrebbe costituire un approdo o una via di fuga verso l'Europa per militanti del *Califfato* presenti in Libia o provenienti da altre aree di crisi, una base per attività occulte di propaganda, proselitismo e approvvigionamento logistico, nonché una retrovia o un riparo anche temporaneo per soggetti coinvolti in azioni terroristiche in altri Paesi, come verosimilmente accaduto nel caso dell'attentatore di Berlino, Anis Amri.

GLI SCENARI REGIONALI

Nelle aree di instabilità, soprattutto in taluni quadranti africani ed asiatici, l'azione pervasiva di DAESH ha interagito con gruppi islamisti locali, accentuandone la connotazione antioccidentale.

Si tratta di una tendenza che, da un lato, ha accresciuto la competizione con *al Qaida* – attivamente impegnata a preservare i propri "presidi" – e, dall'altro, ha innescato fermenti e dinamiche di confronto suscettibili di innalzare il livello della minaccia terroristica. Ciò in una prospettiva che non fa escludere la possibilità di convergenze tra frange qaidiste e filo-DAESH per la realizzazione di attentati contro gli USA e l'Europa.

In base agli indicatori raccolti, è destinata a rimanere elevata l'esposizione degli interessi italiani e dei connazionali all'estero, soprattutto nelle aree direttamente interessate da conflitti ed in quelle più vulnerabili al richiamo delle istanze jihadiste, come dimostra l'attacco del 1° luglio contro un ristorante di Dacca (Bangladesh), frequentato per lo più da occidentali, che ha provocato la morte di venti persone tra cui nove italiani.

Il poliedrico jihadismo in Africa

La penetrazione di DAESH in Africa ha modificato significativamente equilibri e rapporti di forza nella galassia jihadista continentale. In particolare, nei quadranti nordafricano e saheliano si è assistito ad un incremento delle iniziative delle formazioni legate ad AQ volte a ricercare più estesi spazi di manovra, nuove reclute e fonti di finanziamento, anche per mantenere un elevato profilo nel confronto mediatico con l'organizzazione irachena.

Nel contempo, sono stati raccolti inediti segnali in ordine a sopravvenute convergenze tattico-operative tra formazioni qaidiste e adepti del *Califfato*.

Dossier Libia

DAESH ha tentato di consolidare la propria posizione nel Continente africano attraverso l'acquisizione di un ruolo di primo piano in Libia, sfruttandone la fragilità del contesto politico e l'assenza di un efficace dispositivo di controllo del territorio, che hanno reso possibile l'insediamento di una base

strategica dell'organizzazione terroristica a Sirte e di cellule più o meno strutturate a Sabratah e Bengasi, in un generale contesto caratterizzato, a livello locale, da numerose realtà estremiste con proprie differenziate finalità.

Sul piano interno, il persistente clima di sfiducia tra la Camera dei Rappresentanti basata a Tobruk ed il Governo di Accordo Nazionale di Tripoli ha acuito le difficoltà del travagliato processo di riconciliazione nazionale e di stabilizzazione del Paese promosso dalle Nazioni Unite. La precarietà del quadro ha facilitato la proliferazione di milizie ed ostacolato la ristrutturazione di un apparato di sicurezza unitario che assicurasse un effettivo controllo del territorio.

La confusione istituzionale e i problemi dell'ordine pubblico hanno, dunque, offerto spazio alla pianificazione di azioni ostili da parte delle organizzazioni terroristiche attive nel Paese – tra cui *al Qaida nel Maghreb Islamico* (AQMI), *al Murabitun* (AM), *Ansar al Sharia* e lo stesso DAESH – che hanno goduto di ampi margini di agibilità per l'approvvigionamento di armi, il reclutamento di nuove leve e lo svolgimento di attività addestrative. La libertà di movimento ha anche favorito le sinergie tra i vari gruppi e l'interscambio di equipaggiamento e di personale, nonché il coinvolgimento delle citate organizzazioni nei traffici illeciti.

L'intervento militare messo in atto all'inizio di agosto 2016 dalle milizie di Misurata con il supporto della Comunità internazionale per debellare la presenza di DAESH a Sirte (operazione "*al Bonyan al Marsous*", "Edificio solido") ha causato un deflusso dalla città e una ricollocazione di jihadisti, perlopiù stranieri, i quali, scappati dalla città, si sono diretti ad Ovest (verso la Tripolitania), ad Est (verso Bengasi) e verso Sud (nel Fezzan). Quest'ultima area geografica era già caratterizzata dalla compresenza di etnie locali storicamente in conflitto tra loro (i Tebu e i Tuareg), di focolai di elementi riconducibili ad AQMI e, ancora, di gruppi criminali transazionali legati al traffico illegale di esseri umani.

Più in generale – anche per la mancanza di efficaci controlli – il Paese è risultato segnato, in numerose aree strategiche, da focolai più o meno consistenti di realtà jihadiste spesso eterogenee tra loro, in taluni casi alleate, in altri in conflitto.

L'attivismo radicale nelle altre realtà del Maghreb

La situazione libica ha concorso ad alimentare l'efervescenza dei gruppi estremisti nell'intera fascia del Maghreb, dove il terrorismo jihadista, endemicamente intrecciato con i fenomeni di criminalità, ha registrato un rafforzamento negli "organici" di DAESH, grazie soprattutto alle affiliazioni di gruppi locali. Ulteriori indici della pervasività e della capacità di presa della formazione irachena sono dati dal crescente numero di *returnees* provenienti dai teatri libico e siro-iracheno e dalla diffusione di dinamiche di radicalizzazione religiosa, fenomeno che attecchisce specialmente tra giovanissimi in cerca di un senso di appartenenza e di affrancamento dalla povertà.

In questa cornice si collocano le numerose operazioni di polizia condotte in Tunisia, Algeria e Marocco che hanno portato allo scompaginamento di reti terroristiche e filiere di supporto logistico al *jihad* combattente.

Nella nebulosa estremista del quadrante, specifico interesse riveste il gruppo *Ansar al Sharia in Tunisia*, i cui esponenti di maggior spicco (alcuni dei quali con trascorsi penali in Italia) hanno trovato rifugio in Libia, dove potrebbero rappresentare una minaccia per la sicurezza degli interessi nazionali. Tali ambienti hanno favorito, nel tempo, la creazione di centri di addestramento per militanti da instradare in teatri di *jihad* o da impiegare in operazioni terroristiche, come avvenuto nel 2015 con gli attentati a Tunisi (18 marzo) e Sousse (26 giugno).

L'influenza di DAESH è risultata particolarmente evidente nel panorama del jihadismo algerino, storicamente qualificato da AQMI e da ricorrenti sinergie fra gruppi terroristici e criminali di varia estrazione.

Le dinamiche regionali hanno trovato inoltre un punto di sensibilità nell'annosa questione del Sahara Occidentale, elemento di attrito e potenziale *vulnus* nella cooperazione antiterrorismo tra Algeria e Marocco.

Le reti del terrorismo subsahariano. Il Sahel...

Nel Sahel, AQMI ha incrementato la diffusione di comunicati contenenti minacce in direzione dell'Occidente, nonché dato nuovo impulso ad atti terroristici in Mali e nei Paesi limitrofi, grazie anche alla rinnovata collaborazione con AM ed *Ansar al Din*. Ciò ha determinato una ripresa delle attività terroristiche che dal 2013 si erano temporaneamente ridotte a seguito dell'avvio di operazioni internazionali di contrasto nel Nord del Mali e nel Sahel (operazioni *Serval/Barkhane* ed operazione MINUSMA). Sul piano operativo, AQMI ha dimostrato di essere in grado di condurre una serie di attacchi anche ad elevato impatto mediatico contro obiettivi ed interessi stranieri, come dimostrano gli attentati compiuti a Ouagadougou (Burkina Faso) il 20 gennaio 2016 e quello al *resort* di Grand Bassam (Costa d'Avorio) del successivo 13 marzo.

Alla minaccia proveniente da AQMI si è aggiunta quella posta dall'*Islamic State in Greater Sahara* (ISGS), attivo nell'area al confine tra Mali, Niger e Burkina Faso e composto da elementi che si sono dissociati da *al Murabitun* per affiliarsi a DAESH, che ne ha accettato l'alleanza il 30 ottobre.

..il versante occidentale...

Nel quadrante, spicca il ruolo di *Boko Haram* (BH), attivo in Africa Occidentale, specie in Nigeria, Niger, Camerun e Ciad. La formazione, che da marzo 2015 si è affiliata a DAESH ed ha assunto la denominazione di *Islamic State West Africa Province*, è stata attraversata da un confronto interno che ha causato una scissione tra la fazione fedele ad Abubakar Shekau e quella guidata da

Abu Musab al Barnawi, il quale è stato insignito da DAESH del titolo di "*Governatore dell'Africa Occidentale dello Stato Islamico*".

...e quello orientale

La principale formazione jihadista nel Corno d'Africa resta *al Shabaab* (AS), basata in Somalia ma con ramificazioni sia in Africa Orientale (Kenya, Etiopia, Gibuti, Tanzania) sia in Europa, dove operano soggetti dediti per lo più al supporto logistico.

In Somalia, la minaccia terroristica rimane elevata, poiché il citato gruppo si è mostrato ancora in grado di condurre azioni ostili di rilievo nonostante l'azione di contrasto posta in essere dalle Forze di sicurezza somale e da AMISOM. All'interno del movimento – tradizionalmente caratterizzato da una frammentazione di origine clanica che riflette il tessuto sociale somalo – è emersa all'attenzione una minoranza che ha dichiarato la propria affiliazione a DAESH, pur in assenza di una accettazione ufficiale da parte dell'organizzazione di al Baghdadi. La contrapposizione tra componenti qaidiste e filo-DAESH si è inasprita fino a produrre scontri anche molto violenti.

Nell'ambito della progressiva azione di espansione di DAESH nel quadrante si è collocata l'affiliazione della Brigata di AS denominata *Jaysh Ayman*, che rappresenta la branca di AS in Kenya ed opera nella zona confinaria tra i due Paesi.

Medio oriente: il teatro siro-iracheno, il confronto sunnita-sciita

Nell'articolato scenario mediorientale, il teatro siro-iracheno ha continuato a rappresentare il centro nevralgico della minaccia derivante da DAESH, nonché una sensibile arena di confronto tra interessi eterogenei.

In Siria, il coinvolgimento, diretto e indiretto, di attori esterni ha continuato ad influenzare l'andamento della crisi, in relazione alla contrapposizione tra potenze sunnite che sostengono, seppur in misura diversa, le formazioni politiche e i gruppi armati che avversano Bashar al Assad e l'asse sciita, comprendente l'Iran, gli *Hizballah* libanesi e le milizie sciite irachene, che supportano il regime alawita di Damasco.

Quest'ultimo, nel corso del 2016, ha riguadagnato terreno nelle aree di Aleppo, Damasco, Homs, Hama e Dara'a, tentando al contempo di riaccreditarsi presso la Comunità internazionale quale soggetto indispensabile nella lotta al terrorismo di matrice jihadista. Per altro verso, a fronte di un'accelerazione dell'offensiva governativa, le forze dell'opposizione hanno incrementato la propria collaborazione tattico-operativa con i gruppi di orientamento più marcatamente islamista, quali *Ahrar al Sham*, *Failaq al Sham* e *Nureddine al Zinki*, nonché con l'ex braccio armato di *al Qaida* in Siria, *Jabhat al Nusra*. Quest'ultima formazione si è dichiaratamente dissociata da *al Qaida-Core* (AQ-C), dandosi la nuova denominazione di *Jabhat Fatah al Sham*. Tale separazione è stata tuttavia da più parti valutata come

un'operazione puramente cosmetica volta a garantire, attraverso un riavvicinamento con i gruppi islamisti non jihadisti, la sopravvivenza stessa dell'organizzazione, oggetto di costanti bombardamenti.

Per quanto attiene alle modalità di attacco nell'ambito del confronto sul terreno, assume rilievo l'impiego di iprite da parte di DAESH, che ha evocato la possibilità di attacchi terroristici con aggressivi chi-

box 9

LA MINACCIA CBRN

Il rischio di attacchi CBRN, ovvero con armamento chimico-batteriologico-radiologico-nucleare, da parte di organizzazioni terroristiche permane alla costante attenzione della Comunità internazionale e degli Apparati di intelligence di tutto il mondo.

Per quanto attiene, di contro, ai programmi di proliferazione condotti da attori statuali:

- in relazione al *deal* iraniano, continua lo stretto monitoraggio dell'*Agenzia Internazionale per l'Energia Atomica* (AIEA) sull'attuazione del *Joint Comprehensive Plan of Action* (JCPoA) siglato a Vienna il 14 luglio 2015. Al riguardo, a fronte di un sostanziale rispetto, da parte di Teheran, delle clausole dell'accordo, rileva l'impegno della Comunità internazionale volto a trovare soluzioni definitive su talune questioni ancora oggetto di contrasti interpretativi. Il tema dello sviluppo del programma missilistico resta comunque un fattore di preoccupazione, anche in considerazione dei *test* effettuati da Teheran fino ai primi mesi del 2016;
- quanto all'attivismo nordcoreano, rilevano gli esperimenti nucleari effettuati nel gennaio e nel settembre 2016, che hanno suscitato clamore ed aumentato la preoccupazione della Comunità internazionale anche in relazione alle dichiarazioni del regime di Pyongyang sull'asserito raggiungimento di capacità di miniaturizzazione di ordigni nucleari veicolabili mediante sistemi missilistici a lungo raggio. Sotto quest'ultimo profilo, assume rilievo il lancio in orbita, nel mese di febbraio, di un satellite per l'osservazione terrestre, cui peraltro sono seguiti ulteriori lanci a scopo dimostrativo o sperimentale di altri sistemi missilistici. Ciò avrebbe concorso all'emanazione da parte del Consiglio di Sicurezza dell'ONU, in marzo, di un nuovo impianto sanzionatorio nei confronti della Corea del Nord, che implementa, aggravandole, le misure previste dalle precedenti deliberazioni delle Nazioni Unite (Risoluzioni n. 1718/2016 e 1874/2009). Il nuovo dispositivo, oltre a limitare ulteriormente l'interscambio commerciale nordcoreano con l'estero e a irrigidire il sistema dei controlli delle merci *in itinere*, prevede, tra l'altro, il congelamento degli *asset* riferibili a persone legate alla *leadership* di Pyongyang, nonché il divieto di apertura di uffici finanziari/bancari all'estero salvo approvazione del Consiglio di Sicurezza;
- in Libia, la precaria situazione di sicurezza ha contribuito ad imprimere una accelerazione al processo di smantellamento dell'arsenale chimico locale, costituito da precursori. Rientra in tale contesto la Risoluzione ONU n. 2298 del 22 luglio 2016, che ha autorizzato l'OPAC ad adottare talune misure che hanno consentito l'invio di quelle sostanze chimiche libiche in Germania per la successiva distruzione presso impianti opportunamente individuati.

mici, sebbene le capacità di guerra chimica dell'organizzazione siano parse limitate ad una produzione artigianale dell'agente vescicante (*vds. box n. 9*).

Come già detto, DAESH, dalla fine del 2015, contestualmente all'intervento russo in Siria e all'incremento dei *raid* aerei della Coalizione internazionale, ha subìto un progressivo ridimensionamento, territoriale, nella dirigenza – con l'eliminazione di esponenti di spicco, a partire dal portavoce Abu Mohammad al Adnani – e nelle risorse economiche. Le sue richiamate capacità di proiezione offensiva asimmetrica hanno trovato un significativo indicatore, tra l'altro, nella campagna terroristica condotta contro la Turchia, teatro, altresì, dell'uccisione dell'Ambasciatore russo ad Ankara (19 dicembre) – per mano di un poliziotto turco il quale, prima di essere neutralizzato, ha inneggiato alla vendetta per la perdita di Aleppo da parte di DAESH – nonché di una cruenta, parallela offensiva del tradizionale terrorismo di matrice separatista curda. Tutto ciò, in uno scenario interno attraversato dalle fortissime tensioni connesse al fallito golpe di luglio e alla decisa reazione di Ankara, tradottasi nell'adozione di provvedimenti restrittivi nei confronti di decine di migliaia di persone in seno alla Pubblica Amministrazione, a partire dagli apparati militari, giudiziari e di sicurezza fino al mondo accademico, della stampa e degli affari.

Anche in Iraq – ove le tensioni settarie tra la componente arabo-sciita e quella arabo-sunnita e curda avevano favorito le ambizioni di DAESH – il 2016 ha segnato un forte arretramento territoriale dell'organizzazione di al Baghdadi. Nello specifico, nel Governatorato di al Anbar, la presenza di DAESH è stata confinata ad un'area prossima al confine siriano a seguito della liberazione di Falluja, che era sotto il controllo di DAESH dal gennaio 2014. Il gruppo jihadista ha perso terreno anche nelle regioni centrali del Paese e nel Nord, dove ha continuato tuttavia a mantenere una forte presenza. A fronte di questa situazione, DAESH ha varato una strategia volta a distogliere lo sforzo bellico del Governo iracheno dalle zone occupate attraverso la realizzazione di attacchi complessi, azioni suicide ed un alto numero di attentati a mezzo ordigni esplosivi o autobomba in danno delle Forze di sicurezza irachene e di obiettivi sciiti anche nelle aree centrali e nel Sud del Paese.

La postura di Teheran

Dal canto suo, l'Iran ha continuato il percorso di riavvicinamento alla Comunità internazionale avviato con gli accordi sul programma nucleare e rafforzato dall'azione anti-DAESH avvalorata come argine al fondamentalismo di matrice sunnita. Tale processo appare finalizzato essenzialmente a due obiettivi di lungo termine: vedere riconosciuto il proprio ruolo di potenza regionale e consolidare la posizione di Teheran quale riferimento per la comunità sciita mondiale.

Le filiazioni di DAESH basate nel Sinai e a Gaza

Gli attentati compiuti sia nella Penisola del Sinai sia nella Capitale egiziana hanno confermato le persistenti capacità offensive di *Ansar Bayt al Maqdis-Wilayat Sinai* (*Stato Islamico-Provincia del Sinai*), affiliazione di DAESH, impegnata, da un lato, in attacchi pressoché quotidiani contro le Forze armate egiziane e, dall'altro, nel reclutamento di jihadisti anche all'interno della Striscia di Gaza.

La formazione ha espresso l'intenzione di colpire gli interessi di Paesi partecipanti a vario titolo ed in differenti contesti ad iniziative anti-DAESH. Al riguardo si sono registrati, tra l'altro, segnali di azioni di matrice jihadista nel Delta del Nilo, nella zona del Canale di Suez e nella regione del Deserto occidentale, che risente dell'impatto della crisi libica.

Il fenomeno jihadista nella Striscia di Gaza ha fatto registrare altresì l'attivismo di alcuni gruppi contigui a DAESH, anche se non formalmente ad esso affiliati. Le difficili condizioni socio-economiche, correlate con l'irrisolto conflitto con Israele e con il perdurante isolamento della Striscia, accrescono la capacità di presa di formazioni dell'estremismo salafita che tendono a contrapporsi al potere di *Hamas*.

I riflessi destabilizzanti della crisi siriana

La pervasività del fenomeno jihadista è emersa con evidenza in Paesi ove particolarmente onerose risultano le ricadute della crisi siriana. È il caso della realtà libanese, ove persiste la minaccia promanante soprattutto da DAESH e *Jabhat Fatah al Sham*, presenti anche nei campi profughi palestinesi ubicati nel Sud, area in cui è schierato, nell'ambito della Missione UNIFIL, un Contingente militare italiano. Anche con riferimento al contesto giordano rimane concreta l'evenienza che profughi affluiti dalla Siria possano incrementare le file di gruppi jihadisti e criminali.

La crisi yemenita e il confronto inter-jihadista

Il deterioramento della cornice di sicurezza nello Yemen ha reso più fluida la presenza di formazioni islamico-radicali sunnite che combattono i ribelli di matrice sciita Houthi ed oppongono resistenza al ripristino del controllo statuale. In tale contesto, si è evidenziato l'attivismo di DAESH tramite la sua affiliata *Wilayat al Yemen* che, dopo aver assunto di fatto il controllo di importanti zone territoriali, tra cui la stessa Provincia di Sanaa, ha mostrato di voler contendere ad *al Qaida nella Penisola Arabica* (AQPA) il ruolo di primario gruppo terroristico in un'area considerata di importanza strategica: per l'eventuale condotta di azioni ostili ai danni dell'Arabia Saudita; per il controllo del flusso di traffici illeciti da e verso la Somalia; quale snodo per i combattenti da inviare nel teatro siro-iracheno. Dal canto suo, il gruppo qaidista, pur avendo subìto, nel corso del 2016, una sensibile contrazione territoriale con la perdita di al Mukalla e di Aden quale conseguenza dei *raid* statu-

nitensi e della campagna della Coalizione araba, ha continuato a ricevere supporto dalle locali tribù, soprattutto nelle regioni centro-orientali del Paese.

La minaccia terroristica nelle monarchie del Golfo

Nel contesto saudita, fortemente esposto alle crisi che attraversano il quadrante mediorientale, si è rilevato un incremento della minaccia terroristica riferibile tanto ad AQPA quanto a DAESH, quest'ultimo interessato ad esasperare le latenti tensioni interconfessionali con finalità destabilizzanti.

In Kuwait, a seguito dell'attentato suicida del giugno 2015 contro la moschea sciita Imam al Sadeq nella Capitale, rivendicato da DAESH, le capillari contromisure adottate dalle Forze di sicurezza hanno portato, nel luglio 2016, allo smantellamento di cellule terroristiche sospettate di pianificare azioni ostili nell'Emirato.

