III

LE SFIDE GLOBALI

1. Minaccia cibernetica

L'attività di intelligence nel corso del 2011 ha considerato con prioritaria attenzione la minaccia cibernetica che, secondo valutazioni condivise anche in ambito di collaborazione internazionale, ha fatto registrare una crescita esponenziale.

Il primo dato che emerge con evidenza da questa tendenza è quello dell'aumentata vulnerabilità di una moltitudine di attori, statuali e non, cui ha corrisposto il proliferare di sempre più sofisticate tipologie di "attacchi informatici mirati", ovvero finalizzati a colpire obiettivi selezionati.

Un esempio è rappresentato dai cd. virus "asintomatici", in grado di cancellare le proprie tracce e creare con estrema rapidità delle *botnet* (reti di computer infettati), o dai virus della classe *Stuxnet*, caratterizzati da particolare aggressività e dalla capacità di danneggiare gravemente siste-

mi per il controllo dei processi di produzione industriale.

Tra i nuovi strumenti di attacco informatico si annoverano, altresì, sofisticate forme di intrusione (*Advanced Persistent Threat - APT*), miranti alla sottrazione di informazioni sensibili e proprietà intellettuale di aziende e realtà pubbliche. Le tecniche utilizzate sono state costantemente perfezionate e finalizzate a colpire obiettivi selezionati onde interrompere, almeno temporaneamente, la funzionalità dei sistemi e/o dei servizi utilizzati.

tratti della
minaccia

Dai principali episodi di sabotaggio informatico verificatisi nel 2011 possono enuclearsi, a livello globale, alcune linee di tendenza specie per quel che concerne:

- gli obiettivi, che hanno ricompreso prevalentemente enti, nazionali e interna-

Riquadro 19

ANONYMOUS

Sin dal gennaio 2011 si è affacciato sulla rete un gruppo di *hackers* che si identificano sotto il nome di *Anonymous*.

Questi soggetti si ispirano nei loro comportamenti al protagonista dello storico attentato al Parlamento inglese del 1605 (la cosiddetta “congiura delle polveri”), ripreso in un fumetto del 1988, e rilanciato attraverso la trasposizione cinematografica del Film “V per Vendetta” prodotto nel 2006.

La motivazione dichiarata è lo spirito di equità sociale, giustizia e democrazia.

Attaccano siti o *server* di organizzazioni statali, italiane e/o estere, e di aziende ritenute “anti-democratiche” per condotta o settori di attività.

Le modalità tecniche degli attacchi e lo stile delle relative rivendicazioni fanno ritenere che si tratti di un’organizzazione priva di *leader*, animata da un agglomerato di soggetti iper specializzati sparsi nel mondo.

- zionali, di carattere pubblico e privato ritenuti in via di principio “inespugnabili” (Organismi parlamentari, Forze di polizia, strutture finanziarie internazionali, etc.);
- la tempistica, tendenzialmente coincidente con eventi oggetto di elevata attenzione mediatica. Sono state colpite, infatti, le reti *wireless* del primo G8 sulla *cybersecurity*; alcuni siti istituzionali turchi e spagnoli, rispettivamente alla vigilia delle elezioni parlamentari e a seguito dell’arresto di tre attivisti di *Anonymous* (vds. riquadro 19); siti riconducibili a multinazionali del settore in corrispondenza dell’adozione della *cyberstrategy* del Pentagono;
- il tentativo dei principali gruppi di *hacktivist* di presentarsi come sodalizi strutturati e dotati di un programma d’azione e di rivendicare gli atti di sabotaggio attraverso i più noti *social media*;
- le reazioni dei gestori dei sistemi colpiti, con la diffusa tendenza a non denunciare quanto subito o a minimizzare i danni, al fine di non disvelare criticità di carattere infrastrutturale;
- la difficoltà di identificare i responsabili, alla luce dei limiti connessi alla “tracciabilità” degli attacchi e alla riconducibilità degli stessi a entità statuali, nonché di elaborare le necessarie contromisure rispetto a tecniche sempre nuove e in continua evoluzione.

La minaccia cibernetica è andata sempre più evidenziandosi anche per l'ampio spettro delle motivazioni e quindi delle finalità degli attacchi: la sottrazione di dati a fini predatori; la violazione della proprietà intellettuale; il furto di identità; il proposito di danneggiare, sino alla loro paralisi, la funzionalità delle infrastrutture critiche o di manipolare informazioni al fine di delegittimare le istituzioni o favorire il proselitismo in rete; lo spionaggio vero e proprio, con la sottrazione di informazioni privilegiate o segreti industriali, per alterare la concorrenza e favorire la superiorità strategica di un Paese. Con riguardo alle "aggressioni" riferibili ad attori statuali, appaiono significativi gli allarmi diffusi, nel 2011, da enti operanti nel settore della sicurezza circa la possibilità che molti Paesi stiano arruolando gruppi di *hackers* per finalità offensive. In taluni casi, l'obiettivo sarebbe quello di realizzare una sorta di saldatura tra gli *hackers* operanti nelle diverse aree del mondo al fine di acquisirne le collaudate tecniche di sabotaggio e spionaggio.

