di operare, nonché di individuare, analizzare, prevenire e contrastare le minacce geografiche e fenomeniche alla sicurezza nazionale. Si è, in particolare, accresciuta nell'ultimo anno la loro complementarietà nel fornire al decisore politico organici quadri di insieme dei problemi e delle dinamiche trattate.

Il Comparto, oltre ad assicurare il monitoraggio del quadro della minaccia, ha sempre più operato per fare emergere, sulla base delle indicazioni del Vertice governativo e in specie dell'Autorità Delegata, elementi informativi utili all'esercizio di opzioni di *policy* che tenessero adeguatamente conto degli interessi nazionali di volta in volta in gioco. Decisivo, a tal fine, è stato l'intenso lavoro svolto dal CISR, configuratosi quale vero e proprio "Gabinetto per la sicurezza nazionale", per ciò stesso naturale detentore di quella visione olistica indispensabile per affrontare adeguatamente le varie sfide alla sicurezza della Nazione.

Va al riguardo sottolineato come, in termini ancor più accentuati che negli anni precedenti, il 2013 si sia caratterizzato per due fenomeni. Da una parte, le minacce tradizionali allo Stato si sono intrecciate in maniera sistemica a nuovi fattori di rischio, fondamentalmente legati all'utilizzo di avanzate tecnologie cibernetiche, capaci di incidere in profondità sul nostro patrimonio di beni collettivi così da mettere a repentaglio la sicurezza di istituzioni, imprese, cittadini e infrastrutture critiche, dunque il complesso dei nostri interessi vitali.

Dall'altra, la congiuntura ha reso ancor più stringente la necessità di incentrare maggiormente l'attività di AISE ed AISI sulla dimensione economica della sicurezza, al fine di individuare per tempo dinamiche e relazioni potenzialmente pericolose per la salvaguardia e lo sviluppo del sistema produttivo nazionale.

Si è reso pertanto necessario rafforzare, anche sul piano istituzionale, la capacità del Paese di dotarsi di uno sguardo strategico, in grado di fornire all'Autorità di governo un quadro di lungo periodo delle evoluzioni dello scenario di sicurezza nelle sue variegate implicazioni, consentendole in tal modo di assolvere alle sue responsabilità con scelte efficaci, commisurate alla portata ed alla natura delle nuove minacce.

Per questo motivo, l'Autorità politica – nelle sue consuete linee di indirizzo – ha confermato quali priorità di intervento proprio il contrasto alla minaccia cibernetica ed ai pericoli per la sicurezza economica del Paese.

Le linee guida della Relazione

Ed è, specificamente, in riflesso di tale unitarietà di approccio, che la presente Relazione si apre con una disamina fenomenica della minaccia *cyber* – rimandando la descrizione ragionata della risposta degli Organismi all'allegato Documento sulla Sicurezza Nazionale, come previsto dall'articolo 38 della Legge 124/2007 – ed articola le successive sezioni lungo un filo condut-

tore unico, finalizzato a trattare anche in chiave economico-finanziaria le minacce asimmetriche e le aree geografiche di crisi oggetto d'esame.

Quello trascorso è stato l'anno nel quale, in ottemperanza al disposto normativo della Legge 133 del 2012, sono state adottate scelte conseguenti alla consapevolezza del fondamentale rilievo strategico che, ai fini dell'efficace tutela degli interessi nazionali, riveste lo spazio cibernetico.

La sofisticazione degli attacchi informatici sta infatti crescendo ad un ritmo tale da pregiudicare seriamente, in caso di un attacco rilevante, la stessa stabilità e sicurezza del Paese, in virtù della naturale connessione in rete delle infrastrutture critiche nazionali.

Si è dunque inteso assolvere alla responsabilità di potenziare, attraverso uno sforzo coordinato e convergente delle diverse Amministrazioni dello Stato, la capacità di prevenzione e reazione nei confronti della minaccia cibernetica: un impegno che ha visto l'Italia attiva in consessi multilaterali e nei rapporti coi principali *partner*, e che su scala nazionale ha coinvolto anche il mondo delle imprese e dell'università, alla luce dei rischi di sottrazione del patrimonio industriale e tecnologico nazionale insiti nei crimini informatici.