Di rilievo, poi, il rischio che la presenza nel Bahrein sia di predicatori integralisti, sia di *returnees* dai teatri operativi possa favorire l'insediamento nel Paese di circuiti di propalazione dell'ideologia jihadista.

Il quadrante *Af-Pak*

Nel quadrante afghano-pakistano, in parallelo a forze tradizionali come i *Taliban* e altri attori locali, l'attivismo jihadista di maggiore momento è da ricondurre principalmente sia all'affiliazione di DAESH denominata *Islamic State in the Khorasan Province* (ISKP) sia ad *al Qaida*.

ISKP, costituita nel gennaio del 2015, si è attestata soprattutto nelle Province orientali e settentrionali dell'Afghanistan cercando, nel contempo, di conquistare margini di azione anche in Pakistan. È imputabile all'attivismo di tale gruppo l'attacco del 20 giugno 2016 a Kabul al minibus che trasportava addetti alla sicurezza dell'Ambasciata canadese, il primo importante attentato nell'area della Capitale rivendicato dalla citata sigla di DAESH (ma anche dai *Taliban*), cui hanno fatto seguito, tra l'altro, le azioni antisciite del 23 luglio e del 21 novembre. Gruppi armati locali comandati da elementi contigui a DAESH sono poi impegnati in frequenti scontri con le milizie *Taliban* nella Provincia occidentale di Herat, dove è stanziato il Contingente italiano. Pur nell'ambito di una missione *no combat*, il Contingente nazionale è stato quindi nel corso del 2016 esposto, direttamente o indirettamente, ai rischi derivanti dagli scontri in parola.

Con riferimento al territorio pakistano, dove il gruppo terroristico più aggressivo si è confermato il *Tehrik-e-Taliban Pakistan*, DAESH è andato assumendo un ruolo sempre più profilato nell'ottica della programmata espansione nella "*Provincia del Khorasan*", rivelandosi particolarmente attivo sul piano propagandistico e capace di svolgere attività di reclutamento e di addestramento di nuovi jihadisti. La proiezione di DAESH in Pakistan si starebbe affermando progressivamente anche attraverso la realizzazione ed il consolidamento di rapporti di collaborazione con alcuni gruppi radicali locali, tra cui *Lashkar-e-Toyba (LET)*.

AQ ha dal canto suo aumentato il proprio organico in Afghanistan a seguito del trasferimento di numerosi miliziani già attestati nelle *Federally Administered Tribal Areas* (FATA) pakistane, per effetto delle operazioni militari condotte dalle Forze di Islamabad. Di rilievo è inoltre, nello specifico contesto, il messaggio audio di Hamza bin Laden, figlio di Osama bin Laden, diffuso su internet il 10 luglio, in cui lo stesso giura vendetta contro gli Stati Uniti per l'uccisione del padre, avvenuta ad Abbottabad nel maggio 2011. Con tale messaggio, Hamza sembrerebbe volersi accreditare presso la galassia radicale islamica per assumere il ruolo di *leader* già detenuto dal padre e rilanciare AQ-C, ricercando in territorio afghano un nuovo *safe haven* per le proprie attività terroristiche.

In conclusione, il rafforzamento della presenza sia di DAESH che di AQ in Afghanistan profila il rischio di conferire nuovamente a quel quadrante la funzione di polo di attrazione per aspiranti *foreign fighters* provenienti non solo dai Paesi dell'area, ma anche da quelli occidentali, nonché terreno di ridispiegamento per terroristi in fuga dalla Siria e dall'Iraq.

Le formazioni jihadiste nell'Asia meridionale e sudorientale

Sotto il profilo della minaccia terroristica, il Sud-Est asiatico è stato caratterizzato dall'attivismo di formazioni terroristiche autoctone di matrice islamista che, organizzate su base territoriale, perseguono un'agenda autonoma finalizzata alla costituzione di un califfato nell'area e, più recentemente, dalla penetrazione di DAESH, determinato a guadagnare consenso presso le formazioni radicali locali e a promuovere iniziative a connotazione marcatamente anti-occidentale, con il fine ultimo di costituire una *wilayah* (Provincia) nella regione.

Nel Subcontinente indiano, la presenza di *al Qaida nel Subcontinente indiano* (AQIS) riflette la volontà di AQ di riconquistare la propria credibilità a fronte dell'ascesa di DAESH, di consolidare ed ampliare la presenza nel Sud-Est asiatico e di condurre azioni ostili in danno di istituzioni locali ed obiettivi occidentali. La capacità offensiva di AQIS si è manifestata con il gruppo affiliato *Ansar al Islam Bangladesh* (AaIB) che ha rivendicato gli omicidi di intellettuali, docenti universitari e *blogger* accusati di blasfemia.

Nei suddetti quadranti, DAESH ha "marcato il territorio": in Bangladesh, rivendicando una serie di attentati, incluso il citato attacco del 1° luglio al ristorante *Holey Artisan Bakery* di Dacca, realizzati, secondo quelle Autorità, dal gruppo locale *New Jamaat-ul-Mujahideen Bangladesh*; in Indonesia, assumendosi la paternità degli attentati di Jakarta del 14 gennaio 2016, che avrebbero visto il coinvolgimento, in qualità di organizzatore e finanziatore, di un indonesiano affiliato a DAESH e basato in Siria; nelle Filippine, dove ha recentemente proclamato la nascita di una nuova *wilayah* nell'isola di Basilan il cui emiro è il *leader* del gruppo terroristico *Abu Sayyaf*; in Malesia, dove la presenza dell'organiz-

zazione risulta confermata dall'attacco condotto il 28 giugno presso il *night-club Movida* di Puchong a Kuala Lumpur; in Myanmar, dove il movimento potrebbe giovarsi del supporto di segmenti della minoranza etnica musulmana dei Rohingya; in Thailandia, dove un gruppo affiliato a DAESH avrebbe creato una propria cellula, denominata *Black Swan*, ritenuta in contatto con i separatisti musulmani delle Province del Sud di lingua malese e a maggioranza musulmana, che da anni rivendicano l'indipendenza.

LA FINANZA DEL TERRORISMO

L'attività informativa e d'analisi sul versante del finanziamento al terrorismo ha posto in luce una sempre più accentuata tendenza alla diversificazione sia nelle fonti di approvvigionamento di risorse economiche, sia nei canali e negli strumenti di trasferimento dei fondi.

Per quel che attiene allo scenario estero, la ricerca intelligence si è focalizzata su DAESH, che in *Syrak*, nonostante la perdita di importanti posizioni e la correlata diminuzione di fondi raccolti e di liquidità complessiva, ha conservato nell'anno una sostanziale tenuta finanziaria. La primaria fonte di entrate è stata ancora espressa dal commercio illegale di prodotti petroliferi estratti dagli *oil field* all'interno ed all'esterno delle aree occupate, con traffici attestati su volumi considerevoli.

In particolare in Siria, i traffici di greggio, gas e derivati, pur se in diminuzione, hanno continuato a generare rilevanti proventi, anche perché i massicci *raid* aerei avrebbero marginalmente intaccato l'area siriana più produttiva di ricavi per DAESH (quella a Sud-Est di Dayr Az Zawr), con danneggiamenti parziali ma non definitivi alle principali strutture energetiche della zona, ridimensionate nei livelli di produttività, ma in grado, nel corso del 2016, di generare introiti consistenti.

Anche in Iraq, DAESH avrebbe continuato ad acquisire ingenti risorse finanziarie sia attraverso il contrabbando via terra, sia grazie alle contaminazioni con il circuito economico legale che gestisce l'*export* del greggio siriano e, soprattutto, iracheno e curdo, verso i mercati internazionali. Particolare rilievo assumono in tale ambito anche le attività finanziarie collegate al petrolio ed al reimpiego dei fondi sul campo, agevolate dalla penetrazione che DAESH è riuscito a realizzare nel sistema bancario sia dell'Iraq che di attori non statuali.

In Libia, i successi registrati sul piano militare dalle milizie oppostesi a DAESH hanno intaccato le capacità di finanziamento dell'organizzazione terroristica. In tale contesto, particolare criticità hanno rivestito le potenziali interazioni tra gruppi terroristici e *network* criminali attivi nel traffico di esseri umani e nelle relative condivisioni dei proventi illeciti.

In continuità con quanto rilevato nella Relazione 2015, le mire espansionistiche di DAESH nel quadrante afghano-pakistano

sono parse ancora sostenute dalle contribuzioni di *sponsor* localizzati nella Penisola arabica, oltre che da quelle rese disponibili dai vertici dell'organizzazione. Tali flussi finanziari – canalizzati nell'area prevalentemente attraverso i circuiti informali dell'*hawala*, nonché con la complicità di uomini d'affari afghani e pakistani – hanno registrato, nei primi mesi del 2016, un *trend* in ascesa, cui ha corrisposto una progressiva contrazione di quelli diretti alle formazioni *Taliban*. Queste ultime hanno mantenuto comunque significative capacità operative e finanziarie: il movimento, infatti, oltre a poter contare sulle entrate derivanti dal sistema estorsivo adottato nelle aree controllate e, soprattutto, dalla tassazione dei lucrosi traffici di droga, avrebbe sfruttato la congiuntura per catalizzare nuove risorse da attori regionali nel dichiarato intento di contrastare fattivamente l'avanzata di DAESH.

Nel Corno d'Africa, nonostante gli sforzi di AMISOM e il dibattito interno circa l'affiliazione al DAESH, l'organizzazione terroristica *al Shabaab*, complice anche un complesso sistema di relazioni sociali che le ha permesso di insinuarsi nell'economia legale inquinando i circuiti finanziari, ha continuato ad esercitare un controllo forte, capillare e stabile su estese aree della Somalia. Le fonti diversificate di approvvigionamento, legali o illegali, hanno assicurato all'organizzazione terroristica una solidità finanziaria che ha potuto sostenerne le capacità operative.

Per quanto concerne il monitoraggio intelligence sul territorio nazionale, specifica attenzione è stata prestata ai flussi finanziari movimentati – sia attraverso il sistema *hawala*, sia mediante la complicità di *money transfer* – da elementi a rischio potenzialmente in grado di offrire sostegno a strutture jihadiste operanti nei Paesi di origine.

Al fine di individuare anomalie o criticità connesse a possibili operazioni di supporto finanziario al terrorismo jihadista, hanno rivestito interesse informativo le attività rientranti nel "microcredito", strumento particolarmente usato dalle diaspore presenti in Italia.

PAGINA BIANCA

IL FENOMENO MIGRATORIO NELLA PROSPETTIVA INTELLIGENCE

PAGINA BIANCA

IL FENOMENO MIGRATORIO NELLA PROSPETTIVA INTELLIGENCE

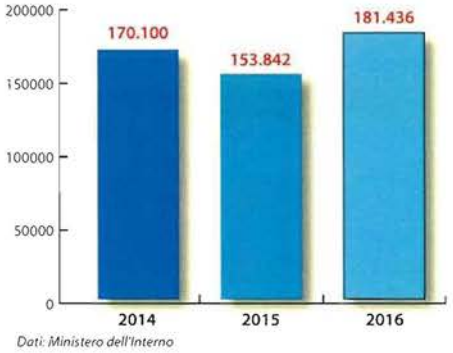
L'impegno intelligence in direzione dei flussi migratori irregolari si è dispiegato in una logica coordinata e multidisciplinare, in stretto raccordo interministeriale, a fronte di un fenomeno complesso tanto nelle cause concorrenti – guerre, instabilità politiche, povertà, squilibri demografici, cambi climatici – quanto nelle sue implicazioni sul piano della sicurezza.

Ai livelli emergenziali assunti dalla corrente migratoria via mare (*vds. box n. 10*), anche per i costi in vite umane, ha corrisposto una sua connotazione sempre più strutturale, che alle cause endemiche profonde accompagna fattori eterogenei e di diverso segno, quali il persistere del *vulnus* libico, la posizione cruciale dell'Italia nel Mediterraneo, la crescita organizzativa dei *network* criminali interessati ad alimentare il traffico di migranti per ragioni di profitto, le difficoltà di maturazione di una piena e condivisa consapevolezza, in ambito europeo, della portata del fenomeno e della sua posta in gioco, cui ha corrisposto il ruolo propulsivo

box 10

LE CARATTERISTICHE DEL FENOMENO MIGRATORIO VIA MARE

Secondo i dati del Ministero dell'Interno, nel 2016 sono sbarcate in Italia (per la quasi totalità dopo essere state soccorse in mare), 181.436 persone, quasi il 18% in più rispetto al 2015, con ciò superando (di poco meno del 7%) il dato record del 2014.



Dati: Ministero dell'Interno

Dall'analisi dei dati del Viminale, inoltre, possono enuclearsi alcune linee di tendenza. Per quel

che concerne i Paesi di partenza, in termini percentuali il fenomeno, pur a fronte dell'aumento in cifre assolute e di variazioni nella geografia dei flussi, è rimasto sostanzialmente invariato non solo per quel che concerne la Libia, ancora territorio di imbarco in quasi il 90% dei casi, ma anche per l'Egitto, che si conferma secondo Paese per numero di imbarchi (7%). Con valori più contenuti, va segnalato un incremento delle partenze dall'Algeria (la cui incidenza percentuale è passata dallo 0,2% allo 0,6%) e dalla Tunisia (all'incirca dallo 0,4% allo 0,6%). Anche i flussi provenienti dalla Turchia hanno fatto registrare un lieve incremento percentuale (dall'1,6% al 2,1%). Per quel che concerne le nazionalità dichiarate al momento dello sbarco, come per il 2015 vi è stata prevalenza di africani della fascia subsahariana, primi fra tutti i nigeriani (oltre 37mila), seguiti dagli eritrei (più di 20mila).

svolto dal nostro Paese per il varo e l'attuazione di mirati interventi comunitari .

Geografia dei flussi ed attori coinvolti

La rotta del Mediterraneo centrale che lungo la direttrice nordafricana attinge alle nostre coste meridionali ha rappresentato la principale via d'accesso all'Europa, anche in relazione ai mutamenti intervenuti ad Ovest e ad Est. Sul versante del Mediterraneo occidentale, i rafforzati controlli congiunti tra Marocco e Spagna hanno sostanzialmente bloccato i flussi attraverso quell'itinerario, riorientandoli in parte verso la Libia. La direttrice del Mediterraneo orientale ha registrato una notevole riduzione dei transiti per la rotta balcanica a seguito delle restrittive politiche di accoglienza e di gestione delle frontiere adottate a più riprese dagli Stati interessati dall'emergenza migratoria, nonché dell'accordo siglato in marzo per il contenimento del fenomeno (*vds. box n. 11*).

La rotta libica

Il territorio libico ha consolidato il preminente ruolo di *hub* di raccolta e partenza dei migranti diretti verso l'Italia, risultando la via di transito più battuta per i migranti provenienti soprattutto dal Corno d'Africa e dal Golfo di Guinea. In particolare, le rotte utilizzate per il trasferimento di profughi e irregolari verso l'Europa hanno seguito anche nel 2016 le seguenti direttrici principali:

- la cd. "transahariana", che congiunge i Paesi dell'Africa occidentale alla Libia attraverso Burkina Faso, Mali e Niger;
- quella "sudanese", che vede transitare masse migratorie provenienti dai Paesi del Corno d'Africa dirette prevalentemente in Libia e, in misura minore, in Egitto;
- una terza, di minore consistenza, che interessa i territori algerino e tunisino, verso i quali vengono indirizzati migranti nordafricani e subsahariani già presenti in Marocco ed impossibilitati a raggiungere l'Europa attraverso la Spagna. Dagli snodi algerini e della Tunisia meridionale, i migranti proseguono per lo più in direzione della Libia e quindi verso l'Italia.

L'evoluzione della situazione in Libia ha concorso a determinare, a partire dalla fine del 2015, alcuni cambiamenti nelle dinami-

box 11

LE ALTERNE VICENDE DELLA ROTTA BALCANICA

La cd. *rotta balcanica* è da intendersi come tratta intermedia di un itinerario ben più lungo ed articolato che trova origine in Paesi asiatici e mediorientali (Afghanistan, Pakistan, Iran e Iraq) e arriva nella regione dell'Anatolia. Successivamente, sia attraverso il Bosforo e il Mar Nero in direzione della Bulgaria, sia attraverso la Grecia continentale (quest'ultima raggiunta via mare direttamente dalle coste turche con imbarcazioni spesso non adeguate a sopportare la traversata e pertanto talvolta causa di drammatici naufragi), la rotta penetra nei Balcani in direzione dell'Europa centrale e settentrionale.

Le dimensioni assunte dal flusso migratorio sulla rotta balcanica tra la fine del 2015 ed i primi mesi del 2016 hanno provocato la chiusura delle frontiere anche da parte dei Paesi tradizionalmente più ospitali (ad es.: le Nazioni scandinave), che si è progressivamente estesa a gran parte della UE e agli Stati balcanici.

Dall'attuazione degli accordi di marzo 2016 tra UE e Turchia, gli arrivi in Grecia sono drasticamente diminuiti. Infatti, mentre nel periodo luglio-dicembre 2015 sono transitati per la rotta balcanica oltre 800mila migranti e profughi (e nei primi tre mesi del 2016 circa 160mila), nel resto del 2016 hanno viaggiato poche decine di migliaia di individui, perlopiù destinati nei Paesi del Nord Europa.

che locali circa i porti e i punti di partenza. Infatti, dopo che le milizie governative locali si sono insediate nella zona, le partenze da Zuwarah si sono fortemente ridotte (e pressoché azzerate quelle da Bengasi). L'aumento dei controlli ha contribuito a spostare i movimenti dei migranti specialmente nell'area di Sabratah e Garabulli, ove insistono strutturate reti di trafficanti talora contigui, se non interni, a milizie e ad ambienti estremisti. L'organizzazione del viaggio dalle coste libiche prevede l'impiego di natanti economici, appena in grado di coprire distanze utili all'intercettazione e al soccorso da parte dei dispositivi nazionale ed internazionale.

Le aree secondarie di imbarco

Dai porti dell'Egitto – a sua volta Paese di destinazione di ingenti flussi – si è rilevato un sostenuto ritmo delle partenze via mare, anche per l'attivismo delle locali filiere criminali e malgrado i maggiori costi dovuti al

tragitto più lungo. Si è evidenziato, in tal senso, il prevalente impiego di imbarcazioni in legno, più idonee – rispetto ai precari gommoni utilizzati sulla rotta libica – a coprire distanze maggiori.

L'incremento, seppure contenuto, delle partenze dall'Algeria, in conseguenza della citata chiusura della via migratoria verso la Spagna – interrotta dal rafforzamento del presidio a Ceuta e Melilla, le due *enclavi* spagnole in territorio africano – testimonia la flessibilità operativa delle organizzazioni criminali, indotte a deviare parte dei flussi verso il Sud della Tunisia da cui raggiungere la costa libica e infine l'Italia, oppure, in alternativa, ad organizzare trasferimenti diretti dalle coste algerine verso la Sardegna meridionale.

Per quel che attiene alla citata direttrice del Mediterraneo orientale, le acquisizioni raccolte hanno consolidato le pregresse evidenze attestanti la parziale riconversione al traffico di migranti da parte di contrabbandieri brindisini, in grado di assicurare alle reti presenti nei Balcani supporto logistico, inclusa la fornitura di natanti veloci per l'attraversamento dell'Adriatico, utili ad eludere la sorveglianza e l'intercettazione da parte delle Forze di polizia. In particolare per la tratta Turchia-Italia è stato segnalato, come già in passato, l'impiego anche di imbarcazioni da diporto affidate a *skipper* dell'Europa dell'Est che permettono ad una utenza facoltosa, disposta a pagare cifre più elevate rispetto a quelle pretese per raggiungere l'Italia partendo dalla Libia o dall'Egitto, di approdare eludendo i controlli, così da proseguire il viaggio alla volta del Paese di destinazione finale.

Le modalità operative

Più in generale, per quanto concerne le organizzazioni criminali coinvolte nel fenomeno migratorio irregolare, si è ulteriormente accresciuta nel corso del 2016 la competitività dei trafficanti internazionali, mostratisi in grado di:

- cooperare secondo criteri di specializzazione, formando *network* dinamici e transnazionali;
- esercitare un controllo capillare del territorio di riferimento, avvalendosi, all'occorrenza, di collusioni a livello locale che garantiscono sia il transito sia il supporto logistico dei migranti nelle aree di raccolta e di imbarco;
- monitorare le politiche di contrasto e di accoglienza adottate dai Paesi europei, ponendo in essere contromisure rapide e imprevedibili e fornendo, anche via internet, informazioni di tipo logistico e "promozionale" ai migranti.

Nel contesto, l'attività informativa in direzione delle organizzazioni criminali attive sulle diverse rotte percorse dai flussi migratori nel Mediterraneo, accompagnatasi alla promozione e allo sviluppo di mirate formule di collaborazione internazionale d'intelligence, è stata volta soprattutto a:

- svelare dinamiche e caratteristiche dei diversi sodalizi criminali quali i principali *hub* di raccolta, le rotte di trasporto marittimo, la tipologia dei natanti, le modalità di consegna dei migranti;

- identificare i vertici delle principali organizzazioni, le relative reti di supporto e gli eventuali collegamenti in territorio nazionale;
- tracciare i canali di movimentazione dei flussi finanziari e le correlate modalità di impiego, anche con riguardo alla possibile gestione "congiunta" di più attività illecite (traffico di esseri umani, narcotraffico, pirateria, contrabbando, prostituzione e, non ultimo, terrorismo).

Riflessi sulla sicurezza

La convergenza di interessi nella condivisione degli enormi profitti derivanti dalla gestione del traffico migratorio illegale può favorire, in aree caratterizzate da diffusa instabilità, l'interazione tra attori criminali ed espressioni dell'islamismo più radicale che condividono il locale controllo del territorio e le opportunità di autofinanziamento.