Da questa minaccia non sono esenti sistemi operativi e piattaforme mobili in considerazione della loro vasta diffusione e della scarsa attenzione che generalmente si presta nel loro utilizzo. La sempre più diffusa consuetudine di memorizzare su tali supporti documenti, anche di natura sensibile, espone al rischio di sottrazione sia di dati personali sia di informazioni riservate.

La rilevanza che la *cyber-threat* ha assunto nel quadro complessivo delle minacce alla sicurezza ha posto da tempo, come detto, la materia tra gli obiettivi informativi prioritari dell'attività intelligence nazionale, nell'ambito di un più ampio dispositivo basato su un approccio dinamico, integrato e di sistema.

iniziative e
strategie di
risposta

In particolare, è andato strutturandosi presso il DIS un articolato progetto di comparto che prevede, da un lato, il coordinamento e la valorizzazione delle competenze di AISE e AISI e, dall'altro, il necessario raccordo con la struttura di *governance* che dovrà, a livello centralizzato, assumere compiti di coordinamento generale e pianificazione unitaria della risposta nazionale.

La descritta architettura, in linea con le *policy* dei principali Paesi occidentali (vds. riquadro 20), si pone in coerenza con le raccomandazioni formulate nel luglio 2010 dal COPASIR in ordine alla necessità e urgenza di elaborare un modello di *governance* nazionale in materia di sicurezza cibernetica, nel cui ambito l'intelligence, ai sensi della *mission* delineata dalla legge 124/2007, svolga un ruolo centrale per quel che concerne l'individuazione della minaccia.

L'attività informativa è stata, pertanto, orientata alla sicurezza delle reti telematiche – infrastrutture critiche in sé e, talora, strumento di gestione di altre infrastrut-

Riquadro 20

SICUREZZA CIBERNETICA – STRUTTURE DI COORDINAMENTO

Per meglio rispondere alle sfide sempre più incalzanti poste dalla minaccia cibernetica alcuni Stati si sono dotati di organismi di coordinamento nazionale costituendo un'entità centrale presso il vertice dell'Esecutivo. Tale è la soluzione adottata nel Regno Unito, dove la struttura cui è affidato l'indirizzo strategico delle azioni in ambito governativo, denominata OCSIA (*Office of Cyber Security and Information Assurance*), è istituita in seno al *Cabinet Office*; in Francia, dove l'*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) opera alle dirette dipendenze del Primo Ministro; negli USA, ove, sebbene la responsabilità federale dell'azione di prevenzione e contrasto della minaccia cibernetica sia affidata al Dipartimento della *Homeland Security* (DHS), l'organismo di coordinamento, rappresentato dal *Cybersecurity Coordinator* è istituito e opera in seno al *National Security Council*, struttura di diretto supporto del Presidente in materia di sicurezza nazionale.

ture critiche nazionali – nonché dei sistemi informatici delle aziende di rilevanza strategica.

Nel tentativo di circoscrivere la minaccia, si è proceduto, da un lato, a proporre soluzioni volte a garantire la sicurezza dei dati e ridurre i costi di gestione dei sistemi informatici quali a esempio il *cloud computing* (vds. riquadro 21) e, dall'altro, ad avviare iniziative volte a fornire supporto info-operativo di natura tecnica alle infrastrutture critiche telematiche nazionali. Tale ultima attività si è sostanziata, in particolare, nello sviluppo di capacità di *early warning* rispetto alle potenziali minacce cibernetiche nonché in termini di analisi *ex post facto* per la determinazione della provenienza della minaccia e la definizione di contromisure tecniche.

Sempre in ambito nazionale, l'intelligence ha posto in essere attività finalizzate a:

- acquisire e integrare, nello strumento operativo nazionale, sistemi tecnico-operativi di ultimissima generazione, necessari allo svolgimento dell'attività istituzionale;
- perfezionare una struttura tecnologica in grado di supportare l'attività informativa in termini di tracciabilità delle minacce e cognizione degli interessi che le attivano;
- conseguire *standard* e procedure operative compatibili con i contesti dell'Unione Europea e della NATO anche attraverso la pianificazione e lo svolgimento di esercitazioni mirate;
- normalizzare il flusso di informazioni di Intelligence Tecnologica verso le

Riquadro 21

IL CLOUD COMPUTING

Il cloud computing o nuvola elettronica (“cassaforte” virtuale all’interno della quale riporre l’intero sapere informatico della collettività) consente di non memorizzare più i *file* di dati e *software* sul PC. Questi ultimi vengono invece conservati e operano a partire da server remoti, messi a disposizione a prezzi convenienti da grandi aziende informatiche ai quali è possibile accedere solo attraverso *internet*. Tuttavia, tale opzione è stata criticata per l’eccessiva concentrazione del patrimonio di conoscenze e per la conseguente maggiore remuneratività in caso di attacco portato con successo ai server, nonché per la delega “assoluta e incondizionata” al gestore di sistema relativamente alle operazioni di amministrazione dei dati. L’unicità del mezzo utilizzato espone a ulteriori rischi e criticità ove si consideri che, in assenza di connessione a *internet* (casuale o provocata), sarebbero inutilizzabili tutti i servizi *cloud* e i computer dipendenti da questi ultimi per il loro funzionamento.