In seguito ad un lavoro condotto per tutto l'anno dagli esperti dell'intelligence e delle diverse Amministrazioni coinvolte, il Presidente del Consiglio ha adottato, su proposta e deliberazione del CISR e dando seguito ad una specifica direttiva di indirizzo, il "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico" e il "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica".

Sono stati così individuati, insieme con i profili e le tendenze evolutive delle minacce alle reti ed ai sistemi di interesse nazionale, anche gli strumenti e le procedure per contrastarle e sono stati allo stesso tempo definiti tanto i compiti dei vari attori pubblici e privati, quanto gli obiettivi specifici e le linee di azione prioritarie.

È sempre in un'ottica di sistema che l'intelligence italiana, nel 2013, ha approfondito l'analisi della natura economico-finanziaria delle molteplici situazioni di rischio per gli interessi nazionali. Con una visione più organica che in passato, nella messa a punto delle direttrici strategiche e nel concreto corso dell'attività info-operativa ed analitica è stata riconosciuta l'importanza della dimensione economica delle minacce, con particolare attenzione alle vulnerabilità del sistema produttivo, all'impatto della crisi sulla conflittualità sociale e sul rapporto fra cittadini e istituzioni, nonché alle concause geo-economiche, prima ancora che politiche, delle situazioni di instabilità e delle correlate evoluzioni che caratterizzano i quadranti di più immediato interesse per l'Italia.

Si tratta di aspetti prioritari per la comunità intelligence nazionale, come tali riflessi nella narrativa della presente Relazione.

La tutela degli interessi economici, scientifici e industriali del Paese, delle sue proprietà intellettuali e del suo *know-how*, in altri termini del suo ingegno, ha costituito tratto qualificante della riforma dei

Servizi di informazione. In epoca di scarsità di investimenti e crisi di liquidità, si guarda peraltro con inevitabile ed opportuno interesse all'afflusso di capitali stranieri nel sistema economico nazionale.

Nell'ultimo anno, l'attività informativa è stata dunque ampliata secondo una nozione di sicurezza nazionale che incorpora la competitività, la crescita economica e la connessa coesione sociale fra i beni essenziali da difendere, partendo da una prioritaria individuazione – condivisa con le Amministrazioni centrali rappresentate nel CISR – dei settori strategici del Sistema Paese.

È all'interno di questo perimetro concettuale, concepito quale coerente integrazione delle necessarie, importanti iniziative attuate dall'Esecutivo per rafforzare la capacità attrattiva del nostro mercato, che i Servizi hanno monitorato le manovre acquisitive suscettibili di incidere sulla competitività del Paese, nonché le attività di spionaggio diretto, in Italia ed all'estero, ai danni del nostro comparto economico-scientifico.

In sinergia con questo ambito di ricerca informativa nel settore economico-finanziario, sono stati sviluppati, lungo il 2013, anche altri filoni ad esso complementari: da quelli, tradizionali, concernenti le pratiche illegali d'impatto sull'erario e le pervasive infiltrazioni della criminalità organizzata nel tessuto produttivo ad altri più innovativi, quale l'analisi dei potenziali rischi insiti nella crescente diffusione della moneta virtuale.

La perdurante congiuntura recessiva non ha, tuttavia, esaurito le sue conseguenze solo nel naturale ambito della dimensione economica della *polis*, dispiegando, piuttosto, tanto ricadute capillari sulle dinamiche sociali interne, quanto effetti indiretti sugli assetti e sui processi evolutivi che hanno contraddistinto gli scacchieri di più diretto rilievo per la proiezione geopolitica dell'Italia e dell'Europa.