Con riferimento al rischio di infiltrazioni terroristiche nei flussi migratori, è significativo che due dei responsabili degli attentati di Parigi nel novembre 2015 abbiano raggiunto l'Europa sfruttando l'ondata di migranti che ha attraversato in quel periodo la dorsale balcanica.

Per quel che concerne la direttrice nordafricana, a fronte delle ripetute segnalazioni di minaccia sul possibile transito di estremisti in area UE attraverso la rotta libica, non sono emerse univoche indicazioni sull'esistenza di una strategia – riferibile a DAESH o ad altre organizzazioni terroristiche – intesa all'invio sistematico di propri operativi in Europa attraverso il canale dell'immigrazione clandestina via mare. Si tratta comunque di un'ipotesi alla costante attenzione informativa.

Uno dei principali ambiti di contaminazione tra circuiti criminali e terroristici resta, peraltro, quello dell'approvvigionamento di documenti di identità e titoli di viaggio. Infatti, come dimostrato dagli sviluppi d'indagine e dagli approfondimenti d'intelligence seguiti ai citati attacchi di Parigi e, altresì, a quelli di Bruxelles e Berlino (marzo e dicembre 2016), la mobilità di estremisti tra il teatro siro-iracheno e l'Europa, nonché all'interno dello "spazio Schengen" ha rappresentato e rappresenta un fattore di vulnerabilità per la nostra sicurezza anche in relazione all'utilizzo di documenti falsi, contraffatti o autentici (*vds. box n. 12*).

Per altro verso, l'ingente afflusso di migranti in territorio nazionale in un lasso di tempo relativamente breve rischia di:

- "stressare" le comunità straniere, anche a carattere etnico, presenti nel nostro Paese, incapaci di assorbire la gran mole di nuovi arrivi che vengono così esposti all'emarginazione sociale, determinando il rischio di possibili derive criminogene ed islamico-radicali quale frutto del risentimento per le aspettative tradite e del disappunto per le condizioni di disagio nei contesti ospiti. Peraltro, una presenza migratoria in cui assume rilievo una componente islamista più "radicale" ed aggressiva potrebbe condizionare e intimidire la prevalente

box 12

IL FALSO DOCUMENTALE

La falsificazione documentale svolge un ruolo chiave nelle dinamiche di favoreggiamento dell'immigrazione clandestina e rappresenta uno dei principali fattori di rischio in quanto non consente di valutare compiutamente l'entità e la caratterizzazione del fenomeno. Si tratta di un aspetto critico poiché, come nel caso degli ingressi "occulti", inclusi gli sbarchi in elusione dei controlli, la mancata identificazione e la correlata dissimulazione dell'effettiva provenienza del migrante possono veicolare:

- ex combattenti e soggetti in fuga da aree di crisi e da conflitti bellici, caratterizzati da un portato esperienziale in grado di conferire loro modalità reattive più aggressive;
- elementi dotati di un significativo *curriculum* criminale il cui impatto sulle comunità etniche di riferimento potrebbe comprometterne i legali percorsi di integrazione;
- individui esposti, nelle aree di transito, alle attività di proselitismo delle formazioni islamico-radicali capaci di sfruttare la costante connessione al *web* dei migranti per indirizzare loro messaggi di propaganda antioccidentale una volta giunti a destinazione.

componente "moderata" della comunità etnica di riferimento;

- incrementare lo sfruttamento dei migranti irregolari nei circuiti del lavoro nero, sovente dettato dall'impellenza del migrante di dover estinguere il debito contratto con le organizzazioni criminali per il trasferimento in Italia, oppure di reperire ulteriori risorse economiche per proseguire il viaggio alla volta dei Paesi del Nord Europa;
- affollare le strutture di accoglienza nazionali e ritardare le procedure di esame delle istanze di protezione, aumentando così il senso di frustrazione nei migranti e favorendo l'insorgere di proteste anche violente e, comunque, un atteggiamento nel complesso più aggressivo;
- favorire temporanee convergenze tra reti criminali nazionali e transnazionali nella gestione del remunerativo *business* legato al traffico di clandestini;
- aumentare l'impiego di sistemi informali per il trasferimento dei proventi illeciti del traffico migratorio, la cui gestione alimenta sia circuiti criminali sia ambiti legati al radicalismo confessionale.

LA TUTELA DEL SISTEMA PAESE

LEGENDA DEGLI ACRONIMI

DLT	Distributed Ledger Technology
EFTA	European Free Trade Association
GNL	Gas Naturale Liquefatto
IOC	International Oil Companies
NPL	Non Performing Loan
OPEC	Organization of Petroleum Exporting Countries
PIL	Prodotto Interno Lordo
PMI	Piccole e Medie Imprese
SICAV	Società di Investimento a Capitale Variabile
WTO	World Trade Organization

LA TUTELA DEL SISTEMA PAESE

Il quadro economico internazionale

Lo scenario economico mondiale è stato caratterizzato nel 2016 da una situazione di sostanziale incertezza. Mentre alcuni sistemi avanzati hanno registrato una crescita moderata, i Paesi emergenti hanno presentato, nel complesso, un quadro congiunturale debole, che ha negativamente inciso, in particolare, sulle loro transazioni commerciali a livello globale.

Numerosi sono stati i fattori di contesto che hanno contribuito a rendere più debole la ripresa economica, specie nel Continente europeo: le ripercussioni delle tensioni geo-politiche, il persistere di una bassa inflazione nonostante una politica monetaria accomodante di *quantitative easing* (volta ad alimentare la liquidità, a ridurre i premi per il rischio sulle obbligazioni private e a contenere le tensioni sui titoli sovrani), nonché le fragilità del sistema bancario gravato da crediti deteriorati, pesante eredità del periodo di recessione seguìto alla crisi del 2008.

A livello europeo, inoltre, la pronuncia referendaria del 23 giugno in favore dell'uscita della Gran Bretagna dall'Unione Europea ha aperto una fase nuova nelle dinamiche comunitarie, con conseguenze ancora ampiamente imprevedibili. Tempi, modalità e procedure, così come gli aspetti riferibili al futuro rapporto economico-commerciale tra la Gran Bretagna e lo spazio economico europeo (*vds. box n. 13*), dovranno infatti essere definiti in sede di negoziato per l'accordo di recesso.

Per quanto concerne l'Italia, la congiuntura interna, oltre a generare incertezza nelle imprese e nei consumatori, appare destinata ad avere effetti di breve/medio periodo sul Prodotto Interno Lordo (PIL) che, sulla base delle stime Istat, anche per i prossimi due anni viene previsto in crescita a saggi annui convergenti intorno alla soglia dell'uno per cento.

box 13

L'ITALIA E LA *BREXIT*

Alla luce dell'esito del referendum britannico è iniziata la riflessione sulle possibili linee di azione che l'Italia dovrà adottare per migliorare la cornice che garantisce lo sviluppo economico-finanziario del nostro Paese nell'ambito comunitario. A tale proposito appare rilevante, nelle trattative tra UE e Regno Unito, la difesa degli interessi nazionali che potranno essere messi in discussione durante la fase negoziale.

In un quadro più esteso, l'impatto commerciale, economico e finanziario della *Brexit* sull'Italia, nel breve-medio termine, sarà legato alle:

- dinamiche della domanda, e nello specifico ai consumi e agli investimenti di attori economici britannici e nazionali, strettamente collegati al percorso di uscita del Regno Unito;
- decisioni che saranno prese dalle Autorità di politica economica e dalle istituzioni finanziarie britanniche nonché europee;
- aspettative degli operatori economici e degli investitori in merito alla solidità del progetto comunitario. Tali aspettative stanno alla base dei complessi meccanismi di funzionamento del mercato reale, finanziario e valutario.

Il debole incremento, sostenuto da una ripresa della domanda interna e da un calo del tasso di disoccupazione, si prospetta, tuttavia, suscettibile di miglioramento, nella misura in cui i consumi delle famiglie continuano a crescere (+1,2% nel 2016), grazie a un costante aumento del reddito disponibile ed a contenuti livelli di inflazione, mentre il rafforzamento degli investimenti (+2% nel 2016) è sostenuto da mirate misure fiscali e da più efficienti condizioni di accesso al credito, rispetto all'immediato passato

Interesse nazionale e assetti strategici (*golden power*)

Lo stato dell'economia mondiale ha continuato a mantenere elevata la concorrenza internazionale, specie per quanto riguarda la capacità dei singoli Paesi di sviluppare efficaci politiche di attrazione degli investimenti esteri, fondamento essenziale per la crescita di un Paese inserito nelle *global value chains*.

Nel corso dell'anno appena trascorso, il monitoraggio dei settori rilevanti per gli interessi economici nazionali ha confermato il perdurare di consistenti interessi stranieri verso le imprese italiane, che hanno trovato concrete attuazioni sia attraverso l'acquisizione di partecipazioni nel capitale, sia tramite forme di *partnership* di diversa natura.

In tale quadro, la ricerca informativa è stata finalizzata alla tutela degli assetti strategici nazionali rientranti nel campo di applicazione della Legge 11 maggio 2012 n. 56 (*golden power*), fornendo specifico supporto informativo all'Autorità di governo circa l'applicazione dei poteri speciali su articolate operazioni societarie che hanno interessato perlopiù i settori dei trasporti, dell'energia, delle telecomunicazioni e della difesa. Il contesto è stato caratterizzato da un accentuato dinamismo che ha portato a vari casi di razionalizzazione degli assetti societari interni ed al coinvolgimento di primari *player* internazionali.

Le iniziative oggetto di approfondimento in quanto passibili di costituire rischi o

minacce per le infrastrutture critiche nazionali e per settori strategici del Paese, hanno riguardato prevalentemente conferimenti di rami d'azienda, costituzioni di *joint venture*, fusioni d'imprese, nonché cessioni ed acquisizioni di vario tipo.

L'interesse degli investitori esteri è stato principalmente focalizzato sull'acquisizione di *know-how* altamente specializzato di società dei settori difesa, infrastrutture, comunicazioni ed energia, come pure nei confronti di imprese nazionali specializzate nella realizzazione di reti internet. L'evoluzione di tale settore implica, infatti, lo sviluppo incrementale delle interconnessioni tra Paesi industrializzati e il rafforzamento dei canali esistenti in chiave securitaria. Ciò in un contesto che vede il Mediterraneo, e in particolare l'Italia, quale Paese sempre più strategico per il passaggio di dorsali di collegamento tra l'Europa e il Continente asiatico.

L'attività di intelligence si è orientata, altresì, nei confronti di condotte estere potenzialmente lesive del corretto sviluppo della concorrenza internazionale e dell'allocazione efficiente delle risorse, nonché verso politiche economiche aggressive nell'attrazione di capitali stranieri.

Nell'ambito di questa attività, improntata a fornire sostegno all'internazionalizzazione del sistema produttivo nazionale, l'attenzione si è concentrata sull'individuazione di profili di opportunità e di rischio connessi all'attivismo di soggetti legati ad entità statuali terze (*in primis* Fondi Sovrani).

Il sistema bancario e finanziario

L'attività intelligence di tutela della solidità dei mercati del credito e finanziario si è espletata lungo due direttrici: anzitutto si è guardato alle dinamiche tecniche in materia di mercati finanziari internazionali, approfondendo temi afferenti al settore del *fintech* (raccolta di capitali dal pubblico dei risparmiatori, valute digitali quali ad esempio il *bitcoin*, sistemi di valutazione del rischio del credito ecc.), alla disintermediazione bancaria, al *crowdfunding* ed alla *Distributed Ledger Technology* (DLT), cercando di identificare ed anticipare eventuali fattori di rischio per il sistema finanziario nazionale; in secondo luogo, si è mantenuta alta l'attenzione per le strategie adottate da grandi fondi di investimento o da istituzioni finanziarie estere al fine di individuare comportamenti lesivi degli interessi nazionali ed eventuali minacce alla stabilità sistemica.

A tal riguardo, l'attenzione informativa si è concentrata sia sulle eventuali ingerenze passibili di interferire nel corretto funzionamento del mercato creditizio nazionale che sulle violazioni da parte dei fondi di investimento delle norme a tutela dei risparmiatori.

Sullo sfondo, le sensibili dinamiche del sistema creditizio correlate alla gestione dei crediti deteriorati (cd. *Non Performing Loan* – NPL) e all'eventualità di operazioni di ricapitalizzazione di istituti nazionali, indotte dalla necessità di ottemperare ai parametri prudenziali europei fissati a livello centrale.

Nella medesima ottica di tutela, hanno rivestito interesse i rischi correlati, tra l'altro, a:

- ingresso speculativo nell'azionariato da parte di soci stranieri (in considerazione, soprattutto, del basso livello di capitalizzazione), con lo spostamento dei centri decisionali al di fuori del Paese;
- conseguenze sistemiche derivanti dall'applicazione per gli istituti in difficoltà del cd. *meccanismo di risoluzione* noto come *bail-in* (ovvero mediante il coinvolgimento di azionisti, obbligazionisti e correntisti).

Interessi stranieri per le imprese nazionali e tutela del *know-how*. Il supporto all'internazionalizzazione delle imprese italiane

Nel corso dell'anno, l'attenzione intelligence a tutela del patrimonio industriale nazionale è stata focalizzata sulla salvaguardia della eccellenza tecnologica, capace di generare e mantenere un vantaggio competitivo per il nostro Paese.

Nel senso, si sono confermate, come visto trattando dell'esercizio dei poteri speciali, mire espansionistiche di società estere nei confronti di aziende italiane in difficoltà dotate di elevate tecnologie e qualificato *know-how* industriale e commerciale, per consolidare le posizioni di mercato e diversificare le attività.

Tali manovre acquisitive, se da un lato rappresentano un'indiscussa opportunità, dall'altro potrebbero comportare criticità riconducibili alla eventuale natura speculativa degli investimenti, alla razionalizzazione dei costi riguardanti il personale e gli *input* produttivi, nonché alla sostituzione dell'indotto industriale di riferimento.

Alcuni settori industriali tradizionali del nostro Paese – a causa della congiuntura internazionale ancora fragile – si sono trovati in difficoltà, con cali degli ordinativi dall'estero che hanno determinato un ridimensionamento dell'attività industriale e conseguenti tagli di personale.

Con riferimento alla cessione di quote societarie riconducibili ad aziende di primaria rilevanza nazionale, sono emersi rischi di negative ricadute occupazionali, produttive e più in generale per il benessere economico e sociale del Paese, considerato anche il progressivo trasferimento all'estero di *asset* strategici nazionali.

In tale contesto, l'interesse è stato rivolto, inoltre, a:

- mercati strategici, come quello della chimica e delle materie plastiche, al fine di individuare eventuali comportamenti lesivi degli interessi industriali nazionali posti in essere da attori esteri in grado di manipolare i prezzi di mercato delle materie prime;
- operatori stranieri che hanno manifestato interesse nei confronti di piccole e medie imprese (PMI) italiane detentrici di elevato valore tecnologico che le rende *target* appetibili e, nello stesso tempo, sensibili sia per il loro portafoglio clienti, sia per la struttura delle filiere in cui operano.

Non è stato trascurato, poi, il settore della sicurezza dei trasporti marittimi internazionali, di valenza strategica per l'economia italiana, in relazione alla movimentazione sia delle materie prime provenienti dall'estero che dei prodotti esportati in tutto il mondo.

In considerazione della centralità assunta dall'internazionalizzazione del sistema produttivo nazionale quale leva di crescita del Paese, specifico interesse è stato riservato, all'estero, nella individuazione di possibili profili di rischio e opportunità riguardanti aziende colà operanti, ovvero intenzionate ad espandersi oltre confine, nonché nel rafforzamento dei rapporti con le istituzioni e gli enti competenti. Ciò, in particolare, con riferimento alla possibile realizzazione da parte di imprese italiane di significativi investimenti connessi a rilevanti progettualità di natura infrastrutturale.

Nello stesso tempo, sono stati oggetto di attenzione i temi legati al commercio internazionale ed alla promozione dell'*export*, nonché, in particolare, alla tutela del *made in Italy*, la cui valorizzazione e difesa (rispetto, tra gli altri, ai fenomeni della contraffazione e dell'*Italian Sounding*) assumono un ruolo cruciale in una prospettiva di sostegno dell'intero sistema economico nazionale.

Spionaggio industriale

In parallelo allo spionaggio di stampo tradizionale, spesso agevolato da dipendenti infedeli, ha continuato a registrarsi la forte crescita della minaccia facente uso del *cyber* (*vds.* *allegato Documento di Sicurezza Nazionale*), in alcuni casi favorita dall'utilizzo di tecniche di ingegneria sociale. Trattasi di modalità di manipolazione consistenti in espedienti sempre nuovi volti a catturare informazioni sensibili, quali, ad esempio credenziali di accesso a sistemi informatici. Il che evidenzia come il fattore umano, anche in relazione all'uso dell'informatica, continui ad essere elemento decisivo e discriminante ai fini della sicurezza.

Sicurezza energetica: fonti e canali di approvvigionamento

I mercati energetici nel 2016 sono stati caratterizzati da marcata volatilità, indotta da una serie di concomitanti fattori: un eccesso di offerta (sostenuta anche dalle strategie dei maggiori produttori di greggio come Arabia Saudita e Russia e dalla ripresa delle esportazioni iraniane), il rafforzamento del dollaro statunitense e una crescita economica inferiore alle aspettative degli energivori Paesi orientali.

L'andamento, nel corso dell'anno del prezzo del greggio con oscillazioni massime al di sotto dei 50 dollari USA al barile, ha favorito le produzioni dei Paesi della Penisola Araba e indotto le maggiori *International Oil Companies* (IOC) e le aziende della filiera energetica a strategie di razionalizzazione dei costi e di ottimizzazione dei processi produttivi, dando vita, in alcuni casi, ad operazioni di concentrazione societaria.

Dopo un accordo informale raggiunto in settembre per determinare una risalita dei prezzi, in occasione della Conferenza dei Paesi dell'*Organization of Petroleum Exporting Countries* (OPEC) di Vienna del 30 novembre gli Stati membri hanno concordato di tagliare la produzione di 1,2 milioni di barili al giorno, riducendo l'*output* complessivo a 32,5 milioni. Sempre con la finalità di accelerare la crescita del prezzo del greggio, inoltre, il 12 dicembre i Paesi non-OPEC, per parte loro, hanno deciso di ridurre la propria produzione di 558mila barili al giorno.

Per altro verso, l'abbondanza di greggio sui mercati che ha caratterizzato parte del 2016 ha contribuito ad attenuare gli effetti della contrazione produttiva di fornitori come la Libia (*vds. box n. 14*), a causa delle perduranti tensioni interne, o la Nigeria, in relazione ai sistematici sabotaggi alle infrastrutture petrolifere.

In termini di dipendenza energetica, il deficit petrolifero dell'Italia con l'estero è rimasto sostanzialmente stabile, attestandosi intorno al 90%. Tuttavia è aumentata la diversificazione dei fornitori, rafforzando così la resilienza del sistema nel suo complesso.

Per quanto riguarda la raffinazione del greggio, si è registrata una leggera flessione delle lavorazioni da parte degli impianti nazionali, in linea con i *trend* europei. Sono inoltre lievemente diminuiti – pur restando positivi – anche i margini di raffinazione, sia in Italia che in tutta l'area mediterra-

box 14

LA LIBIA E L'APPROVVIGIONAMENTO ITALIANO

Pur nel difficile contesto di instabilità interna, la Libia ha contribuito in misura significativa all'approvvigionamento energetico nazionale, fornendo circa il 7% del gas e il 4% del petrolio importati dal nostro Paese nel corso dell'anno (dati MiSE e Unione Petrolifera).

Ciò è stato reso possibile, in particolare, dal fatto che non si sono verificati significativi danni alle infrastrutture gestite dalla *joint venture* ENI-NOC (l'ente petrolifero libico).

Nell'ottica del possibile incremento dell'*output* complessivo di greggio del Paese, si segnala la decisione assunta il 14 dicembre dalle brigate di Rayayina, villaggio sito a 30 km da Zintan, di riavviare dopo circa tre anni di blocco la produzione petrolifera dei giacimenti di Sharara (operato dalla spagnola REPSOL) ed *Elephant* (operato dall'ENI) verso, rispettivamente, la raffineria di Zawiya ed il complesso petrolifero di Mellitah.

Nondimeno la tensione nell'area rimane elevata, anche perché le poche infrastrutture petrolifere funzionanti (Mellitah e Wafa *in primis*) sono divenute luoghi simbolo che catalizzano, per la loro visibilità, iniziative di dissenso con continue minacce di chiusura.

A ciò si aggiungano le frizioni dovute alla conflittualità registrata in corso d'anno tra le *Petroleum Facilities Guard* (PFG) di Ibrahim Jadran e le forze fedeli al Generale Haftar per il controllo dell'*Oil Crescent* e dei principali *terminal* petroliferi per l'esportazione del greggio libico (Es Sider, Ras Lanuf, Zueitina). Sullo sfondo di tali contrasti, si è posto il delicato compito (da parte del *Governo di Unità Nazionale*-GAN libico) di distribuire equamente i fondi ancora disponibili per il pagamento degli stipendi del personale – che sorveglia le poche infrastrutture petrolifere ancora funzionanti – e per la manutenzione ordinaria delle stesse.

nea, mentre sono rimasti pressoché stabili nell'area nordeuropea.

In merito all'approvvigionamento di gas naturale via dotti, sono emersi profili di criticità connessi alla potenziale interruzione del flusso proveniente dalla Libia, mentre non si sono evidenziate particolari problematiche relativamente alle altre direttrici di approvvigionamento nazionale.

Nel contempo, le acquisizioni di gas sotto forma liquefatta (GNL) sono aumentate in tutta Europa, in conseguenza dell'eccesso di offerta globale e della connessa diminuzione dei prezzi. Si tratta di una tendenza che, a livello continentale, appare destinata a rafforzarsi, coinvolgendo potenzialmente anche l'approvvigionamento nazionale.