strutture tecnico-operative “di pronto intervento” attive in territorio nazionale (*Computer Emergency Response Team – CERT*);

- sviluppare ogni utile sinergia con il settore privato, al fine di far evolvere la conoscenza e la consapevolezza della minaccia cibernetica;
- rafforzare la cooperazione con i principali Servizi occidentali, con l’intensificazione dello scambio informativo e l’avvio di un progetto basato su omogenee metodologie di lavoro.

A ribadire la rilevanza unanimemente assegnata alla materia del “cyberspazio” è intervenuta la Conferenza internazionale sullo spazio cibernetico, svoltasi agli inizi di novembre a Londra, che ha visto la partecipazione di alte personalità sia del mon-

do politico che di quello delle Tecnologie dell’Informazione e delle Telecomunicazioni (*Information and Communication Technology - ICT*).

Di interesse, in particolare, nel quadro di una trattazione multidisciplinare e di ampio respiro, i sette principi illustrati dal *Foreign Office* britannico, definiti imprescindibile riferimento in vista della messa a punto di regole di comportamento globalmente condivise. Si è fatto stato, in particolare, della necessità che:

- gli Stati agiscano nel *cyberspace* in modo proporzionato e in conformità con le leggi internazionali;
- sia garantito a chiunque l’accesso allo spazio cibernetico e alle tecnologie che ne consentono l’uso;
- siano rispettate le diversità (lingui-

stiche, culturali e ideologiche) degli utenti;

- il *cyberspace* rimanga aperto all'innovazione, alla libera circolazione delle idee, delle informazioni e delle forme di espressione;
- sia rispettato il diritto alla *privacy* dei singoli e sia adeguatamente tutelata la proprietà intellettuale;
- si pongano in essere congiunte metodologie di contrasto alla criminalità cibernetica;
- si promuova uno spazio cibernetico competitivo, idoneo a garantire a chi vi opera adeguati ritorni economici.

Vale evidenziare, infine, come, nel complessivo scenario cibernetico, vada confermandosi il ricorso all'utilizzo delle reti informatiche a scopo offensivo quale fattore caratterizzante delle politiche militari di un numero crescente di Governi.

Alla luce di ciò va letta la decisione degli Stati aderenti all'Alleanza Atlantica di inserire la minaccia cibernetica tra le priorità nel nuovo *Concetto Strategico della NATO* onde individuare i settori maggiormente esposti e gli strumenti idonei a prevenire e/o contrastare eventuali attacchi informatici.

2. Minaccia terroristica in Italia e in Europa

Sebbene i drammatici eventi del 22 luglio in Norvegia (con il duplice attentato di Oslo e Utoya) abbiano riproposto motivazioni di matrice diversa, segnatamente dell'ultradestra xenofoba, il terrorismo internazionale di ispirazione jihadista continua a rappresentare il principale fattore di rischio per l'Occidente.

A fronte della confermata "regionalizzazione", il terrorismo di ispirazione qaidista resta ancorato, per sua stessa connotazione ideologica, a una visione marcatamente anti-occidentale, cui si accompagna la perdurante aspirazione a concretizzare progettualità offensive anche sul suolo dei "miscredenti".

il trend della minaccia jihadista

Sulla base dei riscontri dell'attività informativa svolta da AISE e AISI, il livello della minaccia jihadista in

Europa risulta nel complesso stazionario.

in Europa ...

Le operazioni di controterrorismo condotte nel 2011 – che hanno portato alla neutralizzazione di

cellule e ad arresti di elementi sospettati di pianificare attacchi terroristici contro obiettivi diversificati, in particolare in Spagna, Regno Unito, Germania, Fran-

cia, Finlandia e Svezia – testimoniano, oltre che l'attenzione di Servizi e Forze di polizia verso il fenomeno, la perdurante rilevanza del territorio del Vecchio Continente principalmente quale:

- retrovia logistico-finanziario e bacino di reclutamento per il sostegno al *jihad* nelle aree di crisi;
- obiettivo, più che di gruppi strutturati riconducibili alle principali organizzazioni qaidiste, di autonome iniziative a opera di elementi radicali isolati, i cd. terroristi solitari "fai-da-te", mossi da spirito emulativo ovvero alla ricerca di fama e notorietà personali (vds. riquadro 22). In tal senso, vanno inquadrati gli attentati – effettuati con armi da fuoco, a Francoforte, il 2 marzo, da un estremista kosovaro – contro un gruppo di militari statunitensi diretti in Afghanistan, da un attivista islamico di orientamento wahhabita e di cittadinanza serba (due morti e due feriti) e a Sarajevo, il 28 ottobre, contro personale della Rappresentanza diplomatica statunitense.