La crisi economica ed occupazionale senza precedenti nella storia recente, correlata, a sua volta, a profondi fenomeni trasformativi della società e ad una significativa disaffezione anti-istituzionale, ha anzitutto indotto l'intelligence a cogliere segnali e linee di tendenza della conflittualità sociale relativi a possibili tentativi di strumentalizzazione da parte di formazioni dell'oltranzismo politico.

Gli Organismi hanno inoltre inteso analizzare, durante l'anno, la possibile traduzione del diffuso disagio sociale, conseguito alla crisi, in rischi inediti per la sicurezza: nuove tensioni e spinte antisistema, tenuto conto della sempre più ampia dimensione ed eterogeneità delle fasce sociali, soprattutto giovanili ma non solo, esposte al deterioramento delle condizioni di vita ed al carico di incertezza per l'avvenire.

Si è infine continuato a riservare attenzione alle situazioni di fermento nel mondo del lavoro, alle dinamiche del movimento antagonista nelle sue plurime sfaccettature ed attività di mobilitazione, ed alla minaccia eversiva di varia natura.

Quanto al versante internazionale, è stata l'incidenza dei fattori geo-economici sui processi di transizione in Nord Africa, come pure sulla ridefinizione degli equilibri regionali nel "Mediterraneo allargato", a costituire la filigrana ermeneutica per l'impegno della comunità di intelligence relativo ai complessi fenomeni in atto in quella vasta area.

Le acquisizioni informative hanno corroborato che dalle aree di instabilità – dal Medio Oriente allargato all'Afghanistan – sono promanate, per il nostro Paese, sfide decisive tanto di natura economica, in primo luogo per gli approvvigionamenti energetici, quanto di sicurezza, come il controllo dei flussi migratori, il contrasto ai traffici di armi e la lotta al terrorismo internazionale di matrice jihadista.

Anche la crisi dell'eurozona ha giocato un suo ruolo, riducendo l'interscambio con la sponda Sud del Mediterraneo e concorrendo ad acuire, in quella regione, un generalizzato circolo vizioso fra squilibri macroeconomici, segmentazione politica e *spillover* negativi sulla sicurezza.

Le dinamiche geopolitiche nell'area mediorientale e nel Golfo hanno continuato ad essere condizionate dalla millenaria contrapposizione, interna all'Islam, tra sciiti e sunniti. Al contempo, l'Afghanistan, altro quadrante dove l'intelligence ha proseguito l'azione a tutela della nostra presenza militare e civile, si è caratterizzato per la persistenza di fattori di criticità, nella prospettiva del ritiro delle Forze internazionali.

L'organicità del quadro prospettico così delineato in questa Relazione rispecchia la coesione di approccio del lavoro quotidiano svolto dagli Organismi.

Tale coerenza è stata favorita dall'ulteriore sviluppo di un processo inteso a realizzare, da una parte, la sempre maggiore integrazione istituzionale dei Servizi nell'architettura di governo e, dall'altra, il sempre più esteso *outreach* verso i soggetti pubblici e privati che concorrono – come nel caso delle infrastrutture critiche – alla comune responsabilità per la tutela della sicurezza del Paese.

Più serrate modalità di coordinamento hanno permesso di definire strategie unitarie nell'affrontare le minacce fenomeniche identificate come settori prioritari della ricerca informativa, quella economico-finanziaria e quella cibernetica. In relazione alla prima, sono state anche intessute sinergiche relazioni con Enti pubblici esterni al Sistema, nell'ottica del vicendevole sostegno all'attività informativa ed all'internazionalizzazione del sistema produttivo. In merito alla seconda, si sono, in aggiunta, tenute frequenti riunioni di due appositi consessi, l'uno esteso alle Amministrazioni CISR ed agli attori pubblici competenti per la risposta al rischio cibernetico, l'altro alle imprese private convenzionate con il DIS secondo le apposite previsioni della Legge 124 e del DPCM del 24 gennaio 2013.

