crisi economico-finanziaria, dalla contrazione dei consumi da parte delle economie maggiormente avanzate, nonché dalle strategie poste in essere da alcuni consumatori di rilievo (pubblici e privati di rilevante dimensione) per diversificare fonti energetiche e mercati di approvvigionamento. In questo contesto, possono giocare un ruolo importante alcuni fattori, quali:

- le *policy* dei principali detentori di risorse energetiche, i quali, a causa della generalizzata contrazione dei consumi avvertita in ambito OCSE, sembrano aver conferito maggior impulso alle iniziative per diversificare i tradizionali mercati di sbocco e la propria economia dal cd. "settore *oil*";
- lo sviluppo delle tecnologie che favoriscono lo sfruttamento di risorse presenti in aree di difficile accesso, rendendo possibile il trasporto delle stesse, l'interconnessione energetica tra Paesi consumatori e l'incremento dell'efficienza energetica da parte dei sistemi economico-industriali dei principali produttori;
- l'adozione di soluzioni in grado di incidere in misura significativa sulle attuali dinamiche energetiche globali come, ad esempio, l'ottimizzazione dei processi estrattivi del cd. *shale* gas, l'estrazione e la lavorazione dei cd. greggi ultra pesanti, le evoluzioni e relative applicazioni nel campo del nucleare ad usi civili e delle energie rinnovabili;
- la crescente competizione internazionale per l'accesso e lo sfruttamento di idrocarburi e materie prime energetiche utili al processo di diversificazione dai combustibili fossili (Litio);
- gli avvenimenti riguardanti i principali Paesi produttori o di transito delle risorse destinate in Italia. Tra le variabili più critiche figurano:
  - la cornice di sicurezza in Nigeria, in vista delle elezioni, calendarizzate per l'aprile 2011. Le consultazioni saranno precedute, con tutta probabilità, da un significativo incremento della tensione politica, con ricadute sul piano sociale e dell'ordine pubblico. Particolare rilevanza assumerà il confronto tra le componenti politico-sociali del Nord (rappresentative delle popolazioni musulmane) e quelle del Sud (in maggioranza espressione delle popolazioni cristiane e animiste), con il rischio di inserimenti terroristici ad opera di formazioni jihadiste. La sensibilità del contesto potrebbe riflettersi sulla stabilità nelle regioni del Delta del Niger, con nuove "saldature di interessi" – se non di intenti – tra organizzazioni di matrice essenzialmente criminale e ambienti irredentisti locali, determinati a perseguire i propri obiettivi – in chiave più o meno separatista/autonomista – anche con il ricorso all'uso della forza;
  - le incidenze sui programmi di sviluppo nel settore degli idrocarburi dell'accresciuta pressione della Co-

munità Internazionale verso la Repubblica Islamica dell'Iran;

- l'evolversi delle tensioni in alcuni Paesi produttori (es. Iraq, Sudan), tra le Autorità centrali e quelle locali, per la gestione delle risorse e/o la ridistribuzione dei proventi derivanti dalla commercializzazione delle stesse, con ricadute negative sull'approvvigionamento energetico nazionale. Nella realtà sudanese, in particolare, dopo il referendum che ha sancito la volontà di indipendenza del Sud Sudan, resta l'incognita sulla regione petrolifera di Abyei, che potrebbe riaccendere le tensioni con Khartoum;
- il rischio di nuove tensioni nel Caucaso ove, a Nord, potrebbe inasprirsi il confronto tra Mosca e i movimenti separatisti locali e, a Sud, restano difficili le relazioni russo-georgiane.

le infiltrazioni criminali in ambito nazionale ...

Il fattore d'incidenza più insidioso per il nostro sistema economico-produttivo resta la criminalità organizzata, sempre attenta alle evoluzioni di scenario che possano profilare opportunità di guadagno illecito.

Sono in effetti aumentati i tentativi di infiltrazione in numerosi settori dell'economia legale, in particolare legati alla produzione di energie rinnovabili e allo smaltimento dei rifiuti, talora con la complicità di amministratori locali e imprenditori del territorio.

Rimane invariata inoltre la capacità delle organizzazioni criminali di infiltrarsi nei "tradizionali" settori:

- dell'edilizia, sia privata sia pubblica, attraverso la gestione del ciclo del cemento, del movimento terra, dei trasporti e di ogni altro servizio connesso;
- della grande distribuzione, con nuove concentrazioni al Nord;
- della sanità pubblica e privata, dove frequente è la collusione con soggetti professionali e/o istituzionali locali;
- turistico-alberghiero, specialmente nelle aree della Sicilia e della Calabria a ciò destinabili;
- delle opere pubbliche, relative anche alle ricostruzioni in Abruzzo.

Nel mezzo di una fase di forte recessione economica – condizione in sé propizia per le attività di usura e di riciclaggio – un'ulteriore prospettiva di rischio è rappresentata dalla possibilità che i profitti derivanti dai traffici illeciti gestiti dalle organizzazioni criminali possano confluire nei capitali sociali di istituti di credito in via di costituzione. Ciò, oltre a rappresentare un pericoloso inquinamento dei mercati bancari e finanziari, può determinare l'acquisizione da parte della criminalità (eventualmente mediata attraverso società-schermo residenti in Paesi *off shore*) di rilevanti quote dell'economia reale, fino a ricomprendere addirittura società d'interesse strategico per l'economia nazionale.