In generale, le prospettive di sviluppo infrastrutturale a livello europeo, specie con riguardo alle forniture di gas russo, appaiono destinate a vivacizzare il dibattito tra Paesi europei con interessi e priorità non sempre convergenti. Significativo, tra l'altro, il dinamismo attorno ai due progetti concernenti, rispettivamente, la direttrice settentrionale (raddoppio del *Nord Stream)* e quella meridionale (*Turk Stream*).

Le economie illegali: riciclaggio, evasione ed elusione fiscale

L'intelligence ha continuato a fornire supporto informativo nel quadro del più ampio sforzo per individuare capitali irregolarmente detenuti all'estero o sul territorio nazionale, nonché a colpire le organizzazioni e i canali che alimentano tale pratica illecita approfittando delle asimmetrie legislative che persistono in diversi Stati esteri.

Il contrasto all'occultamento dei capitali ha assunto valenza prioritaria, non solo in chiave anti evasione, ma anche per colpire fenomeni di maggiore e più diretta pericolosità sociale, rappresentando lo stadio finale di attività quali il riciclaggio e la corruzione. In tale ambito non vengono trascurati i nuovi strumenti che si stanno affermando con la *fintech*, che, sebbene perfettamente legali, in alcuni casi potrebbero prestarsi ad essere utilizzati per finalità illecite.

L'onda lunga della crisi economica che condiziona la crescita e le dinamiche di sviluppo del Paese ha continuato a produrre effetti in termini di penetrazione criminale nell'economia e di occultamento di fondi illecitamente accumulati.

Tra le pratiche illecite rilevate, quelle più insidiose si sono confermate:

- l'uso di carte di credito/pagamento anonime, alimentabili senza limiti di spesa;
- la strutturazione di architetture finanziarie realizzate attraverso *Società di Investimento a Capitale Variabile* (SICAV) e *trust*;
- le possibilità di sub-commissionare, solo cartolarmente, lavori appaltati in Italia al fine di drenare la maggior parte dei guadagni verso il territorio estero, scontando imposte di molto inferiori rispetto alla tassazione in Italia.

Sono emerse, inoltre, patologie in grado di incidere direttamente sull'efficienza e stabilità del sistema. In partico-

lare, si è registrata l'operatività di taluni circuiti professionali in grado di offrire ai cittadini italiani titolari di posizioni "in nero" soluzioni alternative alla regolarizzazione dei capitali posseduti all'estero.

Tra le iniziative illecite adottate, le principali sono risultate il trasferimento delle "provviste" disponibili su piazze finanziarie non cooperative e lo spostamento della residenza fiscale (in alcuni casi fittiziamente) così da eludere la normativa sullo scambio di informazioni. Parallelamente si è rilevata una significativa diffusione sul territorio nazionale di carte di credito "anonime", legate a conti *offshore*, in grado di garantire cospicui volumi di spesa non tracciabili e rimpatri "non contabilizzati" di capitali.

Il permanere di una dinamica ancora debole dei prestiti alle imprese, ha generato come ulteriori conseguenze l'abusiva mediazione creditizia nei confronti di imprenditori in difficoltà economica e l'acquisizione di società che versano in grave crisi finanziaria da parte di circuiti criminali.

Gli effetti sulla media e piccola imprenditoria sono stati rilevanti, accrescendo le attività usuraie, da un lato, e le sofferenze bancarie, dall'altro.

Sul fronte del riciclaggio internazionale, crescente rilievo hanno assunto due pratiche utilizzate sia dalla criminalità organizzata, sia dall'imprenditoria illegale: l'una che fa leva sul ricorso ad operazioni prive di sostanza economica, pur legali, con lo scopo di realizzare vantaggi fiscali illeciti (cd. *abuso di diritto*), e l'altra consistente nell'utilizzo sostanzialmente irregolare del *trust* per dissimulare, attraverso i meccanismi legittimi di tale istituto giuridico, origine ed effettiva titolarità dei capitali.

Le infiltrazioni della criminalità organizzata nel tessuto economico e produttivo nazionale

La criminalità organizzata ha continuato a occupare spazi imprenditoriali e a inquinare il libero mercato grazie all'ingente liquidità di denaro, provento dei traffici illeciti.

L'edilizia, i giochi *on-line*, lo smaltimento di rifiuti, la *green economy* e, soprattutto, gli appalti pubblici si sono confermati i settori dell'economia legale di principale interesse per gli investimenti da parte delle mafie nazionali. In relazione a tanto, sono state oggetto di attenzione le reti relazionali che la criminalità organizzata ha intessuto con gli altri attori delle *lobby* crimino-affaristiche: imprenditori, professionisti, faccendieri, dipendenti e amministratori pubblici.

Gli strumenti principe che la criminalità organizzata utilizza per penetrare i circuiti affaristici e ingerirsi nei processi decisionali pubblici e nel libero mercato sono, da una parte, lo scambio di reciproche utilità e il raggiungimento di un comune interesse economico, dall'altra, la corruzione, soprattutto nei confronti di pubblici amministratori e burocrati. In tal senso, la riforma del codice degli appalti, varata nell'aprile 2016, potrà contribuire a

contenere i fenomeni di ingerenza criminale nello specifico settore.

La criminalità organizzata di matrice nazionale, a fattor comune seppur con diverse gradazioni, ha continuato ad affinare le proprie capacità di infiltrare i processi decisionali pubblici e di alterazione del libero mercato, pur non rinunciando a mantenere, attraverso la pressione estorsiva e intimidatoria effettivamente esercitata, o semplicemente percepita, una pervasiva proiezione sul territorio di riferimento (*vds. box n. 15*). Unitamente al traffico di sostanze stupefacenti, che si conferma la principale fonte di finanziamento delle attività illecite e di riciclaggio dei sodalizi criminali, si è registrato il crescente interesse degli stessi su taluni aspetti della gestione del fenomeno migratorio.

box 15

MAFIE NAZIONALI: DINAMICHE ASSOCIATIVE

Cosa Nostra ha vissuto una stagione di incertezza. Fiaccata dalla sempre più incisiva e costante attività giudiziaria, è apparsa all'incessante ricerca di nuovi assetti che le consentano di sopperire a *leadership* dall'incerto carisma. In quest'ottica, la scarcerazione di alcuni esponenti di spicco della "vecchia guardia" da una parte potrebbe restituire alle famiglie maggiori progettualità, dall'altra essere foriera di fibrillazioni con le temporanee reggenze. L'organizzazione criminale siciliana è rimasta la forma più evoluta di mafia presente nel nostro Paese, capace da tempo di ibridare il proprio patrimonio genetico e finanziario nelle pieghe della società civile.

La **'ndrangheta** ha continuato, con grande spregiudicatezza e aggressività, nel suo processo evolutivo verso un modello di "mafia d'affari", svolgendo un ruolo sempre più centrale nei comitati criminoaffaristici tanto nella regione di radicamento quanto nelle aree di proiezione. Pur nella ricerca esasperata di nuovi spazi imprenditoriali e collusivi, nonché dell'adattabilità alla mutevolezza dei contesti, le cosche calabresi non hanno, però, allentato la presa sul territorio né hanno rinunciato alle tradizioni e ai riti arcaici di affiliazione e di riconoscimento. La modernità della 'ndrangheta ha trovato linfa vitale proprio nella sua storia criminale e nei suoi antichi codici, simbolo della tenuta delle cosche, della loro difficile permeabilità e dell'indissolubile legame con il territorio. La misura della perniciosità dell'organizzazione criminale calabrese per la sicurezza nazionale è data dalle operazioni di polizia giudiziaria, nonché dal crescente numero di attentati intimidatori, soprattutto in danno di pubblici amministratori, ma anche di imprenditori, professionisti e burocrati, verificatisi in Calabria nel 2016.

È proseguita la condizione di fluidità dei clan di **camorra** napoletani. Nel territorio della metropoli partenopea, il defilamento degli storici clan, indeboliti dall'azione repressiva che ne ha fortemente minato le *leadership*, ha continuato a lasciare spazio a gruppi e bande che caoticamente hanno continuato a contendersi il controllo delle piazze di spaccio, rappresentando, a causa dell'efferata spregiudicatezza dei nuovi giovanissimi protagonisti criminali, un *vulnus* per la sicurezza e l'ordine pubblico. Il respiro imprenditoriale e la capacità di ingerenza nei processi decisionali pubblici sono rimasti, pertanto, riservati

principalmente alle espressioni camorristiche più evolute dell'*hinterland* partenopeo settentrionale, del nolano e del casertano.

È rimasto fortemente variegato il panorama della **criminalità organizzata pugliese**, che ha confermato a fattor comune, la propria vocazione a presentarsi come mafia di "servizio", aperta a *joint venture* criminali, nonché la grande adattabilità ai contesti socio-economici. Le formazioni criminali presenti in Puglia hanno mantenuto, per la gran parte, ancora un carattere banditesco di limitato respiro imprenditoriale, con interessi soprattutto nel settore del traffico delle sostanze stupefacenti. Hanno fatto eccezione le espressioni del crimine organizzato salentino, maggiormente strutturate e in grado di esprimere progettualità, anche infiltrative, di più ampio spessore, evidenziando interessi anche nel traffico dei migranti.

Le mafie straniere in Italia

La criminalità straniera in Italia ha consolidato i propri caratteri competitivi nella gestione delle attività illegali interferendo sempre più sistematicamente nelle dinamiche e nei processi evolutivi delle comunità etniche di riferimento, nei confronti delle quali ha continuato a esercitare un forte potere intimidatorio e di controllo funzionale al reperimento di nuove risorse e a garantirsi un prezioso alveo omertoso in cui risiedere impunemente.

A tale scopo è ricorsa all'imposizione di propri modelli, sia sul piano sociale che imprenditoriale, secondo uno schema di tipo mafioso utile ad acquisire il dominio su attività economiche organizzate su base etnica e, con esso, un miglior posizionamento sociale per aumentare, in prospettiva, la capacità di esercitare la propria influenza relazionale e stringere legami, anche collusivi, con il contesto ospite.

Più in generale, il crimine organizzato transnazionale dimostra una maggiore attenzione all'immigrazione clandestina quale prezioso bacino per il reclutamento della manovalanza e per alimentare i circuiti dello sfruttamento sessuale e del lavoro in nero.

Tra le matrici criminali straniere che hanno evidenziato un'elevata strutturazione e i caratteri della transnazionalità, emergono i sodalizi:

- **nigeriani**, particolarmente attivi nel narcotraffico, nella tratta degli esseri umani, nell'immigrazione clandestina di connazionali e nello sfruttamento della prostituzione. La crescita dei *network* è stata sostenuta dallo strategico supporto fornito da una ramificata rete di omologhi gruppi criminali presenti sia in patria, sia in altri Paesi europei, che ha consentito di massimizzare i profitti del traffico di droga e della tratta degli esseri umani. I clan nigeriani hanno controllato con modalità mafiose le comunità etniche di riferimento e reclutato i clandestini africani quale manovalanza nelle piazze di spaccio, nel lavoro nero, nel caporalato e nello sfruttamento sessuale. Particolare criticità ha rivestito la crescente diffusione delle bande organizzate cultiste; dotate di elevate capacità intimidatorie e pre-

datorie soprattutto nei confronti dei connazionali, esse sono apparse spesso in reciproco conflitto e causa di vivo allarme sociale;

- **russofoni**, che sono andati affermandosi sia all'interno delle diaspore, ove hanno consolidato un atteggiamento paramafioso, parassitario e violento, sia all'esterno, relazionandosi con sistemi criminali transnazionali ed imponendo la propria competitività con modalità collusive e intimidatorie. Nonostante al suo interno conservi tipicità etnico-nazionali, la galassia russofona è riuscita a razionalizzare sinergicamente le risorse criminali per l'acquisizione di potere nei mercati illeciti internazionali, ben calibrando esercizio predatorio e infiltrazione economico-finanziaria;
- **del Corno d'Africa**, che hanno acquisito nel corso degli ultimi anni un'elevata capacità nel gestire, anche autonomamente, i flussi migratori che provengono dall'area d'origine e si dirigono, attraverso l'Italia, prevalentemente verso i Paesi del Centro e del Nord Europa. In tale ambito, dimostrano un'elevata competitività e abilità non solo nel reindirizzare prontamente i flussi migratori in ragione delle opportunità e delle criticità registrate nello scenario in parola, ma anche nel gestire i proventi illeciti;
- **di matrice albanese**, che occupano una posizione di primo piano nello scenario delinquenziale nazionale, favoriti da consistenti flussi migratori clandestini e dalla capacità di produrre efficaci sinergie con le organizzazioni mafiose italiane e straniere. Si radicano agevolmente nei diversi contesti nazionali, facendo perno, con la forza dell'intimidazione, sul supporto delle numerose comunità di connazionali. Il narcotraffico e lo sfruttamento della prostituzione continuano a rappresentare le principali fonti di arricchimento illecito, la cui efficiente e competitiva gestione permette loro di svolgere servizi di intermediazione a favore della criminalità organizzata nazionale;
- **cinesi**, sempre più modulati in un *network* crimino-affaristico transnazionale in grado di connettersi con le realtà criminali della medesima nazionalità presenti nell'area europea. Forti di un'estesa presenza sul nostro territorio, hanno esercitato un marcato controllo sulle dinamiche sociali ed economiche della comunità etnica. La *lobby* affaristica ha dimostrato di saper sfruttare le potenzialità criminali delle bande giovanili – attive soprattutto nelle principali aree metropolitane del nord e centro Italia – per condizionare o disarticolare la concorrenza commerciale di operatori connazionali.

Il contrabbando di prodotti petroliferi e il narcotraffico

Ha continuato a delinearsi nel corso del 2016 l'attivismo e la pervasività dell'industria criminale che, sfruttando appieno le crisi geopolitiche, in particolar modo dell'area del Mediterraneo e dell'Est

Europa, è in grado di ampliare i traffici illeciti ed accrescere i margini di profitto. In tale contesto è emerso, in particolare, un traffico internazionale di idrocarburi dai Paesi del Nordafrica verso le aree comunitarie.

Sono stati identificati, inoltre, individui di elevata caratura criminale indicati quali elementi chiave del narcotraffico in alcune aree geografiche considerate strategiche, anche sotto l'aspetto del riciclaggio dei proventi.

SPINTE EVERSIVE E ANTI-SISTEMA

PAGINA BIANCA

SPINTE EVERSIVE E ANTI-SISTEMA

Il fronte dell'eversione di matrice anarco-insurrezionalista

Nel corso del 2016 si è assistito ad un rinnovato slancio offensivo di matrice anarco-insurrezionalista con il "ritorno in scena" degli *informali* della *Federazione Anarchica Informale/Fronte Rivoluzionario Internazionale* (FAI/FRI), dopo l'agguato armato del maggio 2012 ai danni dell'AD di Ansaldo Nucleare e i plichi esplosivi inviati, nell'aprile 2013, ad un quotidiano e a un'agenzia di investigazioni privata.

Un attentato compiuto il 12 gennaio ai danni del Tribunale di Civitavecchia con un ordigno a basso potenziale è stato infatti rivendicato dall'inedito *Comitato pirotecnico per un anno straordinario*, FAI/FRI, che, facendo beffardi riferimenti all'evento giubilare e ai connessi appelli alla pietà e alla misericordia, lo ha inquadrato nella lotta contro la *repressione*, esprimendo solidarietà ai militanti prigionieri che "*non si sottomettono*" e critiche alla crescente "*militarizzazione del territorio*".

Qualche mese più tardi è comparsa un'altra sigla, anch'essa inedita, *Nucleo Danaus plexippus-FAI/FRI*, che ha firmato un documento dal titolo *Attacco senza limiti* – pervenuto via posta ordinaria, tra il 7 e il 9 giugno, ad alcune aziende operanti nel settore alimentare e delle biotecnologie e successivamente diffuso *on-line* su siti d'area – nel quale si annunciava una campagna di sabotaggio alimentare.

Sempre il 7 giugno, a Parma, è pervenuto alla sede dell'*Agenzia Europea per la Sicurezza Alimentare* un plico esplosivo, potenzialmente in grado di arrecare gravi danni, poi intercettato dal personale addetto alla sicurezza.

Il successivo 9 giugno, a Milano, presso la sede legale di una società attiva nel settore delle biotecnologie, è giunto un pacco bomba che è poi deflagrato, provocando il lieve ferimento del titolare dell'ufficio. Gli attacchi, pur non rivendicati, verosimilmente inquadrabili nella campagna contro

le *nocività*, sono apparsi riconducibili alla medesima matrice, considerati gli obiettivi presi di mira e i mittenti indicati sulle buste, corrispondenti alle stesse società destinatarie del comunicato FAI/FRI.

In questo quadro è intervenuta, in settembre, l'operazione di polizia giudiziaria *Scripta Manent*, che ha portato all'emissione di provvedimenti di custodia cautelare in carcere per associazione con finalità di terrorismo e di eversione nei confronti di sette soggetti (due dei quali già detenuti per il citato attentato del 2012), ritenuti fra i principali esponenti del "cartello" *informale* della FAI/FRI (*vds. box n. 16*).

Immediate sono state le reazioni della propaganda d'area, anche straniera, con numerosi comunicati che, sottolineando l'esigenza di appoggiare i compagni arrestati con *azioni dirette* di carattere violento, in linea con il messaggio veicolato soprattutto dal bollettino *Croce Nera Anarchica*, hanno dato il via a diverse sortite (sabotaggi, attentati incendiari ecc.), rivendicate in forma anonima, improntate alla *solidarietà rivoluzionaria* contro la *repressione* in Italia e all'estero.

In prospettiva, dopo l'operazione *Scripta Manent*, le possibilità di ripresa del progetto rivoluzionario specifico dipenderanno dall'impegno di quegli ambienti nel sollecitare un rinnovato confronto, anche con altre componenti, su prospettive, metodologie e finalità della *lotta*. In tal senso uno degli autori dell'attentato all'AD di Ansaldo Nucleare ha ribadito dal carcere la validità dell'*anarchismo d'azione* per superare l'*immobilismo* dell'area, mentre altri esponenti d'area hanno sottolineato come ad

box 16

OPERAZIONE *SCRIPTA MANENT*

L'operazione, condotta dalla Polizia di Stato e coordinata dalla Procura della Repubblica di Torino, ha riguardato diversi ambienti militanti nazionali vicini alla pubblicazione d'area *Croce Nera Anarchica*, con perquisizioni effettuate in varie Regioni. Il procedimento, che ne riunisce diversi precedentemente avviati anche da altre Procure, ha consentito di meglio delineare e attualizzare un quadro indiziario in parte già emerso nel corso delle indagini seguite all'attentato esplosivo rivendicato dalla FAI/RAT – *Rivolta Anonima e Tremenda* nel quartiere Crocetta di Torino nel marzo 2007. Gli Organi inquirenti hanno ricostruito la genesi e lo sviluppo del progetto FAI fin dagli anni '90, prima della sua formale costituzione nel dicembre 2003, fino alle vicende degli ultimi anni, con il confluire, nel 2011, nel *Fronte Rivoluzionario Internazionale*. È stata evidenziata, in particolare, la peculiarità dell'entità associativa, caratterizzata da una struttura unitaria, estremamente fluida e priva di gerarchie e ruoli, operante attraverso una pluralità di sigle.

esser presa di mira dalla *repressione* non sia una *singola bandiera* ma la stessa *idea anarchica*. Un impulso alla riattivazione proviene inoltre da omologhe compagini straniere, in particolare l'ellenica *Cospirazione delle Cellule di Fuoco,* da ritenersi l'espressione attualmente più "matura" sotto il profilo militare oltre che di maggior spessore per quanto attiene alla produzione ideologica. In ottobre la formazione, in occasione di un attacco con esplosivo compiuto ad Atene contro l'abitazione di un magistrato – "dedicato" nella rivendicazione anche ai militanti arrestati in Italia – ha annunciato il lancio a livello internazionale del *Progetto Nemesis*. Quest'ultimo, come spiegato in un documento diffuso nel successivo mese di novembre, consiste nella proposta di passare dall'attacco ai simboli del potere all'offensiva diretta contro le persone che lo incarnano; a questo fine è sollecitata la creazione di *liste* di nominativi (ovvero di *capi che ammazzano i propri lavoratori, sbirri... giudici... giornalisti... politici*) con l'obiettivo di studiarne spostamenti e percorsi e poter più facilmente colpire i *target* prescelti.

Non si può pertanto escludere che siano tentate, anche nel nostro Paese, nuove azioni volte a dimostrare la reattività dei circuiti anarco-insurrezionalisti alla *repressione,* sia targate FAI sia con gesti isolati, anche anonimi, coerenti con lo spontaneismo individualista tipico del più ampio movimento anarchico. Indicativi, al riguardo, i commenti positivi, postati su siti d'area, all'azione esplosiva – non rivendicata – perpetrata nella notte di Capodanno a Firenze ai danni di una libreria riconducibile alla destra radicale, che ha provocato gravi lesioni a un artificiere della Polizia di Stato intervenuto per disinnescare l'ordigno.

Proseguiranno altresì le campagne di lotta già intraprese da altre componenti anarco-insurrezionaliste su ulteriori fronti, a partire da quella contro i *Centri d'Identificazione ed Espulsione*-CIE (*vds. box n. 17*).

box 17

LA CAMPAGNA ANONIMA CONTRO I CIE

Nel 2016 è ripresa l'offensiva contro i CIE, lanciata nella primavera dell'anno precedente, con la diffusione sul *web*, da parte di un circuito libertario torinese, di un opuscolo contenente l'elenco delle imprese coinvolte *nella macchina delle espulsioni*, già concretizzatasi nell'invio, in quel periodo, di una serie di plichi esplosivi contro aziende dell'indotto citate nella pubblicazione.