La collaborazione con le Amministrazioni CISR si è al contempo ampliata e ramificata, innervando l'ordi-

nario operare degli Organismi informativi con fecondi rapporti funzionali e scambi info-valutativi, venendo arricchita, nel caso del Ministero degli Affari Esteri, con la prosecuzione di un esercizio permanente intrapreso nel 2012 e poi intensificatosi sul piano dell'interazione informativa e delle sinergie d'analisi.

È stato parimenti proseguito e migliorato lo scambio informativo fra l'intelligence e le Forze di polizia, nel quadro di una consolidata collaborazione istituzionale che trova una delle più significative espressioni nel Comitato di Analisi Strategica Antiterrorismo. Si è altresì continuato ad utilizzare la formula dei formati integrati interorganismi per moduli di scambi analitici con i Servizi collegati esteri, intesi quali momenti qualificanti della collaborazione internazionale di cui l'intelligence si avvale nelle dimensioni tattico-operativa e strategica.

Snodo funzionale dell'integrazione per l'attività di intelligence e l'attuazione delle politiche governative in termini di sicurezza nazionale del Paese, è assicurato dall'organo collegiale permanente – istituito nell'ambito del regolamento attuattivo della Legge 133 – presieduto dal Direttore Generale del DIS e composto, oltre che dai Direttori delle Agenzie, dai vertici delle Amministrazioni dei Dicasteri del CISR. Consesso che, a mente delle previsioni del DPCM 24/1/2013, viene integrato con la partecipazione del Consigliere militare del Presidente del Consiglio dei Ministri alle riunioni aventi ad oggetto la materia della sicurezza cibernetica

Il ruolo così acquisito dall'intelligence nella complessiva capacità decisionale dell'Esecutivo le ha permesso di dare slancio ad una contestuale, continua maieutica con tutte le articolazioni del Sistema Italia, imperniata sul concetto di sicurezza condivisa. Il fatto che i nostri destini si collochino a cavallo fra la capacità di difendere gli assetti critici nazionali e l'abilità nel promuovere a livello globale le potenzialità di innovazione, comporta, per la Pubblica Amministrazione – e dunque in maniera specifica per il Sistema di informazione, alla luce delle peculiari responsabilità di cui è investito – il dovere preciso di essere coeso al proprio interno e di interagire contestualmente verso le sfere del settore privato, dell'industria, dell'università e della ricerca.

È soltanto con un dialogo profondo e continuativo con tutti gli *stakeholders* dei beni collettivi materiali e immateriali, finalizzato ad entrare con essi in sintonia su metodi e contenuti del contrasto alle sfide comuni, che la sicurezza può essere efficacemente perseguita, poiché le "chiavi" di quest'ultima, in un mondo multidimensionale come quello in cui ci ritroviamo a vivere, non possono essere possedute da nessun singolo attore.

L'intelligence deve poter trarre efficacia strategica dall'interazione con le istituzioni e può ottenerla con l'integrazione sistemica e di processo. Deve poter contare sulla legittimazione dell'opinione pub-

blica e può conquistarla, spiegando cosa è e cosa fa.

È chiamata a raccogliere informazioni precise sui possibili *target* e modalità di azioni ostili economico-finanziarie e cibernetiche e può acquisirle coltivando legami e connessioni con il settore privato. Può arricchire il suo bagaglio di competenze analitiche avvalendosi dell'esperienza e delle conoscenze accademiche e dei centri di ricerca. Si è dunque presentata al confronto col mondo universitario con modalità innovative, come il *roadshow* avviato a fine ottobre a Roma con La Sapienza per proseguire nei maggiori Atenei della Penisola fra cui, alla presenza dell'Autorità Delegata, l'Università Cattolica del Sacro Cuore di Milano.