Rimane all'attenzione, pur in assenza di attuali riscontri, l'eventualità che possano far ingresso e rientro in Europa soggetti con esperienze di addestramento o combattimento in teatri di *jihad* intenzionati – autonomamente o per conto di forma-

Riquadro 22

IL TERRORISTA “*LONE WOLF*” (LUPO SOLITARIO)

Secondo la più accreditata definizione in ambito internazionale, per terrorista “*lone wolf*” o “*lone actor*” si intende un soggetto che pianifica e si attiva autonomamente, a differenza del “*solo terrorist*” che agisce parimenti da solo ma riceve l’*input*, organizzativo/logistico, da un gruppo o rete terroristica. A volte il terrorista solitario interagisce o agisce con altri individui, costituendo il cd. “*lone wolf pack*” ovvero un sodalizio/microcellula che opera comunque sempre in completa autonomia.

La casistica non consente di codificare un profilo di terrorista “*lone wolf*”/“*lone actor*”, anche se appaiono riscontrabili alcune caratteristiche ricorrenti: giovane età, sesso maschile, problemi di ordine socio-economico/familiare, talvolta disturbi mentali (ossessioni, atteggiamenti compulsivi), precedenti penali per reati comuni, radicalizzazione attraverso il *web*, disponibilità (legale o illegale) di armi da fuoco, area di operatività terroristica coincidente o contigua al luogo di residenza, assenza di collegamenti tra aggressore e vittime.

Il concetto di terrorista “*lone wolf*” risalirebbe alla prima ideologia anarchica russa del XIX secolo, per essere poi ripreso dalla narrativa jihadista. Nel 2004, nell’opera-omnia “*Global Islamic Resistance Call*” dell’ideologo islamista Mustafa Setmariam Nasar *alias* Abu Musab al Suri, compare il primo riferimento, per il contesto islamico, al terrorismo “*lone actor*” ovvero *jihad* individuale. Più di recente, nel 2010, lo stesso concetto viene ripreso da Adam Gadahn *alias* Azzam l’Americano nel suo video sul *web* “*A call to arms*”, una sorte di manifesto del terrorismo “*lone actor*”, e ribadito dallo yemenita-americano Anwar al Awlaqi nella rivista jihadista *on-line* in lingua inglese “*Inspire*”.

zioni operanti all’estero – a costruire un tessuto logistico e di relazioni funzionale a supportare programmi terroristici da realizzare altrove o sullo stesso territorio europeo. Di rilievo, in proposito, le evidenze concernenti il trasferimento, verso le principali aree di crisi africane e asiatiche, di immigrati da tempo residenti in Europa ovvero europei di seconda/terza generazione che talvolta fanno ritorno nel Vecchio Continente a conclusione di *iter* addestrativi. Tali soggetti sono risul-

tati essere, per la maggior parte, assidui frequentatori di siti *web* jihadisti, tramite i quali avrebbero compiuto il proprio percorso di “auto-radicalizzazione” entrando, sovente, in contatto con elementi in grado di assicurare loro il sostegno necessario.

Cruciale si conferma, al riguardo, il ruolo di *internet* quale strumento per la diffusione di ideologie estremiste atte a favorire processi di radicalizzazione e per il consolidamento di reti relazionali nell’ambito

di attività di indottrinamento, propaganda e proselitismo.

In prospettiva, per effetto degli storici eventi registratisi nel mondo arabo-musulmano a partire dai primi mesi dell'anno – dalle rivolte in Nord Africa e Medio Oriente alla neutralizzazione di numerosi esponenti della *leadership* ideologica e operativa di *al Qaida* – potrebbe assistersi a un incremento:

- dell'attivismo di militanti islamisti – galvanizzati dalla caduta dei regimi “apostati” tunisino, egiziano e libico e intenzionati ad approfittare del ritardo nella stabilizzazione della locale cornice politica e di sicurezza – per offrire supporto a tentativi di rilancio del *jihād* in quelle zone. In tal senso va sottolineato come specialmente l'intervento militare della NATO in Libia abbia fornito ulteriore spunto alla retorica qaidista contro l'Occidente, nonostante la condivisa riprovazione del regime di Gheddafi. Tra i messaggi più significativi, si ricorda quello del 12 ottobre, nel quale il nuovo capo di *al Qaida*, Ayman al Zawahiri, nell'elogiare i ribelli libici per aver conquistato Tripoli e aver “cacciato” Muammar Gheddafi, definisce l'Alleanza Atlantica una “banda occidentale”. Nella medesima ottica, non sono da sottovalutare le minacce nei confronti dei Paesi europei reiterate dalla rete qaidista, segnatamente da *al Qaida nel Maghreb Islamico* (AQMI), che potrebbe tentare di infiltrare propri elementi tra i flussi

di clandestini provenienti dal quadrante nordafricano e/o attivare proprie cellule presenti in territorio europeo;