Tra febbraio e marzo si è registrata sul territorio nazionale una seconda ondata di analoghi attentati contro società/ditte, anch'esse nominate nell'opuscolo, che forniscono servizi alle strutture di accoglienza/gestione dei migranti, rivendicati con un documento anonimo diretto a un quotidiano nazionale. Nel testo, oltre a richiamare precedenti attacchi, si esprime la radicale opposizione ai *lager del terzo millennio* e al sistema di *repressione* in generale, nonché la solidarietà con i *compagni prigionieri*, e vengono sollecitate ulteriori azioni. Una terza serie di plichi esplosivi è intervenuta, tra settembre e dicembre, contro obiettivi già presi di mira nel 2015 nella città di Torino.

Inoltre, dopo la pubblicazione, a fine aprile, di un'edizione aggiornata dello stesso opuscolo, contenente un nuovo elenco – diviso per aree territoriali – delle aziende impegnate nel settore, si sono intensificate le azioni, perlopiù di carattere vandalico, contro filiali del gruppo Poste Italiane, ritenuto anch'esso complice del *meccanismo di espulsione* degli stranieri irregolari, in quanto proprietario di una compagnia aerea impegnata nel rimpatrio dei migranti. Ai primi di giugno sono state anche tentate alcune azioni incendiarie ai danni di uffici postali di Torino, Bologna e Genova, verosimilmente con l'intento di elevare il livello della protesta contro l'aspetto specifico delle cd. *deportazioni*. Iniziative analoghe sono state condotte negli ultimi mesi dell'anno anche in altre città.

Anche nel 2016 è proseguito l'impegno dell'area libertaria sul fronte ostile alle *Grandi Opere, le nocività e la tecnologia*, registrando atti di sabotaggio contro obiettivi collegati a linee TAV fuori del territorio d'elezione valsusino e strutture di telecomunicazione, in particolare ripetitori telefonici. Tali azioni sono solitamente rivendicate in forma anonima con comunicati diffusi sul *web* nei quali motivazioni di carattere ambientalista e antirepressivo si intrecciano con espressioni di solidarietà per militanti inquisiti.

In prospettiva, potrebbero essere presi di mira anche obiettivi collegati al progetto del gasdotto TAP, contro cui si è intensificata la propaganda denigratoria.

Si è rilevato, infine, un aumento dell'impegno propagandistico e operativo – con iniziative di basso profilo – *contro la guerra* e il suo indotto, nel tentativo di promuovere un *antimilitarismo sovversivo* che si concretizzi in *azioni dirette* sul territorio. Allo scopo sono stati divulgati *on-line* documenti volti a individuare e mappare la presenza militare in Italia. Tale impegno potrebbe intensificarsi in relazione ad un maggiore coinvolgimento del nostro Paese in missioni internazionali e in attività di stabilizzazione all'interno dei principali teatri di crisi mediorientale nonché all'impiego di soldati nella prevenzione antiterrorismo e nella gestione dell'emergenza immigrazione.

Sul versante estero, l'attenzione dell'intelligence è stata rivolta, tra l'altro, al dialogo ideologico-operativo tra compagini e individualità dell'area nazionale ed omologhe formazioni straniere impegnate su comuni tematiche di lotta, tra le quali quelle anti-civilizzazione, anti-sistema ed in solidarietà con i *prigionieri politici*. In particolare, sono state monitorate le proiezioni

internazionali della FAI/FRI, con specifico riguardo alle iniziative contro obiettivi strategici all'estero all'indirizzo di simboli di *civilizzazione* e *globalizzazione*, nonché verso i cd. *strumenti della repressione* – soggetti e strutture preposti, a vario titolo e forma, al controllo sociale ed alla detenzione – oltre che nei confronti dei "*poteri economico-finanziari*", dei mezzi di comunicazione, delle strutture di "*sfruttamento delle risorse ambientali e di sviluppo tecnologico*".

In tale cornice, si è ulteriormente confermata l'esistenza di rapporti privilegiati tra gli *informali* italiani e gli omologhi greci della citata *Cospirazione delle Cellule di Fuoco*.

L'estremismo marxista-leninista

Gli esigui ambienti marxisti-leninisti rivoluzionari sono risultati, in continuità con gli ultimi anni, prioritariamente impegnati in attività teorico-propagandistica, intesa a tramandare il ricordo della stagione brigatista, nonché ad attualizzarne il messaggio ideologico. Lo scopo è di contribuire al proselitismo e alla formazione di nuove leve, ponendo quindi le basi per una futura "*ricostruzione/unificazione delle forze*". Funzionale a divulgare l'esperienza *lottarmatista* è la solidarietà ai "rivoluzionari prigionieri", sviluppata pure in contesti internazionali, con riferimento anche a formazioni terroristiche tuttora attive, in particolare in Grecia.

Tali circuiti, peraltro consapevoli delle condizioni di isolamento e debolezza in cui versano, intrattengono relazioni con la composita area antagonista, partecipando ad alcune campagne di lotta, nel tentativo di influenzarne la connotazione politica, volgendola da una dimensione meramente rivendicativa a una postura di irriducibile contrapposizione classe/Stato, in modo da ribadire la persistente necessità di un radicale sovvertimento del sistema costituito. Si assiste, così, all'adesione di realtà di matrice rivoluzionaria – seppure con i necessari distinguo ideologici – a più ampie e trasversali mobilitazioni, specie sul fronte dell'*antirepressione*, della solidarietà alla causa palestinese, della protesta sociale (emergenza abitativa, problematiche occupazionali ecc.).

Strumentale attenzione è rivolta alla popolazione immigrata, considerata componente essenziale del *nuovo proletariato metropolitano* prodotto dalla globalizzazione. Ha continuato inoltre a registrarsi un rinnovato interesse per talune situazioni geopolitiche ritenute espressioni del conflitto di classe e dell'antimperialismo, con attività di propaganda, sensibilizzazione e sostegno a favore delle repubbliche filorusse in Ucraina, dell'opposizione comunista in Turchia e della *rivoluzione curda* nel Rojava. Va infine emergendo l'aspirazione a costituire nel nostro Paese un movimento *contro la guerra*, suscettibile di essere declinato – da parte di questi ambienti – in chiave di *solidarietà di classe incondizionata a tutti i popoli aggrediti e resistenti*.

In linea di analisi, componenti di matrice rivoluzionaria potrebbero individuare in particolari tensioni nello scenario politico

e sociale nazionale e internazionale l'occasione per azioni di modesto spessore operativo, nell'intento di affermare la validità della "propaganda armata" e di provocare adesioni e fenomeni emulativi.

Le campagne antagoniste

Nel corso del 2016, l'attivismo delle compagini d'area si è focalizzato sul contrasto alle politiche economiche del Governo e alle misure di contenimento del *deficit* richieste dalla UE, riverberandosi sui molteplici fronti legati al disagio sociale, con riferimento, in particolare, alle problematiche del reddito/salario, casa, beni comuni.

In tale scenario, i *movimenti per l'abitare* hanno intensificato l'impegno propagandistico sfruttando il rilievo mediatico delle celebrazioni dell'Anno Santo straordinario nel tentativo di conferire visibilità e spessore alle proprie istanze di protesta. Nella propaganda di settore si è rimarcato come l'evento giubilare, *ipocritamente dedicato alla misericordia*, abbia comportato un impegno sociale solo *di facciata*, fornendo occasione per speculazioni affaristiche e spreco di risorse. Sul versante "di piazza", l'area antagonista, probabilmente anche a causa della sua frammentazione, non è riuscita a coinvolgere nella mobilitazione il *nuovo proletariato urbano*.

Nell'ultima parte dell'anno le varie componenti del movimento hanno recuperato una certa coesione intorno alla campagna per il NO al referendum costituzionale, percepita come un *obiettivo tattico* e un'occasione propizia per coinvolgere nel processo conflittuale le varie istanze sociali che si oppongono al Governo.

Da più parti è stata evidenziata la necessità di elevare il livello di protesta interpretando adeguatamente e dando voce al diffuso disagio che si vive in particolare nelle periferie, reputate luogo simbolo della *disuguaglianza sociale*, nonché importante bacino da sfruttare per l'attivismo di piazza.

Tuttavia, nonostante l'intenso impegno propagandistico profuso dagli ambienti d'area, la manifestazione nazionale, tenutasi a Roma il 27 novembre 2016, non ha fatto registrare l'impatto atteso in termini di conflittualità sociale.

Rinnovata rilevanza strategica ha progressivamente assunto la *campagna di lotta in solidarietà ai migranti e ai profughi* in fuga dai contesti bellici, reputata particolarmente pagante per la sua trasversalità.

Al centro dei rilievi critici delle varie formazioni e gruppi d'area si pongono le politiche *di chiusura* in materia di gestione dei flussi migratori, improntate, nell'ottica antagonista, al contenimento e alla *repressione*, anziché all'accoglienza, e funzionali a una crescente *militarizzazione* dei confini tra gli Stati.

La questione migratoria ha offerto alle componenti dell'area anarchica e antagonista l'opportunità di rinnovare efficaci sinergie transnazionali. Significative, a tal proposito, le iniziative promosse dagli ambienti antagonisti nazionali, in collaborazione con analoghi movimenti europei, nei Paesi mag-

giormente interessati dal fenomeno, in particolare tra Grecia e Macedonia e al confine con l'Austria. Nel contempo, la condivisa visione antirazzista e antifascista ha continuato a motivare la contrapposizione con le compagini della destra estrema impegnate a fomentare strumentalmente alcune situazioni di diffusa tensione sociale in chiave anti-immigrati e a cavalcare il disagio popolare a fini di proselitismo, innescando potenziali derive xenofobe e razziste.

Crescente rilievo, sia propagandistico che di piazza, ha rivestito, specie alla luce del progressivo allargamento dei teatri di conflitto, la tematica antimilitarista (*vds. box n. 18).*

Sul versante delle **lotte ambientaliste**, la campagna contro l'Alta Velocità in Val di Susa, considerata emblema delle *lotte di resistenza popolare* contro le *imposizioni* dello Stato, ha attraversato una fase di minor vigore, anche a causa del persistere delle di-

box 18

IL FRONTE ANTAGONISTA *CONTRO LA GUERRA*

L'attivismo in chiave antimilitarista si è tradotto in un'intensificazione della propaganda controinformativa, diffusa sia in rete che nei circuiti d'area, che ha stigmatizzato, tra gli altri aspetti, la percepita intensificazione delle politiche *autoritarie* e *repressive* in ambito nazionale e il protagonismo dell'Unione Europea, indicata come nuovo polo dell'*imperialismo capitalista*, potenzialmente alternativo e autonomo rispetto a quello statunitense.

Gli sviluppi dello scenario libico hanno contribuito a stimolare alcune riflessioni: l'impegno statunitense nel Paese nordafricano è stato, infatti, bollato come un'*operazione neocoloniale* e critiche sono state poi rivolte al ruolo di *supporto logistico* dell'Italia.

Sul versante della mobilitazione, significativi segnali di effervescenza si sono registrati nei contesti isolani, tradizionalmente percepiti come simboli della *colonizzazione imperialista* statunitense. In particolare, talune componenti dell'area sarda hanno avviato una campagna di sensibilizzazione sul tema dell'*occupazione militare* dell'isola, finalizzata a costruire un *movimento di massa organizzato* e a delineare un *percorso di lotta* contro le basi e le servitù militari, di cui si reclama la chiusura, la bonifica e la *restituzione* alle popolazioni.

Indicazioni di un rinnovato attivismo sono giunte anche dall'area siciliana, che, dopo una fase di depotenziamento della protesta, ha mostrato di seguire con interesse gli sviluppi giudiziari inerenti al sistema satellitare MUOS di Niscemi, specie a seguito del provvedimento di dissequestro dell'impianto satellitare avvenuto in agosto. In questo contesto sono emersi, inoltre, i primi segnali di propositi contestativi in direzione del Vertice G7 in programma a Taormina (ME) il 26 e 27 maggio 2017.

vergenze strategico-operative tra gli attivisti anarchici e le altre componenti valligiane che animano la protesta.

Nelle linee d'azione del movimento ***No TAV*** ha continuato ad avere rilievo centrale la tematica della *repressione*, alla luce della stigmatizzata recrudescenza dell'attività investigativa nei confronti dei militanti, considerata un tentativo di *intimidazione* finalizzato a disarticolare la protesta. In tale quadro, sono proseguite le iniziative di sostegno agli attivisti e i presidi di solidarietà, specie in concomitanza delle udienze dei procedimenti giudiziari.

Anche il movimento ***No TAV No Terzo Valico***, che si oppone alla costruzione della linea del "Valico dei Giovi", tra Liguria e Piemonte, ha fatto segnare una fase di ridimensionamento operativo, dovuta, fra l'altro, alla scarsa presa delle iniziative di mobilitazione sulla popolazione locale.

Una crescente attenzione ha suscitato il **progetto Alta Velocità/Alta Capacità Napoli-Bari**, opera attualmente in fase avanzata di costruzione nell'area del casertano e del napoletano, che si va profilando come un ambito suscettibile di sviluppi contestativi. Nella pubblicistica d'area viene sottolineato come l'infrastruttura arrecherà un danno irreversibile a un territorio già pericolosamente minacciato da altre nocività. Rilievi critici vengono inoltre mossi in chiave antimilitarista, potendo la linea rappresentare uno *snodo fondamentale dell'espansione della NATO verso i Balcani* e un'infrastruttura *utile allo spostamento di uomini e mezzi verso lo scenario di guerra mediorientale.*

Sono, inoltre, proseguite le campagne ***No TAP***, contro il gasdotto che dovrebbe portare il gas dell'Azerbaijan sulle coste pugliesi del Salento, ***No Grandi Navi***, che contesta il passaggio nella laguna veneta delle imbarcazioni da crociera e di quelle commerciali di grosso tonnellaggio, e ***No TRIV***, in opposizione alle perforazioni dei fondali marini e del sottosuolo per la ricerca di petrolio e gas, che, sorte come movimenti spontanei di cittadini, hanno rapidamente attirato l'attenzione di formazioni d'area.

Segnali di interesse solidale sono giunti anche nei riguardi della mobilitazione contro la riforma del mercato del lavoro in Francia, nelle cui piazze, secondo l'ottica antagonista, si sarebbe sviluppato l'*embrione* di una rivolta esemplare per la classe operaia italiana. A tal proposito, sono state rimarcate significative analogie con i contenuti del *Jobs Act* italiano, anch'esso stigmatizzato come un provvedimento dai contenuti *ingiusti* e *antioperai* imposto dalla UE.

Sul fronte occupazionale, le formazioni oltranziste, interessate a strumentalizzare vertenze e situazioni di tensione, hanno continuato ad incontrare difficoltà a proporsi come efficace alternativa ai sindacati tradizionali, fatta eccezione per gli ambiti lavorativi meno strutturati o connotati da una dimensione di estrema precarietà. Tra i settori più permeabili alle dinamiche contrappositive hanno continuato ad evidenziarsi quelli dei *call center* e delle cooperative operanti nel comparto della logistica, ove viene impiegata manodopera in prevalenza straniera. In tale ultimo settore

il blocco delle merci e la conseguente paralisi dell'attività sono stati ciclicamente "agitati" come il migliore strumento di lotta, da adoperarsi in maniera sistematica per *innescare il conflitto.*

La destra radicale in Italia e in Europa

Il quadro della destra radicale ha continuato ad evidenziare divisioni interne e dinamiche competitive, che hanno precluso una più incisiva azione comune, nonostante l'esistenza di alcuni condivisi orientamenti sulle tematiche di maggiore attualità.

Le formazioni più rappresentative, che ambiscono a un accreditamento elettorale, hanno incentrato l'attività propagandistica, rivolta soprattutto ai contesti giovanili e alle fasce sociali più disagiate, su argomenti di richiamo come la sicurezza nelle periferie degradate dei centri urbani, le problematiche economico-abitative "*degli italiani*" e l'occupazione, nonché la critica nei confronti del sistema bancario e dell'Unione Europea.

In particolare l'emergenza migratoria, ritenuta tra i temi più remunerativi in termini di visibilità e consensi, ha ricoperto un ruolo centrale nelle strategie politiche delle principali organizzazioni che, nel tentativo di cavalcare in modo strumentale il fenomeno, facendo leva sul malessere della popolazione maggiormente colpita dalla congiuntura economica e dalla contrazione del *welfare*, hanno sviluppato un'articolata campagna propagandistica e contestativa (manifestazioni, presidi, attacchinaggi, *flash mob*) contro migranti e strutture pubbliche e private destinate all'accoglienza, influenzando indirettamente anche la costituzione di "comitati cittadini" di protesta.

Benché lo scenario nazionale rimanga al momento distante da quello di altri Paesi europei – dove la più elevata presenza di militanti neonazisti ha conferito alla protesta accenti violentemente xenofobi, talvolta anche contro le locali comunità musulmane – sussiste il rischio di "contaminazioni", per effetto emulativo e sulla scia di eventi di particolare clamore, come nel caso di attentati terroristici di matrice islamica.

I principali attori della destra radicale hanno evidenziato inoltre una spiccata proiezione internazionale, in quanto interessati a individuare, ai fini della difesa delle radici etnico-culturali della Nazione, potenziali referenti e alleati in chiave anti-USA e anti-UE.

Indicative, nel senso, la realizzazione di manifestazioni congiunte con formazioni identitarie europee e il consolidamento dei contatti con omologhi gruppi stranieri, in funzione dello sviluppo di realtà transnazionali, attestate su posizioni filo-russe. Non è mancata l'attenzione degli ambienti d'area per il teatro mediorientale, segnatamente siriano, oggetto di iniziative a favore della popolazione locale e a sostegno del Presidente Assad.

L'**area *skinhead***, referente di circuiti internazionali neonazisti e xenofobi, dopo una fase di attivismo, soprattutto sui temi dell'anti-immigrazione, ha fatto registra-

re una flessione dell'impegno più prettamente politico. È rimasta quindi prioritaria l'organizzazione di eventi musicali d'area a carattere internazionale, cui partecipano attivisti italiani e stranieri, quale la kermesse *Europa Awake*, tenutasi a novembre in provincia di Milano. Gli *happening*, pur avendo uno scopo ludico e aggregativo, sono funzionali al consolidamento dei rapporti con omologhi gruppi esteri, alla raccolta di fondi a sostegno di militanti coinvolti in procedimenti giudiziari e alla diffusione – attraverso i testi delle canzoni – di una propaganda nazifascista e xenofoba. In Alto Adige intanto sono proseguiti i contatti tra locali realtà *skin* germanofone e analoghe formazioni tedesche attestate su posizioni neonaziste e razziste, che potrebbero, in prospettiva, sfociare in iniziative comuni in tema di contrasto all'immigrazione.

Sodalizi minori, dal canto loro, si sono impegnati in un'attività essenzialmente propagandistica che, connotata da orientamenti oltranzisti, non è parsa comunque in grado di aggregare significativi consensi.

Sul piano previsionale, si ritiene, infine, che continueranno a verificarsi **episodi di contrapposizione** (provocazioni, aggressioni e danneggiamenti di sedi) con frange dell'estrema sinistra, per effetto sia della mobilitazione concorrenziale su tematiche sociali, da parte di entrambi gli schieramenti, sia delle visioni contrapposte in tema di immigrazione.

In generale, il diffondersi in ambito europeo di istanze populiste e nazionaliste, nonché di sempre più estesi timori ed insofferenze verso la presenza extracomunitaria, tende ad essere percepito tra i gruppi della destra radicale come un'opportunità per accrescere il proprio spazio politico, determinando pertanto un incremento della correlata attività di mobilitazione.

SCENARI E TENDENZE: UNA SINTESI

PAGINA BIANCA

SCENARI E TENDENZE: UNA SINTESI

Il 2016 ha rappresentato un anno di rilevanti evoluzioni ed accelerazioni geopolitiche, economiche e nel settore della sicurezza, ponendo le premesse per un 2017 che si prospetta denso di opportunità ma anche di grandi sfide, complesse e tra loro interconnesse, con dinamiche passibili di alterare nel tempo, in modo anche significativo, lo scenario internazionale e interno che abbiamo conosciuto negli ultimi anni. La sempre maggiore presa di coscienza della portata di tali sfide e una accresciuta percezione da parte dei cittadini delle immediate ricadute di fenomeni esogeni e globali nella loro vita quotidiana, comporteranno per la Comunità intelligence un impegno crescente, e la ricerca di metodi e strumenti analitici ed operativi di sempre maggiore efficacia.

Il terrorismo internazionale jihadista, nelle sue variegate manifestazioni, continuerà ad avere centrale rilevanza. Una sconfitta militare di DAESH – che ha dato peraltro prova di feroce determinazione e efficace resistenza – non comporterà una rapida eliminazione dell'organizzazione ma una sua parziale mutazione, per perseguire con forme diverse i suoi obiettivi di destabilizzazione e dominio. Se privata dell'attuale territorialità o di gran parte di essa, l'organizzazione di al Baghdadi potrebbe da un lato accentuare ulteriormente la risposta asimmetrica, dall'altro assumere in modo crescente le modalità di radicamento che da tempo caratterizzano *al Qaida*, ancora attiva e vitale su molteplici scenari. Quest'ultima, in virtù delle difficoltà in cui versa la formazione concorrente, ha dato segnali di voler rilanciare la propria azione in una sorta di competizione con DAESH per la *leadership* sul *jihad* mondiale. Entrambe le organizzazioni continueranno a promuovere il proprio messaggio proselitista ed azioni impattanti, quali attentati su vasta scala da parte dei propri esponenti o attacchi di va-

ria natura ad opera dei cd. *lupi solitari* o di microcellule. Peraltro, se in alcuni scenari il terrorismo jihadista appare in affanno, esso continua ad espandersi e a rafforzarsi in modo preoccupante in altri quadranti, quali il Sud-Est asiatico, l'Afghanistan e l'Africa subsahariana e in quello limitrofo dei Balcani. Rileva inoltre come il jihadismo abbia tratto incoraggiamento e visibilità, e quindi accresciuto la possibilità di attivare in futuro seguaci e imitatori, dal fatto di avere intensificato con successo, nel 2016, i propri attacchi nel cuore stesso di molte Capitali, occidentali e mediorientali, ed esteso timore e apprensione nel quotidiano a crescenti porzioni della popolazione, la quale, legittimamente, richiede accresciute misure di tutela.