Aperta, efficiente, rinnovata, unitaria e integrata: vuol dire, in una sola parola, *consapevole*. *Consapevole* che la sicurezza è condizione essenziale affinché l'Italia possa continuare ad essere protagonista nel mondo al rango che le compete. Dunque *consapevole* di dover essere utile al Paese. È quanto l'intelligence si è impegnata ad essere ed a mostrarsi nel 2013, attraverso l'attività riassunta nelle pagine seguenti. *Consapevole* che lo stesso percorso dovrà essere proseguito in futuro con sempre maggiore coerenza, impegno e determinazione.

Parte prima

LE ASIMMETRIE DELLA MINACCIA

PAGINA BIANCA

LA *CYBERTHREAT*

L'elevato grado di priorità annesso dall'intelligence al contrasto della minaccia *cyber* è correlato all'importanza che riveste lo spazio cibernetico per il benessere e per la sicurezza del Paese. Infatti, solo l'efficace tutela di tale spazio, che comprende tutte le attività digitali che si svolgono nella rete, consente di garantire il normale funzionamento della vita collettiva sotto molteplici profili: politico, sociale, economico, tecnologico-industriale e culturale.

La rilevanza e le caratteristiche del fenomeno

Nell'ottica intelligence, pertanto, prevenire e contrastare il rischio cibernetico significa anche, specie alla luce della persistente crisi economica, proteggere uno strumento indispensabile per potenziare le opportunità di crescita del Paese, sostenendone in tal modo sviluppo e competitività internazionale.

A rendere prioritaria tale minaccia contribuiscono altresì le sfide poste dagli aspetti peculiari che la caratterizzano. Essa, infatti, si presenta come pervasiva, sofisticata, eseguibile con strumenti di facile accesso ed uso, rapida nelle evoluzioni e dotata di elevata capacità di rimodulazione rispetto agli strumenti posti di volta in volta a difesa di reti e sistemi. A complicare ulteriormente tale contesto, interviene inoltre la circostanza che gran parte delle attività intrusive si configurano come anonime, ingannevoli e condotte da soggetti sovente di difficile identificazione grazie all'impiego di dispositivi che permettono l'uso delle identità digitali degli internauti e dei dispositivi connessi alle reti appartenenti a terzi inconsapevoli.

Tutela del *know-how*, penetrazione e spionaggio

Pur costituendo la protezione delle infrastrutture critiche informatizzate *target* prioritario per l'intelligence, atteso che un'aggressione alle stesse è potenzialmente in grado di danneg-

giare o paralizzare il funzionamento dei gangli vitali dello Stato, il monitoraggio informativo svolto nel corso del 2013 ha consentito di rilevare come la concentrazione degli eventi cibernetici di maggior rilievo si sia tradotta in un significativo incremento di attività intrusive finalizzate all'acquisizione di informazioni sensibili e alla sottrazione di *know-how* pregiato. Ciò in danno del patrimonio informativo di enti governativi, militari, ambasciate, centri di ricerca, nonché di società operanti nei settori aerospaziale, della difesa e dell'energia, anche di fonte alternativa.

Quanto al *modus operandi*, tali attività hanno consentito di rilevare il prevalente ricorso a *malware* già noti e sovente reingegnerizzati. All'elevato livello di organizzazione e sofisticazione raggiunto dagli attaccanti, anche in ragione della loro crescente capacità di combinare sinergicamente diverse tipologie di vettori di penetrazione, ha fatto da contrappeso, da parte dei soggetti *target*, la scarsa percezione della minaccia e della necessità di adeguate contromisure.

Cyber crime e relativo impatto economico

La ricerca info-operativa non ha mancato di registrare episodi di sottrazione informativa, specie di natura finanziaria, da parte della criminalità organizzata. Significative, in tale ambito, le acquisizioni attestanti il rapido accrescimento di vettori di attacco verso piattaforme mobili, segnatamente quelle di *mobile banking;* la diffusione di siti *web* dannosi o infetti per la distribuzione di *malware*; il lancio in elevati volumi di campagne di *spam*, finalizzate a promuovere false offerte commerciali; l'inoculazione nei sistemi degli utenti di codici maligni (emblematici quelli occultati all'interno di *file* allegati ad *e-mail* ed indirizzati a *target* remunerativi, il cd. *spear phishing*); il massiccio impiego di *ransomware* ovvero del blocco di un sistema a scopo di riscatto.

