LA *CYBERTHREAT*

Aspetti generali

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

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

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

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

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

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

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

La "guerra ibrida"

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

Attori minacce e finalità

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

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

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

Lo spionaggio digitale

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

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

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

L'hacktivismo

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

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

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

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

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

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

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

Il cyberjihad

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

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

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

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

La criminalità informatica

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

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

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

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

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

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

box 18

LE PAROLE DEL *CYBER*

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

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

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

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

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

Malware. Contrazione di *malicious software*. Programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

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

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

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

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

Trojan. *Malware* che impiega l'ingegneria sociale, presentandosi come un file legittimo (ad esempio con estensione .doc o .pdf), facendo credere alla vittima che si tratti di un file innocuo, ma che in realtà cela un programma che consente l'accesso non autorizzato al sistema da parte dell'attaccante. Il *trojan* può avere diverse funzioni: dal furto di dati sensibili al danneggiamento del sistema *target*.

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

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

PAGINA BIANCA

AZIONE PREVENTIVA E PROSPETTIVE

Le reti di rilevanza strategica

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

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

Le vulnerabilità dei sistemi

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

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

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

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

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

La progressione della minaccia

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

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

PAGINA BIANCA

SCENARI E TENDENZE: UNA SINTESI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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