- di attacchi *low-cost*, con mezzi improvvisati, a opera di singoli/microgruppi *self-starter*, stimolati dai crescenti appelli propagandistici al *jihād* individuale, contro obiettivi ritenuti coinvolti nella “crociata anti-islamica” o espressione della perdurante “ingerenza occidentale” nei Paesi arabo-musulmani. Esemplicativi, in tal senso, un video del 2 giugno diffuso sul *web* da *as Sahab*, centro mediatico ufficiale di *al Qaida*, in cui viene elogiata l'efficacia del *jihād* individuale, e i plurimi riferimenti all'attivazione, anche singola e spontanea, comparsi nella rivista jihadista *on-line* di lingua inglese *Inspire* (vds. riquadro 23). Nelle strategie della *leadership* qaidista, l'offensiva “diffusa” e “a bassa intensità”, risulta funzionale, in questa fase, a compensare la temporanea difficoltà di realizzare attacchi di alto impatto, conseguente anche al ripiegamento del nucleo storico di *al Qaida* (*AQ Core*), al momento impegnato soprattutto a mostrare, attraverso i contatti con le articolazioni regionali, la propria vitalità in Africa e a proseguire la guerriglia nell'area di elezione afghano-pakistana, al fianco dei *Taliban*.

In termini di tendenze evolutive con specifico riferimento all'Italia, l'onda lunga della “Primavera araba” non ha determinato, sino a oggi, signifi- ... e in Italia

Riquadro 23

INSPIRE

Il primo numero della rivista è apparso nel giugno 2010 sui maggiori *fora* estremisti. Pubblicazione di impronta jihadista, riconducibile al defunto ideologo di *al Qaida nella Penisola Arabica* (AQAP), Anwar al Awlaki, e dal significativo titolo, *Inspire* è portavoce della citata formazione terroristica e rientra, a pieno titolo, nella strategia comunicativa della rete qaidista. Una strategia volta a utilizzare in misura crescente e sempre più sofisticata il circuito mediatico, con l'obiettivo di dare massima risonanza, a livello globale, alle proprie tesi anti-occidentali, in funzione di consenso e proselitismo. I *target-audience* della rivista sono le comunità musulmane presenti nei Paesi occidentali.

Proprio da un numero di *Inspire* il ventenne cittadino americano di origine dominicana, Josè Pimentel – arrestato il 19 novembre 2011 dalla polizia di New York con l'accusa di aver cercato di realizzare ordigni esplosivi artigianali per colpire uffici del Governo ovvero militari statunitensi reduci dall'Iraq o dall'Afghanistan – avrebbe acquisito le nozioni necessarie per costruire gli ordigni.

Pimentel, auto-radicalizzatosi attraverso *internet*, pur avendo manifestato sul *web* il suo sostegno ad *al Qaida*, non sembra riconducibile ad alcuna organizzazione terroristica, rappresentando quindi un tipico esempio di *lone terrorist*.

ficative ripercussioni sotto il profilo della minaccia terroristica.

La comunità musulmana nel suo complesso ha infatti mostrato una composta partecipazione agli accadimenti e, pur cogliendosi segnali di fermento soprattutto nei segmenti nazionali delle varie organizzazioni dissidenti (dinanzi alle inattese prospettive di affermazione politica nei Paesi di origine), non si è assistito entro i nostri confini né a violente contrapposizioni tra sostenitori degli insorti ed elementi filo-governativi, né a una concreta risposta, da parte di ambienti

radicali sul territorio, agli appelli qaidisti che peroravano una jihadizzazione dei moti popolari.

Nondimeno, restano all'attenzione le implicazioni connesse agli ulteriori sviluppi delle transizioni in atto soprattutto nello scenario nordafricano, considerato che:

- estremisti rilasciati o evasi dalle carceri nel corso dei tumulti, in passato già coinvolti in indagini sul terrorismo nel nostro Paese, potrebbero riannodare contatti sul territorio nazionale per guadagnare sostegno alla "causa" in madrepatria. La loro influenza, infatti,

potrebbe rivitalizzare i residui circuiti di riferimento (specialmente in ambito lombardo), dove non sembrano da tempo emergere figure di particolare spessore ideologico e carisma in grado di svolgere una funzione d'indirizzo sui più giovani correligionari;

- differenti profili di rischio potrebbero scaturire dal contesto libico, qualora a un eventuale rallentamento del processo di normalizzazione post-bellica corrispondesse una riorganizzazione e controffensiva di componenti del vecchio *establishment*. Un ulteriore fattore di minaccia che viene valutato è legato all'eventuale rafforzamento di formazioni islamiste anti-occidentali (alcune delle quali accusano l'Italia di aver agito contro il popolo libico sin dai tempi dello sfruttamento coloniale) o gruppi filo-qaidisti. Al riguardo, infatti, si ricorda che il nostro Paese è stato espressamente richiamato in un videomessaggio del 13 settembre, nel quale, tra l'altro, il *leader* di *al Qaida* al Zawahiri ha incitato i libici a non dimenticare “*l'Italia e i suoi crimini nel vostro Paese, contro i vostri padri*”.