Particolarmente indicativi sono apparsi, poi, i segnali del coinvolgimento di realtà criminali in attività di spionaggio industriale – finalizzate alla sottrazione di brevetti industriali, piani aziendali, studi e ricerche di mercato, analisi e descrizioni dei processi produttivi, etc. – attività di cui non si esclude una committenza da parte di *competitor*.

Il costante monitoraggio dell'attivismo informatico di matrice criminale va ricondotto al rilevante impatto economico che lo stesso è in grado di generare, specie nei sistemi-Paese come l'Italia, per i quali il furto di *know-how* scientifico, tecnologico ed aziendale è in grado di condizionare la capacità di rimanere innovativi e competitivi nei mercati internazionali.

Contribuisce a rendere ancor più insidiosa la minaccia di stampo criminale il frequente reinvestimento dei cospicui capitali illecitamente ottenuti nella ricerca di nuove vulnerabilità dei sistemi *target* e nello sviluppo di strumenti più sofisticati e performanti per il loro sfruttamento.

box 1

IL MERCATO *CYBER UNDERGROUND* E IL *BITCOIN*

Il costante monitoraggio del fenomeno rivela la tendenza ad una sempre maggiore sofisticazione di tecniche e strumenti utilizzati per gli attacchi. La disponibilità di questi dispositivi è sovente resa accessibile anche a chi non disponga di competenze specialistiche, grazie ad un fiorente mercato nero.

Si tratta del cd. mercato *underground*, presente nel *deep web*, dove è possibile acquistare servizi di ogni tipo che si estendono dalla sottrazione di dati agli strumenti per perpetrare un attacco o per attuare un'attività illegale verso o attraverso lo spazio cibernetico.

In tale contesto, assumono particolare rilevanza anche la disponibilità di strumenti di regolazione finanziaria e tecniche che permettono di garantire l'anonimato e la non tracciabilità delle transazioni, quali la rete TOR o simili, ed il crescente impiego della moneta digitale denominata *bitcoin* (*vds.* capitolo *Le dinamiche economico-finanziarie*).

L'attività info-operativa svolta ha consentito di confermare la stretta relazione tra le dinamiche delineate e il cd. *computer crime market*, quale settore appetibile e redditizio sia per singoli *hacker*, sia per organizzazioni criminali che continuano ad alimentare un mercato nero ove è possibile smerciare contenuti illegali (stupefacenti, materiale pedopornografico o protetto da *copyright*) e strumenti per compiere, in proprio o con il supporto degli stessi gruppi criminali, reati contro il patrimonio (truffe, ricatti, estorsioni, furti, etc.), sottrazione di dati sensibili e d'identità (ad esempio a fini di riscatto o per perpetrare altri reati), riciclaggio di capitali illeciti, giochi d'azzardo e scommesse illegali (*vds. box 1*).

Il dominio cibernetico, quale veicolo comunicativo e cassa di risonanza, ha offerto spazio anche ad espressioni del disagio sociale che, amplificate dalla crisi economica, hanno trovato concretizzazione in chiave di *antagonismo digitale* a scopo propagandistico o anche solo dimostrativo. In tale ambito, significativo è stato l'incremento dei *raid* effettuati da gruppi *hacktivist* che hanno ampliato anche la rosa dei potenziali *target* (*vds. box 2*). Con le loro azioni hanno mirato a catturare l'attenzione delle grandi platee al di fuori della primaria cerchia di contatti, nel tentativo di trasformare la rete da strumento in teatro di iniziative propagandistiche. Molteplici sono state le tipologie di attacco ideologicamente motivate, con intento sostanzialmente dimostrativo, il cui principale obiettivo è stato

box 2

L'*HACKTIVISM*: EVOLUZIONE DEL FENOMENO

L'hacktivismo – principalmente riconducibile al movimento *Anonymous* – ha registrato, nel periodo novembre-dicembre 2013, un'evoluzione relativamente a:

- motivazione: dalla lotta per la libertà di informazione sulla rete ad offensive di più marcata ispirazione antagonista (ad es. le campagne a sostegno dei movimenti NO TAV e NO MUOS), concretizzata anche attraverso l'indirizzo delle attività ostili verso temi e personaggi di primo piano della politica e delle istituzioni italiane (operazione "OpItaly");
- incremento del potenziale offensivo: da attacchi di tipo DDoS e *Web-Defacement* si è passati al SQL *Injection* (immissione di codici in grado di estrapolare informazioni da un *data base*) nonché all'impiego di *worm* e a tecniche di *spear-phishing*, finalizzate alla sottrazione di dati sensibili per la loro successiva pubblicazione *on-line* (cd. *dataleak*).

quello di creare danni d'immagine e/o alla funzionalità temporanea di sistemi e reti. Si è trattato, in particolare, di attacchi *Distributed Denial of Service* (DDoS), che attraverso il coordinato utilizzo da remoto di reti di computer di utenti inconsapevoli (*botnets*) hanno provocato il sovraccarico dei *server*, e di *Web Defacements* per alterare dati di un determinato sito a fini disinformativi, di calunnia o semplice dileggio. In altri, residuali casi, è stato rilevato il ricorso a *malware* per sottrarre, rendendoli di pubblico dominio, dati di proprietà di Governi, aziende o singoli individui.

Le acquisizioni informative hanno evidenziato che il possesso di sofisticate capacità informatiche è limitato ad una cerchia ristretta di individui, costituenti lo "zoccolo duro" del movimento, mentre la maggior parte dei simpatizzanti dello stesso dispone di scarse abilità tecniche.

L'antagonismo in chiave digitale

L'antagonismo digitale si è inoltre rivelato strumentale alle proteste di piazza. Significativo, al riguardo, l'attacco lanciato *on-line* contro siti *web* governativi ed istituzionali dagli hacktivisti italiani di *Anonymous* in concomitanza con la manifestazione romana di ottobre *per il diritto alla casa e contro la crisi* (*vds.* capitolo *Strumentalizzazioni estremiste e minaccia eversiva*). In questo senso, l'azione cibernetica sembra pertanto destinata ad entrare a pieno titolo nel panorama del dissenso antagonista come innovativo e complementare strumento di "*lotta*".

Sul piano previsionale, il crescente sviluppo di reti e di sistemi basati su tecnologie dell'informazione e della comunicazione se, da una parte, si porrà quale moltiplicatore di diversificate opportunità di crescita, dall'altra, continuerà a generare una serie di criticità per lo spazio cibernetico, potenzialmente lesive per la sicurezza sia nazionale che internazionale. Tenuto conto di ciò, una delle sfide con la quale sarà chiamata a confrontarsi l'intelligence è rappresentata dal contribuito che dovrà essere garantito alla sicurezza ed alla protezione della sempre più consistente mole di dati personali, anche di particolare sensibilità (sanitari, giudiziari, etc.), destinati ad essere custoditi e trattati con servizi accentrati quali il *cloud computing* (la cd. "*nuvola*").

PAGINA BIANCA

LE DINAMICHE ECONOMICO-FINANZIARIE

L'azione dell'intelligence sul versante economico-finanziario è stata sviluppata in uno scenario estero caratterizzato da persistenti fattori di incertezza e da un diffuso rallentamento dello sviluppo, che ha riguardato non solo le economie avanzate, ma anche, in linea tendenziale, quelle emergenti.