Le sempre più raffinate tecniche messe a punto dal terrorismo, come testimoniato ad esempio dall'affinamento delle modalità per promuovere tramite internet iniziative individuali, renderanno necessario un continuo perfezionamento delle modalità operative volte a prevenire e reprimere l'azione jihadista, nei vari settori del proselitismo, della propaganda, della promozione di azioni violente e nella dimensione di confronto aperto. Ciò comporterà anche un accresciuto ricorso alla collaborazione delle comunità straniere residenti nei vari Paesi ed interessate a dissociarsi e distanziarsi da fenomeni estremisti e violenti di cui sono anch'esse sovente vittime.

Tela di fondo della lotta al terrorismo sarà una sempre maggiore collaborazione internazionale anche nel settore intelligence, tendenza risalente già ulteriormente stressata nel 2016 e che dovrà necessariamente crescere negli anni a venire, arricchendosi di nuove modalità e strumentazioni.

Parallelamente, in linea con una visione condivisa nei più qualificati consessi multilaterali, anche a livello nazionale la strategia di prevenzione, con il concorso del Comparto informativo, dovrà sempre più articolarsi in misure funzionalmente interconnesse, quali: il dispiegamento di una controarrativa rivolta soprattutto ad un uditorio giovanile; l'attuazione di programmi di assistenza per soggetti esposti a rischio di radicalizzazione; la previsione di percorsi di de-radicalizzazione nei confronti di coloro che rientrano dai teatri di *jihad*.

Pure il fenomeno – che sta assumendo valenza strutturale – rappresentato dalle grandi migrazioni comporterà nel 2017 un crescente impegno di intelligence, anche per quanto attiene alla raccolta informativa necessaria per contrastare adeguatamente le organizzazioni criminali di trafficanti di esseri umani, e ciò in tutti i teatri in cui esse operano con sempre maggiore sistematicità ed efficacia in un'ottica di *learning by doing*, tanto più in considerazione di crescenti contaminazioni, soprattutto nel Sahel e nel Sud della Libia, tra *network* criminali e terrorismo. Con il crescere, nella criminalità transazionale, del livello di specializzazione, delle modalità di finanziamento, di trasporto e nei falsi documentali,

in un giro d'affari ormai dell'ordine di miliardi di Euro, l'impegno dei Servizi di Informazione sarà sempre più articolato e complesso, anche perché determina la necessità di proiettarsi ed operare anche in scenari nuovi ed inediti ove andranno stabilite sempre più strette collaborazioni intergovernative e anche azioni di formazione e prevenzione *in loco*.

L'attività di monitoraggio continuerà a vedere fortemente impegnate le Agenzie in relazione alle crisi geopolitiche che ci lambiscono e che sono passibili di avere nel nostro Paese dirette e indirette ricadute, anche in virtù della partecipazione dell'Italia a coalizioni internazionali e della nostra perdurante attiva presenza su numerosi scenari. Tutto il bacino del Mediterraneo – di cui siamo al centro – e l'area intera del Medio Oriente allargato continuerà ad essere sotto pressione per le varie crisi aperte, la cui soluzione si presenta complessa quanto complesso è lo scenario che vi fa da sfondo. Quella di più immediato impatto, che riguarda la Libia, richiederà crescente impegno stabilizzante che faccia prevalere l'interesse comune del Paese su divisioni, tribalismo e personalismi, fattori che permeano fortemente quella realtà; ma il radicamento di tali fenomeni – rafforzato dal recente conflitto interno – lascia intravedere anche per l'anno a venire una situazione precaria, passibile finanche di deteriorare. Non si intravedono, poi, le premesse per una riduzione – a breve – dell'incalzante azione offensiva del terrorismo all'interno del territorio egiziano o turco, condotta con consapevole volontà destabilizzante. Il conflitto in Siria ha portato il Paese allo stremo e ciò fa intravedere crescente stanchezza nella popolazione, ma l'eredità di odio e rancori accumulatasi (e la percezione di alcune componenti di combattere uno scontro esistenziale) renderà comunque difficili e lunghe una effettiva pacificazione sul terreno e la necessaria, costosa ricostruzione, stante anche la vitalità di cui DAESH continua a dar prova in quel quadrante. In Iraq la resistenza della formazione di al Baghdadi, pur in arretramento, resta rilevante mentre, sul più generale piano politico interno, permangono ostacoli alla realizzazione di quella coesione nazionale, infra ed inter-settaria, che sarebbe necessaria premessa per una normalizzazione della situazione. Lo Yemen vede una resistenza della componente Houti molto determinata ed un crescente attivismo di DAESH ed *al Qaida,* acuito nello scorso anno dalle difficoltà di controllo del territorio da parte delle Autorità; si prospetta pertanto una situazione anch'essa di non facile e vicina soluzione, pur nella prostrazione dei vari contendenti. Anche l'azione di *Boko Haram* in Nigeria e Africa centrale continua a produrre instabilità in numerose aree, mettendo seriamente in difficoltà i locali governi. Ad alimentare la percezione di incertezza, questa volta nel Continente europeo, concorre anche la cronicizzazione della crisi ucraina e la contestuale determinazione delle parti in causa a tutela dei rispettivi obiettivi di lungo periodo. Anche scenari più lontani, in un mondo ormai globalizzato, continueranno ad essere oggetto di attenzione in relazione

al fenomeno jihadista, come l'Afghanistan e l'Asia centrale, ricca di risorse, nonché il Sud-Est asiatico.

Per il 2017 si ravvisano anche le premesse per l'avvio di possibili cambiamenti, anche significativi, nel complessivo andamento del commercio internazionale e nei flussi di investimenti finanziari, in un contesto che potrebbe conoscere una acuita competizione tra attori statuali e tra imprese di vari Paesi, a volte spregiudicata e senza esclusione di colpi. Ciò richiederà, specie nel caso italiano dove la struttura produttiva fatta in prevalenza da piccole e medie imprese rende le stesse più vulnerabili, un accresciuto impegno per la nostra intelligence – a sostegno dell'azione del Governo e del Sistema Paese – in tre sensi. *In primis*, per una interpretazione delle tendenze macroeconomiche in evoluzione discernendo, nel contesto delle stesse, opportunità e minacce. In secondo luogo, per favorire e stimolare le dinamiche virtuose e confacenti ai nostri interessi, come – ad esempio – la promozione di investimenti produttivi che arricchiscano il territorio in termini di competenze e occupazione. In terzo luogo, per prevenire nella misura del possibile i danni derivanti da azioni perniciose ed ostili, come gli investimenti speculativi o miranti a indebolire il nostro sistema (tramite sottrazione di *know-how* tecnologico e industriale), oppure la diffusione di notizie fuorvianti, o da ogni altra iniziativa pregiudizievole. La crescita, in numerosi Paesi, di ampie fasce di disagio e bisogno ed il ridimensionamento di molti sistemi di *welfare* renderanno peraltro la competizione economica sempre più vitale anche tra Stati tradizionalmente allineati e membri degli stessi consessi internazionali. Anche la tutela degli *asset* nazionali di pubblico interesse ha assunto ulteriore valenza negli ultimi anni e si consoliderà nel tempo, in quanto la crescente circolazione di flussi finanziari rende più difficile distinguere tra investimenti strettamente finanziari ed azioni ostili come acquisizioni di controllo con finalità strategiche. Di assoluto rilievo per l'anno a venire è anche l'azione informativa a tutela del sistema bancario e finanziario. Andranno inoltre seguite con immutata attenzione le tematiche attinenti ai mercati internazionali dell'energia, fondamentali per la stabilità stessa del nostro Paese.

Sul piano più strettamente interno, inoltre, si ravvisa una persistente estensione dell'influenza della grande criminalità organizzata sul tessuto imprenditoriale, anche al fine di riciclare gli ingenti proventi derivanti da traffici illeciti, soprattutto di stupefacenti, influenza resa più perniciosa dalla accresciuta vulnerabilità di molti operatori a causa di un più selettivo accesso al credito e della tendenza delle organizzazioni di stampo mafioso a fomentare la corruzione. L'attività informativa su tale versante sarà dunque anche per l'anno a venire un impegno rilevante per il Comparto, specie se si tiene conto della improrogabile necessità di ricostruzione delle aree colpite da terremoti e della conseguente importanza di una vigilanza attenta e approfondita.

Anche l'Italia, come molti Paesi, continuerà nel 2017, nonostante l'avviata ripresa, a risentire delle conseguenze della lunga crisi iniziata nel 2008. È un clima economico che molte famiglie vivono con difficoltà e disagio, che potrebbe favorire l'insorgere di una maggiore conflittualità sociale a sua volta alimentata e strumentalizzata da parte di componenti antagoniste per riportare attenzione e attualità alle loro istanze, di cui potrebbe essere corollario una accresciuta mobilitazione di frange estremiste di opposto orientamento. Sono fenomeni da monitorare anche a fini preventivi nelle loro varie espressioni e manifestazioni, tenuto anche conto del fatto che l'Italia ospiterà numerosi eventi internazionali di rilievo, tra cui quelli legati alla Presidenza di turno del G7. Parallelamente, ristretti circuiti che si richiamano all'esperienza degli "anni di piombo" continuano a ricercare spunti teorici per attualizzare il messaggio rivoluzionario.

Un macrosettore che sta conoscendo un'importanza esponenzialmente crescente per le attività di intelligence – come più estesamente evidenziato nell'apposito annesso – è poi quello, in tumultuosa evoluzione, del *cyber*. L'opinione pubblica sta acquisendo crescente consapevolezza delle grandi opportunità derivanti dallo sviluppo tecnologico, ma anche delle crescenti sfide securitarie e delle minacce che esso determina. Il funzionamento delle moderne società è divenuto, mai come in passato, completamente dipendente dalla tecnologia senza che, in molti casi, si siano in parallelo sviluppate adeguate difese. Strutture di governo, banche, borsa, *asset* strategici e quant'altro sono oggi più che mai esposti. Viviamo una fase in cui attori statali ostili ma anche organizzazioni criminali, gruppi terroristi o antagonisti, fanatici di varia natura o anche singoli individui, beneficiano sovente nel *cyberspace* di un *gap* securitario che deve essere, in larga misura, rapidamente colmato, e che comunque sarà in futuro oggetto di una continua evoluzione, con forme di aggressione sempre più sofisticate. Il Comparto sarà pertanto chiamato a dare il suo fondamentale contributo accentuando ulteriormente la sua pianificazione strategica nel *cyberspace*, e le sue capacità operative a tutela non solo degli obiettivi istituzionali ma anche del mondo imprenditoriale, per cui, nel caso italiano – in un contesto di assenza di materie prime – il differenziale di *know-how* trasformativo è di vitale importanza per la stessa competitività internazionale, e quindi per la sopravvivenza del Paese.

Emerge, alla luce di quanto sopra, un quadro dinamico e complesso, denso di opportunità ma nel contempo di incognite e difficoltà che richiederà, anche nel 2017, alle donne e gli uomini dell'intelligence italiana uno straordinario impegno, l'adozione di conoscenze e metodi in continua ed incessante evoluzione ed un grande sforzo di integrazione con gli altri Organismi dello Stato, in un'azione sistemica a tutela della sicurezza che è per il cittadino bene primario e presupposto necessario e imprescindibile della libertà individuale.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

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

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

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

Premessa

In linea con l'approccio redazionale adottato per il 2015, anche quest'anno il Documento di Sicurezza Nazionale-DSN è stato sviluppato lungo due direttrici: quella relativa alle evoluzioni architetturali, dedicata al potenziamento delle capacità cibernetiche del nostro Paese; quella di natura fenomenologica, incentrata sulla minaccia *cyber* che ha interessato soggetti rilevanti sotto il profilo della sicurezza nazionale.

Il primo filone ha risentito di alcuni importanti "fattori di spinta" sia endogeni che esogeni al sistema-Paese. Tra i primi va annoverata l'esperienza maturata a partire dal 2013, anno di adozione del provvedimento che ha delineato l'architettura nazionale *cyber* dell'Italia, grazie alla quale è stata acquisita una maggiore conoscenza sia dei punti di forza e di debolezza del nostro sistema, sia della mutevolezza senza precedenti assunta dalla minaccia cibernetica. Tale accresciuta consapevolezza ha costituito il punto di partenza di una riflessione volta ad individuare soluzioni in grado di assicurare il costante adeguamento degli strumenti di risposta rispetto alla minaccia ed alla naturale evoluzione degli scenari.

A rendere effettiva tale riflessione ha contribuito, poi, lo stanziamento straordinario operato dal Governo nell'ambito della legge di stabilità 2016, volto a garantire un significativo incremento delle capacità cibernetiche del Paese e ad assicurare, attraverso lo sviluppo di progettualità di sistema, il potenziamento della sicurezza informatica nazionale.

Tra i fattori esogeni, il dato di rilievo è stato l'adozione, il 6 luglio 2016, della Direttiva UE 2016/1148, recante *"misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"* (c.d. Direttiva NIS - *Network and Information Systems*). L'approvazione di tale Direttiva – che dovrà essere recepita nell'ordinamento nazionale entro il maggio 2018 – ha rappresentato l'occasione per l'assunzione di più mirate azioni di manutenzione delle strutture poste a presidio dello spazio cibernetico, parte delle quali già previste dall'esercizio di revisione che ha interessato gli atti di indirizzo strategico (il Quadro Strategico Nazionale) ed operativo (il Piano Nazionale).

La seconda direttrice del presente Documento rimanda alle funzioni proprie dell'intelligence, strettamente correlate allo stato della minaccia cibernetica in Italia e alle sue possibili evoluzioni. In tale ambito, il Comparto ha continuato a sviluppare strumenti per rendere più efficace la prevenzione della minaccia. Quest'ultima, in particolare, è risultata caratterizzata da un elevato grado di eterogeneità e dinamismo tecnologico e da una diversificazione degli obiettivi, delle modalità attuative e delle finalità di attacco in base alle differenti matrici: si è passati da quelle più rilevanti in termini di rischi per gli *asset* critici e strategici nazionali a quelle connesse al *cybercrime,* al *cyber-espionage* ed alla *cyberwarfare,* il cui confine distintivo appare sempre più sfumato, sino a quella hacktivista e all'uso, da parte di gruppi terroristici, di risorse informatiche per finalità di proselitismo e propaganda.

In tale quadro, il Comparto ha incentrato l'attenzione sul monitoraggio e sulla ricerca di indicatori della minaccia, specie quella di natura avanzata e persistente, così da individuarne principali direttrici e paradigmi comportamentali.

Anche nel 2016 il Comparto ha continuato ad accrescere le proprie capacità di *detection, response* ed *attribution*, moltiplicando gli sforzi per far fronte ad una minaccia che ha continuato a far registrare una crescita non solo in termini quantitativi ma anche qualitativi, soprattutto nel caso delle minacce di tipo avanzato e persistente. Le difficoltà insite nella loro rilevazione e attribuzione continuano a rendere pagante il ricorso ad attività malevole nello spazio cibernetico.

Potenziamento delle capacità cibernetiche nazionali

In linea di continuità con gli esercizi avviati nel 2013, il DIS ha operato attraverso due strumenti: il TAVOLO TECNICO *CYBER*-TTC per garantire le attività di raccordo inter-istituzionale; il TAVOLO TECNICO IMPRESE-TTI per rafforzare il Partenariato Pubblico-Privato (PPP).

Il 2016 ha costituito per il TTC un significativo punto di svolta. Gli esiti della verifica dell'attuazione del Piano Nazionale riferito al 2014-2015 – che hanno consentito di rilevare il livello di crescita degli assetti *cyber* nazionali e la loro capacità di rispondere alle sfide/opportunità offerte dallo spazio cibernetico – sono stati il punto di partenza del processo di revisione dello nuovo Piano, valido per il 2016-2018.

Tale processo ha interessato, oltre al Piano Nazionale, anche il Quadro Strategico, al fine di verificarne l'attualità e di procedere al loro

MEMBRI DEL TTC

1. Ministero degli Affari Esteri e della Cooperazione Internazionale;
2. Ministero dell'Interno;
3. Ministero della Giustizia;
4. Ministero della Difesa;
5. Ministero dell'Economia e delle Finanze;
6. Ministero dello Sviluppo Economico;
7. Agenzia per l'Italia Digitale;
8. Nucleo per la Sicurezza Cibernetica;
9. Comparto intelligence.

aggiornamento in ragione del mutato scenario di riferimento, specie avuto riguardo alla richiamata Direttiva UE in materia di sicurezza di *Network and Information Systems* (NIS). L'obiettivo più significativo di tale revisione è stato quello di pervenire alla definizione di strumenti per rendere più efficace l'attuazione degli indirizzi strategici e operativi fissati nei predetti documenti e più misurabili le azioni progettuali che da essi scaturiscono.

Sotto il profilo del metodo, la revisione è stata posta in essere secondo un articolato e ben definito processo di lavoro (vds. *Figura 1*) che, grazie allo sviluppo di una dinamica sinergica in sede di TTC, non si è limitato ad operare un mero aggiornamento dei richiamati documenti, ma ha preso in considerazione differenti piani – giuridico-normativo, organizzativo e finanziario – attraverso cui sviluppare l'azione di potenziamento delle capacità cibernetiche del Paese.

Le direttrici che hanno inciso sul processo di revisione hanno riguardato lo sviluppo delle capacità di prevenzione e reazione ad eventi cibernetici, ambito nel quale si sono evidenziate nel biennio concluso le più rilevanti criticità, e l'indispensabile coinvolgimento del

Figura 1 –Revisione del Quadro Strategico Nazionale e del Piano Nazionale 2016-2018

settore privato ai fini della protezione delle infrastrutture critiche/strategiche nazionali e dell'erogazione di servizi essenziali. Aspetti, questi, sui quali si focalizza con rinnovata attenzione la citata Direttiva NIS. Per un approfondimento sulle novità introdotte dalla stessa, si veda la scheda nel *box 1*.

Gli esiti dell'esercizio di verifica hanno costituito un utile parametro di riferimento anche per l'enucleazione delle attività poste in essere dall'Italia ai fini dell'attuazione del primo e del secondo pacchetto delle misure OSCE (*Organization for Security and Co-operation in Europe*), le cd.

box 1

NOVITÀ INTRODOTTE DALLA DIRETTIVA NIS

La Direttiva NIS prevede:

- sul piano strategico: l'adozione di una strategia nazionale NIS, che contempli la fissazione di obiettivi e priorità, delinei l'architettura di governo (comprensiva di ruoli e responsabilità attribuite ai diversi soggetti), preveda programmi di sensibilizzazione (*awareness*), piani di ricerca e sviluppo, nonché renda operativo un piano di valutazione dei rischi;
- sul versante architetturale e operativo:
- l'istituzione di una (o più) Autorità nazionale NIS e di un punto unico di contatto nazionale per la ricezione delle notifiche di incidenti e la cooperazione alla loro risoluzione;
- la costituzione di uno o più *Computer Security Incident Response Teams* (CSIRTs), cui è – tra l'altro – attribuita la responsabilità della gestione degli incidenti e dei rischi, con specifico riferimento a quelli che dovessero interessare gli operatori di servizi essenziali, dovendo fornire loro supporto per la risoluzione degli incidenti di impatto significativo;
- specifici obblighi di sicurezza informatica per:
  - gli operatori di servizi essenziali (nei settori dell'energia, del trasporto, bancario e finanziario, sanitario, idrico e delle infrastrutture digitali);
  - i fornitori di servizi digitali (come i motori di ricerca *on-line*, i negozi *on-line*, i servizi di *cloud computing*),

  tra cui l'obbligo della tempestiva notifica all'Autorità nazionale NIS degli incidenti informatici subiti.

"Confidence Building Measures (CBMs) *to reduce the risks of conflict stemming from the use of information and communication technologies*", adottate dal Consiglio permanente di quella organizzazione mediante le Decisioni del 3 dicembre 2013 e del 10 marzo 2016.

Il TTC ha seguito anche gli sviluppi maturati sulla materia *cyber* in sede di Alleanza Atlantica. Sono stati oggetto di particolare attenzione il riconoscimento, nel corso del summit NATO tenutosi a Varsavia dall'8 al 9 luglio 2016, del *cyber*-spazio quale nuovo dominio operativo e della necessità che in esso la NATO debba *"defend itself as effectively as it does in the air, on land, and at sea"*. A dare concretezza a tale passaggio hanno contribuito, da una parte, gli Alleati con l'impegno a rafforzare, attraverso il "*Cyber Defence Pledge*", le rispettive difese cibernetiche e, dall'altro, l'adozione di un meccanismo di misurazione dell'attuazione di tali obiettivi da parte dell'Alleanza.

Il Tavolo Tecnico *Cyber*, inoltre, quale tavolo di raccordo inter-istituzionale, ha contribuito allo sviluppo dei lavori e delle azioni concertate di sicurezza cibernetica proposte nell'ambito dei *Cyber Expert Group Meeting* del G7 Finanza ed Energia, anche in vista della prossima presidenza italiana del "Gruppo dei sette".

