box 21

VOLONTARI ITALIANI NELLA CRISI UCRAINA

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

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

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

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

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

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

PAGINA BIANCA

SCENARI E TENDENZE: UNA SINTESI

PAGINA BIANCA

SCENARI E TENDENZE: UNA SINTESI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DOCUMENTO DI SICUREZZA NAZIONALE

ALLEGATO ALLA RELAZIONE ANNUALE AL PARLAMENTO

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

PAGINA BIANCA

Premessa

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

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

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

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

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

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

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

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

PAGINA BIANCA

Potenziamento delle capacità cibernetiche nazionali

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

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

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

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

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

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