Vulnerabilità del Paese

Il contesto nazionale è risultato connotato dal protrarsi della debolezza congiunturale. Nel terzo trimestre 2013, secondo i dati disponibili (*vds.* Istat, *Conti nazionali*), la contrazione del Prodotto Interno Lordo (PIL) si è arrestata; il livello dell'attività produttiva è rimasto però inferiore dell'1,8 per cento rispetto allo stesso periodo del 2012. Nel medesimo arco temporale, la spesa delle famiglie è diminuita del 2 per cento, gli investimenti fissi lordi del 5,1 per cento, le importazioni dell'1,2 per cento. È rimasto elevato il tasso di disoccupazione, che nel mese di novembre 2013 era pari al 12,7 per cento, contro il 10,9 per cento medio dell'Unione Europea a 28 (*vds.* Istat, *Rilevazione sulle forze di lavoro*). Particolarmente colpita è la categoria dei giovani sotto i 24 anni: il 41,6 per cento di coloro che cercano un'occupazione non riesce a trovarla, quasi il doppio rispetto ai coetanei europei.

Questo è il contesto nel quale l'intelligence è stata chiamata ad operare. In continuità con il 2012 e con un ulteriore affinamento nella individuazione dei *target* dell'attività informativa, l'impegno degli Organismi si è concentrato nel prevenire e depotenziare i diversi fattori di rischio, che possono trovare nelle vulnerabilità di attori economici nazionali e nel disagio sociale potenziali spazi di attecchimento con riflessi tanto sulla sicurezza naziona-

le quanto sulle prospettive di sviluppo del Sistema Paese.

L'azione informativa si è dipanata lungo tre direttrici:

- concorrere alla tutela del Sistema Paese rispetto a minacce in grado di significativamente depauperare la competitività tecnologica ed infrastrutturale nazionale, di incidere sulla continuità degli approvvigionamenti energetici, nonché di alterare la solidità del sistema creditizio e finanziario;
- individuare fattori di rischio inediti derivanti dall'utilizzo strumentale, per finalità destabilizzanti, di nuove tecnologie come pure dalla utilizzazione di sistemi di pagamento sempre più aperti alla dimensione globale dei traffici;
- contrastare forme pervasive di interazione ed alterazione della libera concorrenza e degli investimenti economici discendenti da pratiche di evasione ed elusione fiscale su larga scala, nonché dalle molteplici proiezioni criminali nel tessuto produttivo nazionale con un associato fenomeno di riciclaggio.

Opportunità e rischi delle acquisizioni estere

Nel corso dell'anno si è protratta la stretta creditizia al settore privato: secondo gli ultimi dati della Banca d'Italia, riferiti a novembre 2013, i prestiti alle famiglie sono calati dell'1,5 per cento su base annuale, quelli alle imprese del 6 per cento (Banca d'Italia, *Supplementi al bollettino statistico, Indicatori monetari e finanziari – Moneta e banche n. 1 anno XXIV del 10 gennaio 2014*). Si tratta di indici particolarmente negativi, anche rispetto a quanto osservato nei già critici mesi precedenti. Unita alla riduzione dei margini di redditività delle aziende, questa circostanza ha aumentato l'esposizione di realtà produttive italiane, comprese le Piccole e Medie Imprese (PMI), alle mire acquisitive di multinazionali estere, attratte per un verso dal relativo patrimonio tecnologico e, dall'altro, dal portafoglio clienti del *made in Italy* nonché, più in generale, dalla possibilità di accedere a nuovi mercati di sbocco.

Il fenomeno ha presentato anche indubbi profili di opportunità per l'Italia, che negli ultimi anni ha risentito di un indebolimento dell'attrattività rispetto ai capitali stranieri; negli ultimi anni, in questo specifico versante, sono migliorate non solo le più grandi economie europee, come la Francia e la Germania, ma anche quelle di Paesi con un PIL inferiore a quello italiano, come il Belgio, la Spagna e i Paesi Bassi.

Nella prospettiva di aprire ulteriormente il Paese alla globalizzazione, è stato varato il piano "Destinazione Italia", un insieme coerente di misure che mirano a riformare un ampio spettro di settori per l'attrazione, la promozione e l'accompagnamento degli investimenti esteri e per favorire la competitività delle imprese italiane.