Vale poi evidenziare le interlocuzioni tenute dal Comparto con Banca d'Italia sul fronte della costituzione di un CERT Finanziario che – istituito nel dicembre 2016 in seguito ad un accordo tra Banca d'Italia, Associazione Bancaria Italiana (ABI) e Consorzio ABI Lab – opera quale organismo altamente specializzato nella *cybersecurity* nel settore bancario e finanziario, con l'obiettivo di prevenire e contrastare le minacce informatiche legate allo sviluppo delle nuove tecnologie e dell'economia digitale. Sempre con riguardo all'Istituto centrale, l'intelligence ha collaborato nella predisposizione di un elaborato incentrato sulla sicurezza *cyber* delle imprese italiane, allo scopo di ottenere, per la prima volta in Italia, un quadro statisticamente rilevante dell'esposizione alla minaccia cibernetica del sistema produttivo.

Sul fronte della *partnership* pubblico-privato (PPP) come accennato, opera il TTI che, istituito nell'ambito del DIS, fonda la sua azione sulla

condivisione informativa, così da consentire alle infrastrutture critiche ed alle imprese strategiche convenzionate con il Dipartimento di arricchire le loro conoscenze e rafforzare le proprie capacità di difesa cibernetica.

Il formato di collaborazione con gli operatori privati in sede di TTI ha continuato ad essere articolato su incontri di livello strategico, nel cui ambito vengono forniti aggiornati quadri sullo stato della minaccia *cyber* nel nostro Paese, e di livello tecnico, dedicati all'analisi di "casi studio", dei quali vengono condivisi i relativi indicatori di compromissione. Ciò per agevolare, da un lato, il rafforzamento delle misure di difesa cibernetica e consentire, dall'altro, in caso di presenza della minaccia, la sua rapida identificazione al fine di impedirne l'ulteriore propagazione.

In via più generale, lo scambio informativo tra intelligence e privati è assicurato da una piattaforma dedicata, il cui principale obiettivo è quello di porsi sempre più quale *"one-stop-shop"* per la fornitura di servizi informativi e di correlazione dati a supporto delle decisioni di sicurezza cibernetica che le aziende sono chiamate ad assumere.

Tra gli eventi internazionali che hanno coinvolto, su iniziativa dell'intelligence, gli operatori privati, oltre al *17th NATO Cyber Defence Workshop* di cui si è accennato nella premessa alla presente Relazione, va menzionato l'incontro relativo alla *"contractual Private-Public Partnership"* (cPPP) che, come parte integrante della strategia UE sul *Digital Single Market* per la *cyber security*, mira ad accrescere la competitività delle aziende attive nello specifico settore per favorire la produzione, in ambito europeo, di tecnologie affidabili sotto il profilo della sicurezza ed agevolarne altresì l'esportazione.

In ambito nazionale, poi, di rilievo è stata la terza edizione dell'ICT4INTEL 2020 dedicata al tema dei *Big Data* (BD), declinato, tenuto conto delle esigenze dell'intelligence, sulla base degli aspetti indicati in *Figura 2*.

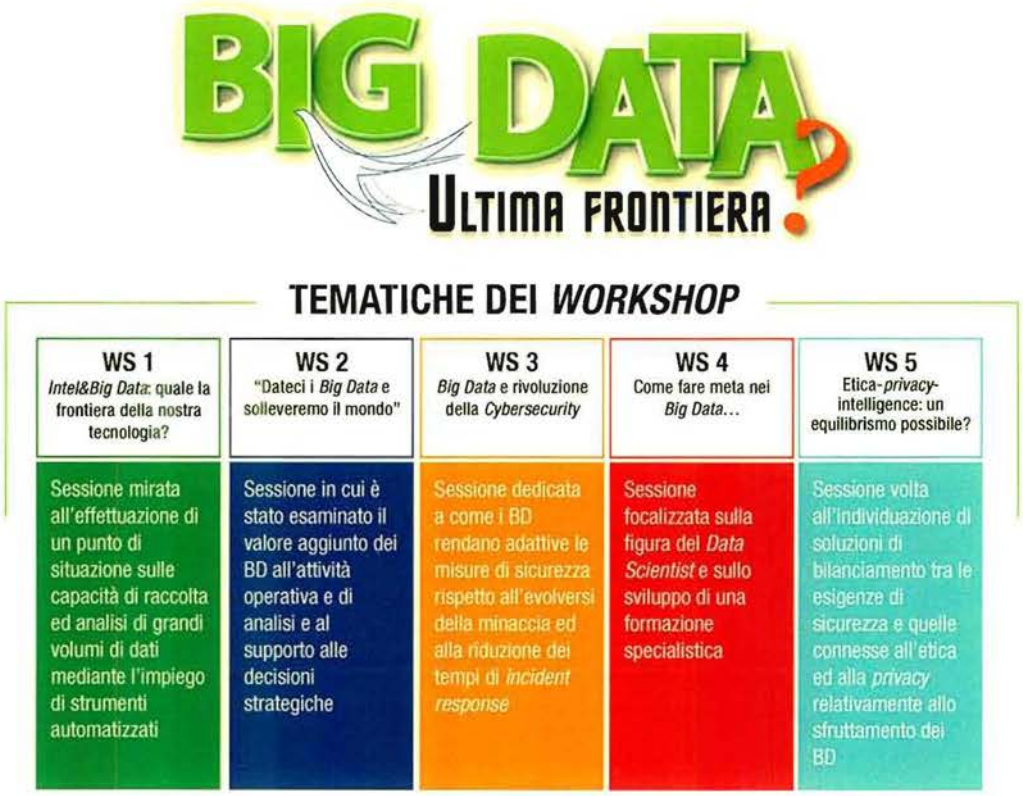
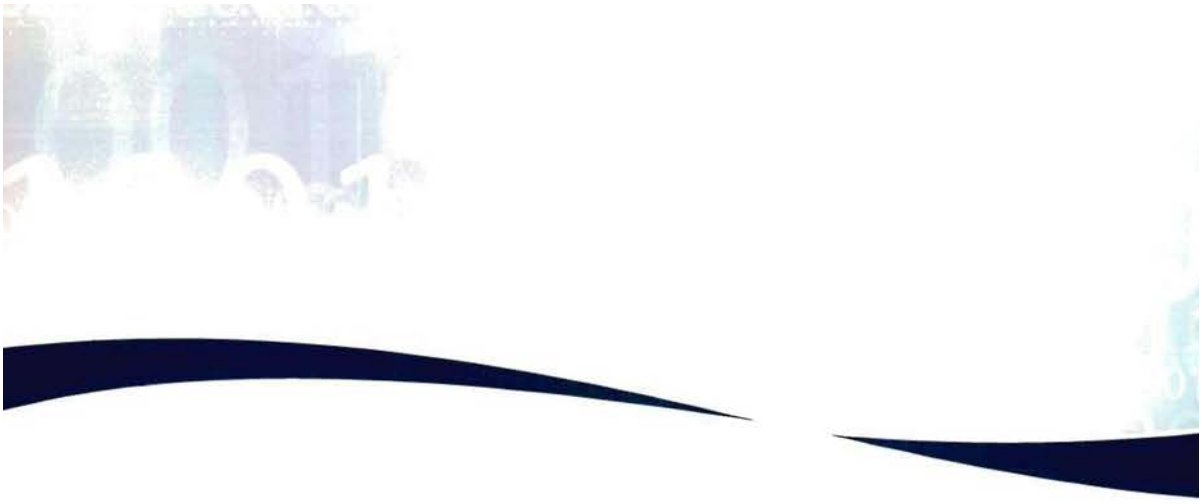


Figura 2 – Tematiche trattate in occasione dell'evento ICT 4INTEL 2020 edizione 2016



Stato della minaccia cibernetica in Italia e possibili evoluzioni

UNO SGUARDO AL CONTESTO INTERNAZIONALE

Gli attacchi *cyber* verificatisi nel corso del 2016 hanno innovato significativamente il panorama della minaccia, segnando un ulteriore cambio di passo sotto molteplici profili: dal rango dei *target* colpiti, alla sensibilità rivestita dagli stessi nei rispettivi contesti di riferimento; dal forte impatto conseguito, alle gravi vulnerabilità sfruttate sino alla sempre più elevata sofisticazione delle capacità degli attaccanti.

Il riferimento è, in ordine di tempo, agli eventi che hanno interessato, secondo quanto riportato dalle più accreditate fonti aperte internazionali, le istituzioni bancarie di diversi Paesi (Bangladesh, Ecuador, Vietnam e

> AZIONI DI *CYBER* SABOTAGGIO IN DANNO DI INFRASTRUTTURE CRITICHE: UN CASO-STUDIO
>
> Nel dicembre 2015 si è verificata una serie di attacchi cyber condotti contro i sistemi di controllo industriale di tre compagnie di distribuzione elettrica dell'Ucraina (Oblenergo), che hanno causato un *blackout*, protrattosi per diverse ore. Nell'attacco è stato impiegato il *malware BlackEnergy*, rinvenuto nel gennaio 2016, come ampiamente riportato da fonti aperte, anche nelle reti informatiche dell'aeroporto Kiev-Boryspil, della compagnia di bandiera Ukraine International Airlines, di una società di trasporto ferroviario e di una compagnia mineraria ucraine.
>
> Un nuovo *blackout* si è recentemente verificato nel dicembre 2016, interessando sempre l'Ucraina e, in particolare, la capitale Kiev.

Ucraina), provocando trasferimenti illeciti di grandi somme di denaro a causa della penetrazione dei sistemi per la gestione delle transazioni interbancarie ovvero della compromissione dei dispositivi ATM (è il caso di Taiwan). Il dato più preoccupante di tali attacchi è stato ricondotto, dai citati media, all'inedito collegamento tra ambienti *cyber* criminali, sodalizi dediti al riciclaggio ed *insider* nei circuiti finanziari (inclusi i *money transfer*). Alla citata casistica sono stati, poi, aggiunti gli eventi di sabotaggio dei sistemi di controllo industriale impiegati nell'ambito di infrastrutture critiche e quelli ricondotti ad attori supportati da entità statuali, che hanno comportato la sottrazione di informazioni rilevanti sotto il profilo strategico o coperte da proprietà intellettuale, ovvero utili, se opportunamente manipolate, per influenzare le dinamiche politiche di Paesi terzi.

AMBITI E ATTORI DELLA MINACCIA

La minaccia nei confronti delle infrastrutture del dominio cibernetico nazionale è stata caratterizzata da un elevato grado di eterogeneità e dinamismo tecnologico. In linea di continuità con il 2015 e con prevedibile estensione per gli anni a venire, anche nel 2016 il monitoraggio dei fenomeni di minaccia collegati con il *cyberspace* ha evidenziato un costante *trend* di crescita in termini di sofisticazione, pervasività e persistenza a fronte di un livello non sempre adeguato di consapevolezza in merito ai rischi e di potenziamento dei presidi di sicurezza.

Una tendenza, questa, cui si è associata anche la persistente vulnerabilità di piattaforme *web* istituzionali e private, erogatrici in qualche caso di servizi essenziali e/o strategici, che incidono sulla sicurezza nazionale, e la presenza di un sostanziale sbilanciamento del rischio, generalmente contenuto, in capo agli attori della minaccia rispetto a quello dei *target*, derivante dalle perduranti difficoltà di *detection, response* ed *attribution* di un evento.

La crescente dipendenza dei processi produttivi e delle forniture di servizi dal dominio digitale, unitamente alle vulnerabilità che affliggono le *supply chain* degli operatori, siano essi imprese, organizzazioni

ed individui, hanno nel tempo determinato una progressiva estensione della superficie di esposizione alla minaccia.

In tale contesto, il connubio tra un livello di rischio contenuto ed un'elevata redditività dei patrimoni digitali *target* ha contribuito a rafforzare le dinamiche di un insieme di attori operanti nel dominio *cyber*, sempre più collegati, tra l'altro, con filiere e sodalizi criminali tradizionali.

Giova inoltre evidenziare come gli incentivi all'innovazione tecnologica delle istituzioni civili e militari hanno costituito un ambito particolarmente appetibile, catalizzando gli interessi di attori privati, anche stranieri, presenti sul territorio nazionale che hanno cercato di accreditarsi, fra l'altro, attraverso condotte poco ortodosse.

Tenuto conto di quanto sopra, l'azione di tutela e prevenzione si è focalizzata sulla raccolta di informazioni utili alla profilazione degli attori ostili in termini di interessi, obiettivi, capacità e modalità di attacco, al fine di ottimizzare la difesa degli Enti della Pubblica Amministrazione, delle infrastrutture critiche, governative e non, degli operatori privati strategicamente rilevanti e, più in generale, delle reti telematiche nazionali esposte a tali minacce.

Attenzione è stata posta all'individuazione e al monitoraggio delle tecnologie caratterizzanti il dominio cibernetico (*social network*, motori di ricerca, piattaforme di *e-commerce*, *dark net* e sistemi di anonimizzazione) e del panorama tecnologico nazionale e internazionale, che hanno evidenziato un crescente sviluppo di armi digitali e di tecnologie potenzialmente ostili, parte delle quali hanno costituito oggetto di analisi e di *reverse engineering* presso il Polo Tecnologico di Comparto, che opera quale centro di eccellenza nazionale in materia.

Per quel che concerne lo stato della minaccia cibernetica, si è continuato a rilevare una diversificazione dei *target*, delle modalità attuative e delle finalità degli attacchi in base alla matrice della minaccia: da quelle più rilevanti per gli *asset* critici e strategici connesse al *cybercrime*, al *cyber-espionage* ed alla *cyberwarfare*, a quella terroristica ed hacktivista, più stabili nella condotta e negli obiettivi. La minaccia terroristica nell'ambiente digitale permane caratterizzata dalle finalità di proselitismo, re-

clutamento e finanziamento, mentre le attività ostili in danno di infrastrutture IT sono consistite principalmente in attività di *Web-defacement.*

Per quanto riguarda il *cyber-espionage,* è stato pressoché costante l'andamento dei "*data breach*" in danno di Istituzioni pubbliche ed imprese private, incluse le PMI, con finalità di acquisizione di *know-how* ed informazioni di *business* e/o strategiche, anche attraverso manovre di carattere persistente (*Advanced Persistent Threat – APT, vds. Glossario*). Tali manovre sono apparse riconducibili, in via diretta o indiretta, a matrici di natura statuale, rilevandosi in alcuni casi una sovrapposizione, ai danni del medesimo *target,* di campagne promosse da vari attori che, seppure in modo indipendente, hanno sfruttato con tecniche diverse le vulnerabilità dei sistemi informatici attinti.

Il quadro delineato dall'analisi dei dati sulle campagne digitali condotte contro le infrastrutture strategiche nazionali ha evidenziato la presenza di elementi ricorrenti in termini di origine delle minacce e di infrastrutture informatiche utilizzate per sferrare gli attacchi digitali.

Con riguardo a queste ultime, è stato rilevato il ricorso sempre più strutturato a *server* rinvenibili nel mercato nero digitale come ordinari prodotti di *e-commerce,* previamente compromessi dall'offerente mediante *trojan* (*vds. Glossario*) così da garantire all'attaccante l'accesso ad un prodotto utilizzabile per la conduzione di attacchi, preservando l'anonimato. Si tratta, questo, di un fenomeno che, fondato sul paradigma *"APT as a Service"*, ha visto il crescente coinvolgimento di gruppi criminali organizzati, specializzatisi nella conduzione di sofisticate attività delinquenziali con finalità estorsive, attuate perlopiù attraverso campagne *ransomware.*

È stata confermata, inoltre, la progressiva saldatura tra le finalità economiche della *cyber*-criminalità con quelle di comuni *player* di mercato, interessati, questi ultimi, a compromettere la competitività dei rispettivi concorrenti. Tale obiettivo è stato sempre più conseguito mediante la realizzazione di un rilevante danno reputazionale in capo al *target,* specie nel caso di organizzazioni per le quali tale aspetto

è correlato alla capacità di garantire la sicurezza, anche informatica, della struttura e dei dati da essa custoditi. È il caso, ad esempio, delle banche, degli istituti finanziari, dei gestori di piattaforme *cloud*, degli operatori nei settori *e-commerce* ed *e-business*, nonché delle infrastrutture critiche nazionali, la cui *supply chain* è tipicamente soggetta a minori presidi difensivi.

La compromissione delle risorse telematiche si è configurata come un'attività strutturata dell'attore ostile finalizzata, sul **piano strategico**, alla raccolta di informazioni tese a comprendere il posizionamento del Paese *target* su eventi geo-politici di interesse per l'attore statuale ostile (laddove obiettivo dell'attacco *cyber* sia un soggetto pubblico), ovvero ad acquisire informazioni industriali, commerciali o relative al *know-how* (qualora si tratti, invece, di un obiettivo privato). Sul **piano tattico**, l'attaccante è parso interessato a minare la reputazione ed il vantaggio commerciale, sul mercato, dei *target* privati ed a profilare il personale dei *target* pubblici, di cui sono state studiate anche le abitudini digitali alla ricerca di eventuali punti di debolezza sistemica, da sfruttare in vista di un possibile reclutamento convenzionale. In relazione al *modus operandi* impiegato dall'attaccante per il conseguimento dei citati obiettivi, si sono registrati, quali elementi di novità, il ricorso a parole-chiave in lingua italiana per ricercare documenti di interesse da esfiltrare, ad ulteriore conferma dell'elevato grado di profilazione delle attività ostili sui *target* nazionali, e la ricerca di singoli individui ritenuti di particolare interesse in ragione dell'attività professionale svolta, ovvero sulla base dell'incarico e della sede di servizio ricoperti, nonché delle informazioni cui hanno accesso.

Sul fronte del *cyber* terrorismo, si è continuato a rilevare sui *social network*, da parte di gruppi estremisti, attività di comunicazione, proselitismo, radicalizzazione, addestramento, finanziamento e rivendicazione delle azioni ostili. La rete consente infatti di raggiungere sia potenziali nuove reclute presenti nelle sacche di emarginazione sociale, sia esponenti degli ambienti ideologicamente distanti dalle rappresentanze moderate. Sul piano delle capacità *cyber* ostili, è risultato particolarmente

attivo il *Tunisian Fallaga Team* – operativo dal 2013 e noto anche come "*Hacker del Califfato*" – che, sebbene nel 2015 abbia subìto un duro colpo ad opera delle Forze di sicurezza tunisine, negli ultimi mesi del 2016 ha dato mostra di un rinnovato slancio delle proprie azioni digitali eseguite, di massima, con finalità di *defacement* ai danni di siti *web* di enti, aziende e privati cittadini. L'azione digitale di tale gruppo si è caratterizzata, al pari di omologhe formazioni, da un basso livello di sofisticazione delle procedure e degli strumenti d'attacco, dall'individuazione randomica dei *target* (perlopiù cd. *soft target*) e dalla numerosità delle attività *cyber* ostili.

Per quel che concerne le campagne di attivismo digitale, riconducibili soprattutto alla comunità *Anonymous Italia*, esse hanno fatto registrare una generale diminuzione del livello tecnologico delle azioni offensive. Flessione, questa, ascrivibile alla riorganizzazione interna del gruppo successiva allo scompaginamento dei suoi assetti organizzativi posto in essere dalle Forze di polizia. Al di là di ciò, le azioni di *cyber* attivismo hanno continuato a connotarsi per la loro impronta antagonista e antigovernativa – come nella campagna di dissenso alla consultazione referendaria sulla riforma costituzionale – e per la scelta di *target* perlopiù istituzionali, i cui sistemi sono stati oggetto di preliminari operazioni di scansione per la ricerca di vulnerabilità da sfruttare in vista di operazioni di *web defacement* e di esfiltrazione dati. Tale *modus operandi* si è configurato, seppure in minor misura rispetto al passato, come una sorta di "pesca a strascico", nella quale vengono attaccati anche *asset* informatici esposti su internet di obiettivi non direttamente connessi con i motivi della rivendicazione, tra i quali sono emersi quelli di enti locali, sovente affetti da vulnerabilità di agevole sfruttamento.

Elemento di rilievo in tale contesto è stato il riavvicinamento del movimento hacktivista ai temi chiave, non solo della politica italiana, ma anche delle istanze di piazza, come nel caso dell'operazione NoMUOS (*Mobile User Objective System*), oggetto di rilancio contro l'installazione, sul territorio nazionale, di un moderno sistema di telecomunicazione satellitare USA.

SERIE STATISTICHE

Allo scopo di consentire l'immediata ed agevole rilevazione del volume degli eventi *cyber* registrati nel nostro Paese nel corso del 2016, sono state realizzate, anche per questa edizione, le serie statistiche relative agli attacchi, andati a buon fine o tentati, compiuti in danno di obiettivi insistenti sul territorio nazionale, ovvero contro soggetti nazionali, pubblici e privati, presenti con proprie strutture all'estero. L'analisi è stata condotta sulla base degli elementi informativi di AISE ed AISI, degli altri soggetti che compongono l'architettura nazionale e dei Servizi Collegati Esteri.

I valori sono espressi esclusivamente in termini percentuali e non assoluti, così da preservare le inderogabili esigenze di riservatezza circa l'entità numerica delle minacce rilevate.

La serie è corredata, come di consueto, dall'indicazione del *trend*, ricavato dalla comparazione dei dati del 2016 con quelli dell'anno precedente, tracciato, secondo la seguente legenda, in corrispondenza della relativa voce nel grafico.