Al di fuori delle specifiche ipotesi sopra delineate, comunque, l'Italia, per la sua partecipazione a missioni militari in aree di crisi, il suo ininterrotto impegno contro il terrorismo, e, in generale, per motivi ideologico-religiosi, continua a essere oggetto di sentimenti ostili da parte di estremisti islamici e perciò resta un potenziale

target di progettualità offensive di matrice jihadista. Si rileva, a esempio, come alcuni utenti del *forum* d'area *al Shumukh*, uno dei più importanti vettori della propaganda qaidista, abbiano commentato con esultanza le alluvioni che hanno colpito Liguria e Toscana alla fine di ottobre, interpretandole come una punizione di Allah contro la “*casa dei miscredenti*” e una “*maledizione per la guerra mondiale che conducono contro l'Islam e i musulmani*”.

Ai rischi sul versante estero – già richiamati nel precedente capitolo specie con riguardo ai militari italiani impegnati nei teatri di crisi e alla pratica dei sequestri – si accompagnano pertanto quelli all'interno dei confini nazionali, ove l'incognita più insidiosa resta connessa, come già detto, all'imprevedibile iniziativa di terroristi solitari “*free lance*” suggestionati dai menzionati appelli al *jihad* individuale. Al riguardo, sebbene non si siano registrate, nel 2011, minacce dirette contro il nostro Paese, appare comunque indicativo che uno dei personaggi di maggiore rilievo della campagna mediatica di *al Qaida*, il convertito americano Adam Gadahn, nel sollecitare (in un video diffuso in giugno) i musulmani in Occidente a colpire personalità pubbliche, considerate “*facili bersagli*”, abbia citato come esempio i due noti episodi occorsi al Sommo Pontefice e all'ex Presidente del Consiglio Berlusconi.

A fronte del quadro di minaccia delineato, nel

gli internauti
del *jihad*

corso del 2011 è apparso sempre più visibile l'impegno profuso – su *web-forum*, *blog* d'area e *social network* – da un'eterogenea galassia di internauti musulmani italofoeni (italiani convertiti inclusi), sia per propagare ideologie estremiste, favorendo la radicalizzazione di correligionari, sia per consolidare reti relazionali sul nostro territorio e all'estero.

Significativa, in tal senso, la rilevata circolazione di pubblicazioni e video di stampo jihadista tratti da *internet* soprattutto in circuiti radicali islamici del Nord Italia, ambito territoriale nel quale sono anche all'attenzione pulsioni marcatamente antisioniste manifestate all'interno di ristrettissimi gruppi giovanili. Un utilizzo del *web* in chiave estremista va emergendo, sebbene ancora a livello episodico, anche in aree solitamente meno "esposte" al fenomeno, come nel caso dell'arresto a Sellia Marina (CZ), il 31 gennaio 2011, dell'*imam* marocchino della moschea locale, del figlio e di un connazionale, ai quali è stato contestato il reato di addestramento con finalità di terrorismo internazionale.

"Sottotraccia" e in ambiti estremamente circoscritti, si muovono invece elementi della filiera radicale nordafricana ancora in contatto con referenti di gruppi salafiti jihadisti attualmente stanziati nei Paesi di origine e interessati a riavviare, avvantaggiandosi dei maggiori spazi di manovra conseguenti ai rivolgimenti popolari, progetti di "reislamizzazione" di quelle società.

..... Riquadro 24

LIBERATION TIGERS OF TAMIL EELAM (LTTE) – PROIEZIONI IN TERRITORIO NAZIONALE

La diaspora *tamil* appare sempre più orientata a considerare con distacco l'esperienza armata del *Liberation Tigers of Tamil Eelam (LTTE)* e a sostenere il percorso politico intrapreso a livello internazionale nel 2010 per il raggiungimento dall'autodeterminazione nello Sri Lanka. Nondimeno, permane al suo interno un gruppo di intransigenti, tra cui alcuni soggetti all'epoca processati (e poi assolti) con l'imputazione di aver sostenuto l'attività terroristica del LTTE che, facendo leva sull'assenza di risultati tangibili, potrebbe spingere la comunità di riferimento verso posizioni più oltranziste.

Opera di supporto ai *network* integralisti in patria continuerebbe a essere svolta anche in seno al compartimentato circuito salafita pakistano, anch'esso attestato prevalentemente nel Nord Italia. Tali contatti potrebbero però assumere maggiore rilevanza alla luce delle dinamiche in Pakistan, dove starebbe emergendo – tra le nuove leve – una componente attratta più dal richiamo all'internazionalizzazione della lotta importata dall'esperienza qaidista, che da rivendicazioni localistiche proprie della "questione kashmira".