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

Per quel che concerne la tipologia di **attori ostili** (***Grafico 1***), i **gruppi hacktivisti** (52% delle minacce *cyber*) continuano a costituire la minaccia più rilevante, in termini percentuali, benché la valenza del suo impatto sia inversamente proporzionale, rispetto al livello quantitativo riferito ai **gruppi di *cyber-espionage***, più pericolosi anche se percentualmente meno rappresentativi (19%). Ai **gruppi islamisti** è imputato il 6% degli attacchi *cyber* perpetrati in Italia nel corso del 2016. Da evidenziare come per le tre categorie si sia registrato, rispetto al 2015, un incremento degli attacchi pari al 5% per i gruppi hacktivisti e quelli islamisti e del 2% per quelli di *cyber-espionage*, così come evidenziato nel paragrafo dedicato agli "Ambiti e attori della minaccia". A tale aumento ha corrisposto un decremento, pari al 12%, dei cd. **"attori non meglio identificati"** che si attestano nel complesso al 23% delle incursioni *cyber*.

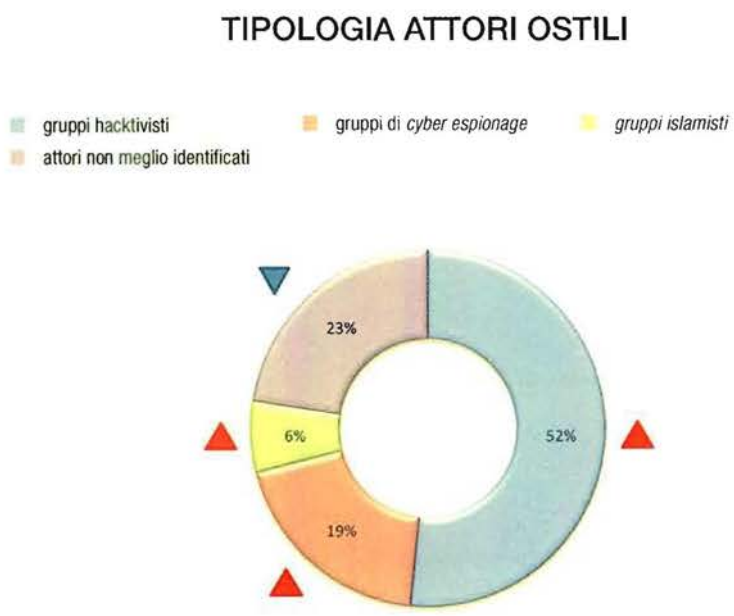


Grafico 1 – Attacchi cyber in Italia in base alla tipologia degli attori ostili (in % sul totale 2016)

Quanto ai dati sugli attacchi *cyber* in base ai **soggetti *target*** (***Grafico 2***) persiste il notevole divario tra le minacce contro i **soggetti pubblici**, che costituiscono la maggioranza con il 71% degli attacchi, e quelli in direzione di **soggetti privati**, che si attestano attorno al 27%, divaricazione, questa, riconducibile verosimilmente alle difficoltà di notifica degli attacchi subiti in ragione del richiamato rischio reputazionale. In entrambi i casi si registra un aumento pari, rispettivamente, al 2% ed al 4%. Un decremento del 6% è stato viceversa osservato nell'ambito dei ***target* non meglio identificati o diffusi** (che costituiscono, complessivamente, il 2%), solitamente oggetto di campagne hacktiviste. Tale dato è esplicativo del fatto che anche queste sono sempre più mirate, privilegiando *target* paganti sotto il profilo simbolico e della relativa rilevanza mediatica rispetto ai cd. *"soft target"*, ossia obiettivi di minore rilievo strategico, accomunati dalla ricorrenza di vulnerabilità comuni e di agevole sfruttamento.

Grafico 2 – Attacchi cyber in Italia in base alla tipologia dei soggetti target (in % sul totale 2016)

Il dettaglio dei dati relativi ai *target* per categoria pubblico/privato consente di rilevare, con riferimento ai **soggetti pubblici** (***Grafico 3***), che pur permanendo una netta predominanza delle Amministrazioni centrali (87% degli attacchi *cyber* verso soggetti pubblici) – dato che ricomprende anche le attività ostili verso movimenti politici – rispetto agli Enti locali (13%), nel 2016 si è assistito ad una inversione di tale *trend*. Gli attacchi contro le Pubbliche Amministrazioni Centrali (PAC) risultano, infatti, in lieve diminuzione (-2%) mentre quelli avverso le Pubbliche Amministrazioni Locali (PAL) sono in aumento (+5%). Vale rammentare come le PAC costituiscano obiettivo privilegiato per azioni di *cyber*-spionaggio, essendo detentrici di informazioni pregiate se non addirittura sensibili, e le PAL siano perlopiù oggetto di campagne di attivismo digitale ovvero condotte per finalità dimostrative da parte di gruppi islamisti.

Rispetto al 2015, non sono stati segnalati eventi cibernetici di particolare rilevanza in danno di organizzazioni internazionali insistenti sul territorio italiano.

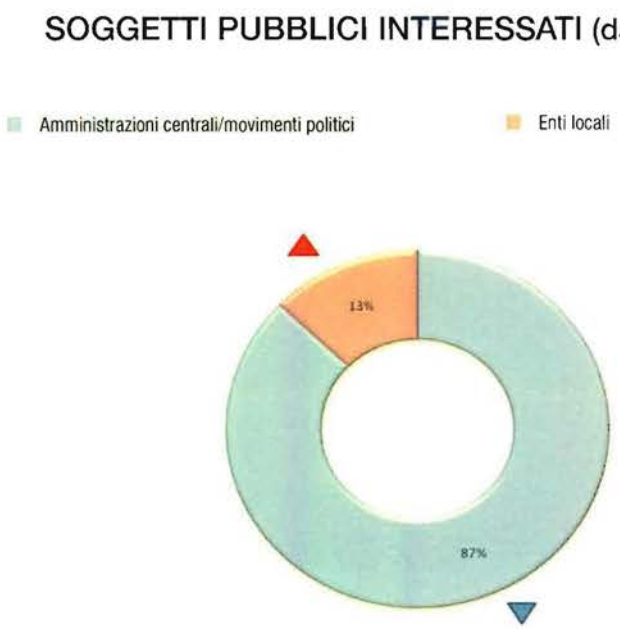


Grafico 3 – Attacchi cyber in Italia in base alla tipologia dei soggetti pubblici target (in % sul totale 2016, dati aggregati)

In relazione ai ***target* privati** (***Grafico 4***), sono emersi elementi di novità. Se nel 2015 *target* principali degli attacchi *cyber* risultavano quelli operanti nei settori della difesa, delle telecomunicazioni, dell'aerospazio e dell'energia, nel 2016 figurano ai primi posti il settore bancario con il 17% delle minacce a soggetti privati (+14% rispetto al 2015), le Agenzie di stampa e le testate giornalistiche che, insieme alle associazioni industriali, si attestano sull'11%. Queste ultime costituiscono una *"new entry"*, insieme al settore farmaceutico che, con il suo 5% degli attacchi verso *target* privati, si posiziona al fianco di settori "tradizionali" come quelli della difesa, dell'aerospazio e dell'energia. Tra questi ultimi, solo quello energetico ha fatto registrare un aumento, pari al 2%, rispetto all'anno precedente, mentre quelli di difesa e dell'aerospazio hanno fatto segnare un decremento, rispettivamente, del 13% e del 7%.

Sotto la voce "altri settori" (41%) sono state ricomprese aziende diversificate che non assumono, qualora singolarmente considerate, rilevanza sotto il profilo strategico.

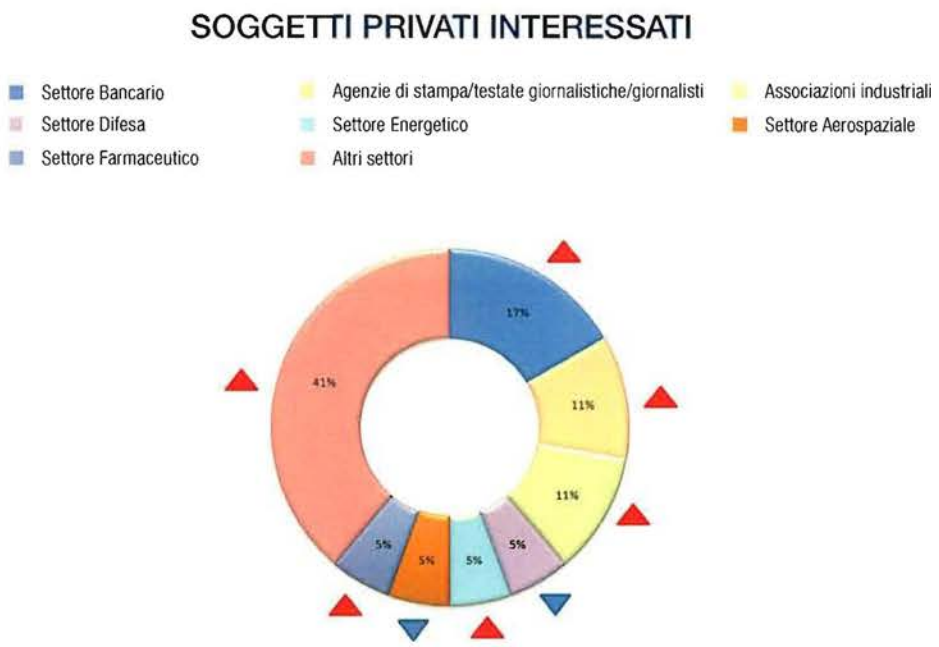


Grafico 4 – Attacchi cyber in Italia in base alla tipologia dei soggetti privati target (in % sul totale 2016)

Con riguardo, infine, alle **tipologie di attacco** (***Grafico 5***), rispetto al 2015, nel 2016 si è registrata un'inversione di tendenza. Se, infatti, nel 2015, poco più della metà delle minacce *cyber* era costituita dalla diffusione di *software* malevolo (*malware, vds. Glossario*), nel 2016 è stata registrata una maggiore presenza di altre tipologie di attività ostili, che ha comportato una contrazione (-42%) del dato relativo ai *malware*, attestatosi intorno all'11%. Tale dato non va letto come una riduzione della pericolosità della minaccia *Advanced Persistent Threat* (APT), bensì come il fatto che gli APT registrati si sono caratterizzati, più che per la consistenza numerica, per la loro estrema persistenza.

Tra le minacce che hanno registrato un maggior numero di ricorrenze vanno annoverate:

l'*SQL Injection* (28% del totale; +8% rispetto al 2015, *vds. Glossario*), i *Distributed Denial of Service* (19%; +14%), i *Web-defacement* (13%; -1%) ed il *DNS poisoning* (2%, *vds. Glossario*), impiegati sia dai gruppi hacktivisti che islamisti.

Le attività prodromiche ad un attacco (23% degli attacchi *cyber*) hanno fatto registrare un aumento del 18% rispetto all'anno precedente. Gli attacchi *cyber* non andati a buon fine e, quindi, "tentati", rimangono sostanzialmente stabili con il 4% (+1% se confrontato col dato 2015).

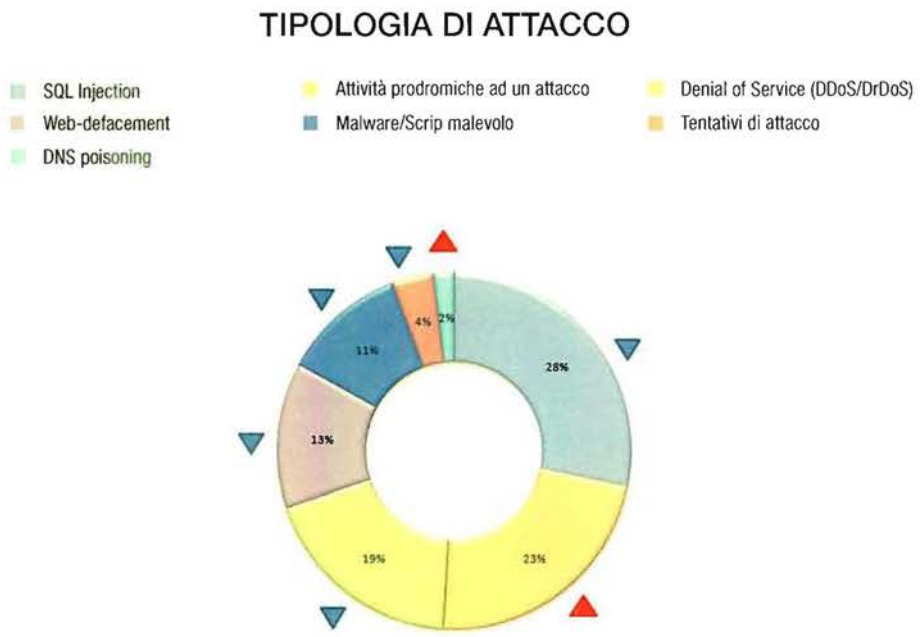


Grafico 5 – Attacchi cyber in Italia in base alla tipologia di attacco impiegata (in % sul totale 2016)

TREND EVOLUTIVI DELLA MINACCIA CIBERNETICA

In prospettiva, alla luce degli elementi considerati e del *trend* in atto, è verosimile nel breve-medio termine, in linea di continuità con il passato, una crescita della minaccia cibernetica ad opera di attori statuali e gruppi connessi alla criminalità organizzata, nonché di potenziali *insider*.

Con riferimento al binomio capacità/intenzionalità degli attori statuali, la consapevolezza dell'entità del rischio ad opera di una moltitudine di attori della minaccia, parallelamente ai massicci investimenti in *cybersecurity* di alcuni Paesi occidentali, potrebbe comportare, a livello internazionale, una allocazione di risorse crescenti finalizzate alla costituzione/consolidamento di *asset* cibernetici a connotazione sia difensiva, sia offensiva, impiegabili nella prosecuzione di campagne di *cyber-espionage*, nonché in innovativi contesti di conflittualità ibrida e asimmetrica (*cyberwarfare*), anche attraverso attività di *disruption* di sistemi critici in combinazione con operazioni di guerra psicologica.

Si prevede una sostanziale stabilità delle attività malevole nel *cyberspace* di matrice attivista (*web defacement*/DDoS, *vds. Glossario*) e terroristica (*defacement*, reclutamento e proselitismo *on-line*), anche se per queste ultime non si può escludere l'acquisizione di capacità operative attraverso il ricorso al cd. *"Cybercrime-as-a-Service"* (*vds. Glossario*). Ciò, a differenza delle attività di natura criminale (sottrazione di dati delle carte di credito, identità personale, frodi *on-line*, commercio illegale di beni e servizi nel *dark web*, ecc.), per le quali permangono le criticità connesse alle crescenti saldature, richiamate in precedenza, con ambienti e sodalizi criminali e non, orbitanti al di fuori del *cyberspace*.

I settori a rischio continueranno ad essere quelli ad alto contenuto tecnologico e di *know how*, con livelli di *time to market* contenuti, quali il segmento farmaceutico e del *software*, ovvero *target* il cui danno reputazionale sia suscettibile di ingenerare significativi impatti economici e di mercato.

I settori bancario e sanitario costituiranno - sempre nel breve-medio periodo - *target* privilegiati, anche per il valore intrinseco dei dati

finanziari e personali posseduti, sfruttabili, attraverso il furto di identità, nell'ambito di attività di frode, nonché, nel caso dell'area finanziaria, per le potenziali ingenti sottrazioni di valuta perseguibili tanto a livello massivo (frodi connesse alle carte di credito/debito), quanto a livello dei circuiti interbancari, nonché attraverso la potenziale manipolazione degli algoritmi di *trading* combinata con attività di speculazione sui mercati. Il gradiente di rischio, per il settore sanitario, potrebbe risultare più significativo in ragione del crescente ricorso al supporto ICT sia nel management dei processi organizzativi (cartelle cliniche, dati sanitari, ecc.), sia nella gestione dei presìdi biomedicali (controllo remoto dei *pacemaker*, robotica sanitaria, sistemi automatici di *monitoring* di parametri critici, ecc.).

L'evoluzione dei sistemi ICS/SCADA (*Industrial Control Systems/Supervisory Control and Data Acquisition, vds. Glossario*) e il progressivo aumento delle possibilità di gestione e controllo in remoto delle attività produttive esporrà, verosimilmente, il settore manifatturiero al rischio di crescenti compromissioni *cyber*, finalizzate ad alterare i dati operativi di processo, con potenziali impatti di ordine non solo economico ma anche cinetico. A questo proposito, una particolare area di criticità è rappresentata dall'evoluzione tecnologica del settore *automotive* e *smart car*, laddove la potenziale interconnessione, già dimostrata da alcuni ricercatori, tra i sistemi deputati all'intrattenimento ed all'ausilio alla guida con quelli dedicati alla gestione elettro-meccanica del veicolo, potrebbe comportare gravi rischi nella condotta dello stesso, in caso di compromissione. Sempre sul piano degli effetti cinetici perseguibili attraverso un attacco *cyber*, l'ampiezza della superficie di attacco delle infrastrutture critiche nazionali (aree del trasporto e dell'energia piuttosto che i sistemi idrici a servizio industriale e/o civile) è direttamente proporzionale al crescente livello di interdipendenza tra le stesse e le rispettive *supply chain*.

Quanto alle metodiche di attacco, l'evoluzione degli APT, oltre a caratterizzarsi per il ricorso ad innovative tecniche di "*spear phishing*" e di "*watering-hole*" (*vds. Glossario*), combinate con sofisticate attività di

ingegneria sociale (*vds. Glossario*), si potrebbe connotare sempre più per l'impiego di *software* nativo, ossia di *Remote Administration Tool* (RAT, *vds. Glossario*), già presente sui sistemi-obiettivo ed utilizzati per lo svolgimento di attività legittime. Ciononostante, lo sviluppo delle manovre intrusive con finalità di *cyber-espionage*, di matrice sia statuale che criminale, continuerà a connotarsi per il ricorso sia ad *exploit* (*vds. Glossario*) e a *malware* "customizzati" sul singolo *target*, sia ad armi digitali *standard*, di larga diffusione nell'ambiente *underground* (*vds. Glossario*). Tale disponibilità, economicità e facilità di accesso a *tool* offensivi è in grado di ampliare il bacino dei potenziali attori ostili, al netto di competenze specialistiche.

PAGINA BIANCA

Le parole del *cyber*

0-day. Qualsiasi vulnerabilità non nota e relativo attacco informatico che la sfrutta.

Advanced Persistent Threat **(APT)**. Minaccia consistente in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti bersaglio al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle reti dell'ente obiettivo.

Attribution. Termine che identifica l'attribuzione di una specifica minaccia *cyber* come, ad esempio, una campagna di *cyber*-spionaggio, ad un determinato attore ostile.

Bring Your Own Device **(BYOD)**. Insieme di *policy* interne ad un'organizzazione, sia essa pubblica o privata, volte a regolare l'impiego di dispositivi digitali personali all'interno della stessa, da parte dei relativi dipendenti.

Cybercrime-as-a-Service. Fornitura, da parte di gruppi criminali, di servizi e prodotti, solitamente acquistabili sul mercato nero digitale, utilizzabili da parte di terzi al fine di sferrare attacchi informatici. Tra i "beni" commercializzati figurano *exploit kit*, *malware*, nonché piattaforme da usare per la raccolta di materiale illegale od oggetto di indebita acquisizione.

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*.

DNS Poisoning. Noto anche come *DNS Cache Poisoning*, è la compromissione di un server *Domain Name System* (DNS) comportante la sostituzione dell'indirizzo di un sito legittimo con quello di un altro sito infettato dall'attaccante.

Domain Name System **(DNS)**. Sistema per la risoluzione di nomi dei nodi della rete (cd. *host*) in indirizzi IP e viceversa.

Exploit. Codice che sfrutta un *bug* o una vulnerabilità di un sistema informatico.

Hacktivista. Termine che deriva dall'unione di due parole, *hacking* e *activism* e indica chi pone in essere 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*.

Indicators of Compromise **(IoC)**. Indicatori impiegati per la rilevazione di una minaccia nota e generalmente riconducibili ad indirizzi IP delle infrastrutture di Comando e Controllo (C&C), ad *hash* (MD5, SHA1, ecc.) ai moduli del *malware* (librerie, *dropper*, ecc.).

Industrial Control System **(ICS)**. I sistemi di controllo industriale includono i sistemi di controllo di supervisione e acquisizione dei dati (*Supervisory Control and Data Acquisition*-SCADA), i sistemi di controllo distribuiti (*Distributed Control Systems*-DCS) e i controllori a logica programmabile (*Programmable Logic Controller*-PLC), impiegati usualmente negli impianti industriali.

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

Internet of Things (IoT). Neologismo riferito all'interconnessione degli oggetti tramite la rete Internet, i quali possono così comunicare

dati su se stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di impiego sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, fino all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

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

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

Remote Administration Tool **(RAT)**. Si tratta, letteralmente, di strumenti di amministrazione remota di *server* o postazioni di lavoro, ossia di una funzionalità che permette all'amministratore del sistema o all'utente di accedere da remoto alla macchina e di eseguire operazioni sulla stessa.

Spear phishing. Attacco informatico di tipo *phishing* condotto contro utenti specifici mediante l'invio di *e-mail* formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o *link* malevoli.

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

Supervisory Control and Data Acquisition **(SCADA)**. Gli SCADA sono una tipologia dei sistemi di controllo industriale. Si tratta di sistemi informatici distribuiti per il monitoraggio ed il controllo elettronico, centralizzato, di infrastrutture cd. *cyber*-fisiche, tra loro anche geograficamente lontane, tipicamente utilizzati in ambito industriale, ovvero da infrastrutture critiche.

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

Underground. Con tale termine si intende l'ambiente, solitamente digitale, frequentato per l'acquisto o la condivisione di strumenti di *hacking*.

Watering-hole. Particolare tipologia di attacco in cui l'attore ostile individua, sulla base di attività di osservazione e profilazione del *target*, i siti *web* di interesse della vittima e li infetta con *malware*, così da poter colpire indirettamente l'obiettivo. Tale strategia si rivela particolarmente utile laddove non sia possibile diffondere il *malware* tramite *spear phishing*.

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.

170330018830