Riquadro 25

KOSOVO SETTENTRIONALE

Nel contesto di origine, le perduranti tensioni interetniche hanno concorso a qualificare la delicata cornice di sicurezza del Kosovo settentrionale, condizionata dai ripetuti scontri tra estremisti serbo-kosovari, contrari all'assunzione dei controlli di confine e doganali da parte delle Autorità di Pristina, e la *Kosovo Force* (KFOR), impegnata a garantire, insieme con EULEX (*European Union Rule of Law Mission in Kosovo*), il ripristino della legalità nell'area e il consolidamento delle istituzioni nel resto del Paese.

Il quadro di situazione potrebbe risentire negativamente, inoltre, dell'attivismo di neo-costituiti gruppi paramilitari di etnia albanese volto a esercitare pressioni sulla Comunità internazionale e sulle Autorità di Pristina, con ciò profilandosi il rischio di iniziative destabilizzanti da parte di gruppi isolati.

le formazioni
separatistiche

Analoghi fattori di rischio non sembrano invece provenire, al momento, dalle organizzazioni – iscritte nelle liste UE delle entità terroristiche – riconducibili alla causa separatista curda (vds. cap. II, par. 3, riquadro 14), all'estremismo *sikh* e all'indipendentismo *tamil* (vds. riquadro 24).

la dissidenza
iraniana

Del pari, non si sono ravvisati particolari rilievi in ordine all'opera del Consiglio Nazionale della Resistenza Iraniana, componente politica del movimento dissidente iraniano dei *Mujahedin-e Khalq* (MeK) i cui sforzi sono attualmente diretti a ottenere un riconoscimento internazionale del proprio ruolo politico e a tutelare i militanti stanziati nella storica base di Ashraf (Iraq). In mancanza di un pieno

accordo sulle modalità dello sgombero finale e sulle destinazioni degli sfollati di Camp Ashraf, con gravi disagi o rischi per gli stessi, non sono state escluse iniziative dei MeK, anche in territorio nazionale, di sensibilizzazione e protesta, nell'ambito delle quali potrebbero verificarsi, in casi limite, episodi di autolesionismo o gesti dimostrativi contro interessi iracheni o iraniani.

l'irredentismo
panalbanese

Anche le sparute articolazioni nazionali dell'irredentismo panalbanese, nonostante il perdurare di contatti con ex appartenenti a formazioni paramilitari separatiste ancora legati alla causa nell'area balcanica (vds. riquadro 25), restano piuttosto disorganizzate, attraversate da tensioni interne e non in grado di dare concretezza ai propri velleitari programmi.

3. Proliferazione di armi di distruzione di massa

Il contrasto alla minaccia non convenzionale si è confermato una voce prioritaria nell'agenda della politica informativa per la sicurezza del Governo italiano e della Comunità internazionale, nella condivisione di una strategia di risposta primariamente basata sullo strumento della dissuasione e della prevenzione.

In questo senso, complementare e di supporto all'azione della diplomazia, l'impegno dell'intelligence si è rivolto non solo ai disegni proliferanti di attori statuali e alle relative reti di *procurement*, ma anche all'eventualità che soggetti e gruppi terroristici possano ricercare materiali e sostanze ad alta nocività per la concretizzazione di propositi offensivi.

Nel 2011, il quadro della minaccia si è qualificato soprattutto per lo sviluppo dei contenziosi riferibili, rispettivamente, ai *dossier* iraniano, siriano e nordcoreano.

il *dossier*
iraniano

L'Iran, in violazione delle Risoluzioni dell'ONU, ha proseguito le attività relative all'arricchimento dell'uranio nel complesso di Natanz, dove sono stati prodotti complessivamente circa 5.000 kg di uranio a basso tenore di arricchimento (3-4%), un quantitativo teoricamente sufficiente alla realizzazione di tre ordigni a fis-

sione. Nel contempo, nell'impianto pilota (*Pilot Fuel Enrichment Plant* – PFEP) situato nello stesso centro di Natanz, sono stati sinora prodotti circa 80 kg di uranio arricchito al 20%.

Gli iraniani, inoltre, sembrano aver risolto parte dei problemi riconducibili alla diffusione, avvenuta nel 2010, del virus *Stuxnet* nei sistemi computerizzati del *Fuel Enrichment Plant* (FEP) di Natanz, che avrebbe provocato il temporaneo *black-out* di circa 1.000 centrifughe. Ciò sarebbe confermato dall'incremento del numero di centrifughe operative, passate da 4.800 a oltre 6.200, mentre la produzione media mensile di uranio arricchito, dopo l'incremento registrato nel primo trimestre del 2011, sarebbe leggermente diminuita nella seconda metà dell'anno.

Il contenzioso con la Comunità internazionale – scandito da dichiarazioni del Presidente Ahmadinejad attestanti la determinazione a proseguire le attività di arricchimento dell'uranio (vds. riquadro 26) e a non fornire spiegazioni in merito ad alcuni punti controversi del programma sviluppato – ha fatto registrare nuovi picchi di tensione a seguito del Rapporto dell'Agenzia Internazionale per l'Energia Atomica (AIEA), pubblicato l'8 novembre, che ha confermato l'impossibilità di dare credibile

Riquadro 26

NUCLEARE IRANIANO — PROGETTI ANNUNCIATI DA TEHERAN

Teheran, oltre a proseguire i lavori di realizzazione del reattore IR-40 nel Centro di ricerche di Khondab e le attività relative all'estrazione/concentrazione dell'uranio presso Gchine e Saghand (Yazd), ha annunciato:

- l'imminente avvio della produzione di uranio arricchito al 20% nell'impianto in caverna di Fordow, presso Qom, dove sono state già installate tre cascate di centrifughe di tipo IR-1;
- l'installazione di nuove centrifughe di seconda generazione (denominate IR-2M e IR-4, con componenti in fibra di carbonio), aventi prestazioni, affidabilità e capacità produttive notevolmente maggiori di quelle sinora utilizzate, di obsoleta tipologia IR-1. A tale proposito si segnala che Teheran, in ragione delle difficoltà nell'approvvigionamento di fibra di carbonio nonché della tecnologia per produrla, sta cercando di dotarsi di autonome capacità produttive nello specifico settore. In particolare, nell'agosto scorso la TV iraniana ha mostrato la cerimonia di inaugurazione del primo impianto per la produzione di fibra di carbonio;
- l'intendimento di realizzare 4-5 nuovi reattori di ricerca, per la produzione di radioisotopi, che potrebbero essere alimentati con l'uranio arricchito al 20%, prodotto con le risorse nazionali.

assicurazione che le attività poste in essere dall'Iran nel settore nucleare siano riconducibili a scopi esclusivamente civili.

In questo quadro si collocano le nuove indicazioni concernenti attività iraniane riconducibili a piani strutturati di sviluppo di armamento nucleare. Secondo le evidenze emerse, il progetto, che avrebbe avuto inizio nel 2003, potrebbe essere ancora operativo (vds. riquadro 27).

Il complesso degli elementi informativi converge nell'indicare che le progettualità iraniane risultano verosimilmente compati-

li con finalità militari. Tuttavia si ritiene che il programma, seppur sostanzialmente inarrestabile a causa del possesso della tecnologia e del *know-how* per produrre il materiale fissile *weapons grade*, possa essere ritardato/ostacolato dalle sanzioni e dagli incidenti che hanno colpito alcuni impianti sensibili.

Per quanto concerne il programma missilistico, nel periodo considerato Teheran ha proseguito lo sviluppo dei propri progetti conducendo numerosi test di sistemi balistici a corto e medio raggio, con gittata, rispettivamente, di 750 e 1.900/2.000 Km.

Riquadro 27

IL CENTRO DI RICERCHE DI PARCHIN

Secondo i documenti di cui l'AIEA è entrata in possesso, parte delle attività relative alla *weaponization* venivano svolte nel centro di ricerche di Parchin, dove è stata osservata, alcuni anni fa, la presenza di un *container* di acciaio, sospettato di essere utilizzato per la conduzione di test idrodinamici, con l'impiego di esplosivi a elevata energia cinetica, finalizzati alla realizzazione di un ordigno nucleare con innesco di tipo implosivo. Tuttavia le due ispezioni effettuate nel 2005 non hanno evidenziato alcuna prova delle suddette attività. Peraltro, a seguito della pubblicazione del Rapporto, gli iraniani starebbero effettuando operazioni di bonifica nel suddetto sito sollevando ulteriori perplessità in merito alle reali finalità del programma sviluppato.

Anche in quest'ambito, non sono mancati annunci, da parte di Teheran, relativi alla realizzazione di nuovi vettori. Dichiarazioni in questo senso hanno riguardato, in particolare, un missile antinave di tipo balistico avente velocità supersonica e gittata massima di 300 Km e un missile da crociera, interamente realizzato con le risorse iraniane, che avrebbe una gittata massima di 200 Km e sarebbe in grado di colpire navi e obiettivi costieri.

le evidenze
sulla Siria

L'atteggiamento della Siria nei confronti dell'AIEA ha provocato il suo deferimento al Consiglio di Sicurezza dell'ONU per violazione del Trattato di Non Proliferazione.

Il provvedimento è stato adottato il 9 giugno 2011 dal Consiglio dei Governatori dell'Agenzia a seguito del Rapporto pub-

blicato il 24 maggio precedente, secondo cui l'edificio distrutto dall'aviazione israeliana nel settembre 2007 in località Dayraz Zawr, presso al Kibar (vds. riquadro 28), era molto probabilmente un reattore nucleare plutonigeno, che avrebbe dovuto quindi essere dichiarato all'Agenzia internazionale.

A nulla è valso l'estremo tentativo delle Autorità di Damasco di disinnescare il contenzioso con l'invio di una lettera al Direttore Generale dell'Agenzia nella quale si sono dichiarate disponibili a collaborare pienamente aprendo i siti alle attività ispettive.

In relazione alla crisi in atto in Siria, l'attività informativa si è focalizzata anche sulla monitorizzazione delle attività nel settore della guerra chimica ove si consideri che Damasco non ha aderito alla Convenzione per il Bando delle Armi Chimiche e