... e in ambito internazionale

Anche con riferimento ai circuiti economico-finanziari internazionali,

le organizzazioni criminali sembrano aver acquisito crescente capacità d'infiltrazione. Uno specifico elemento di rischio è rappresentato dal dinamismo e dalla trasversalità delle organizzazioni criminali, sviluppate attraverso *network* delocalizzati, estremamente mobili, specializzati e flessibili nella struttura e nell'impiego, in questo agevolati dalla diffusione delle moderne tecnologie informatiche di rete che, attraverso servizi innovativi quali l'*on-line banking* (*home* e *mobile banking*), generano rilevanti flussi finanziari e offrono, pertanto ampie opportunità per movimentare denaro anche di provenienza illecita.

Va evidenziato, in proposito, l'aumento, a livello internazionale, dei cd. "*white collar crimes*", riferibili ad ambienti imprenditoriali/professionali svincolati da collegamenti con la criminalità organizzata propriamente detta, ma da questa utilizzati.

I capisaldi del crimine economico restano, da un lato, l'impiego di articolati schermi societari, regolarmente localizzati in Paesi a fiscalità agevolata, dall'altro, lo sfruttamento delle carenze legislative e di controllo in taluni Stati, anche comunitari, nonché – per alcune piazze estere – gli intrecci tra ambienti politico-istituzionali, potere economico e gruppi criminali (vds. box 4).

i rischi per le aziende italiane all'estero

Il quadro sopra delineato è suscettibile di penalizzare il sistema Paese con riferimento alle aziende italiane proiettate in processi di integrazione e sviluppo all'estero. Il rischio di interagire con entità economiche espressioni di capitali illeciti sussiste sia negli ambiti territoriali caratterizzati da fisiologiche vulnerabilità (instabilità politico-istituzionale,

Box 4

Le evidenze emerse attestano come, sempre più spesso, **EVASIONE E RICICLAGGIO**, in quanto fenomeni intimamente connessi, facciano appello alle medesime risorse, agli stessi circuiti finanziari, ad analoghi metodi e intermediari. Più in particolare, il riciclaggio di denaro di illecita provenienza si attua, sostanzialmente, facendo affiorare nell'economia valori di origine delittuosa, dopo aver conferito loro una parvenza di liceità. Tale denaro, una volta immesso nel circuito legale, viene generalmente dichiarato alle autorità fiscali con la conseguenza che, in questo modo, esso acquisisce un ulteriore velo di legittimità (cd. "*fiscal excuses*"). Al contrario, il compimento di condotte di evasione (soprattutto se di carattere fraudolento) comporta la messa in atto di un procedimento inverso in base al quale il denaro, questa volta di provenienza lecita, anziché riemergere, viene occultato per essere sottratto alla pretesa erariale.

scarsa trasparenza dei processi di transizione economica e di privatizzazione) sia in quei contesti in apparenza "affidabili" ma che, di fatto, risultano anch'essi funzionali al perseguimento di finalità illecite.

In Paesi dell'Europa centro-orientale e della regione balcanica, mercati dove da tempo operano numerose aziende nazionali, permangono criticità connesse alla presenza di gruppi affaristici internazionali collegati sia a sodalizi criminali sia ad apparati di sicurezza stranieri.

La circostanza, apparentemente fisiologica in alcune realtà, conferma la necessità di una mirata attività di intelligence diretta a verificare, in alcuni casi, se le iniziative di *holding* internazionali verso realtà economiche nazionali rispondano effettivamente a regolari dinamiche di mercato, ovvero siano originate da finalità "distorsive".

finanziamento a terrorismo

In tema di circuiti finanziari e con specifico riferimento a canali di trasferimento di valuta che potrebbero essere sfruttati per finalità illecite, incluso il finanziamento di organizzazioni terroristiche, si conferma la crescente rilevanza dei sistemi "alternativi" di trasferimento fondi quali, ad esempio, quelli "informali" denominati *hawala* e *euro to euro* (vds. box 5) che, a differenza del *money transfer* – sottoposto a stringenti controlli – possono muoversi al di fuori della normativa vigente.

I sistemi "informali", utilizzati da alcune componenti impiegate per trasferire capitali nell'area di origine, trovano ampio impiego in talune piazze estere e in specifi-

Box 5

Il sistema **HAWALA** (in arabo ordine di pagamento, cambio o assegno), molto diffuso nel mondo islamico, è un circuito bancario parallelo che consente il trasferimento di denaro senza comportarne la movimentazione fisica. Si basa sul versamento di somme a intermediari – legati in genere a vincoli di natura amicale o familiare – che, dietro pagamento di una commissione, garantiscono la consegna di un equivalente importo in valuta locale da parte di un proprio incaricato già stanziato nel Paese di destinazione.

Il sistema ***EURO TO EURO*** invece, utilizzato in particolare dalla comunità nigeriana, si sviluppa attraverso una rete di raccolta del contante strutturata su "sportelli" distribuiti sul territorio nazionale, in genere all'interno di "propri" esercizi commerciali. Ad ognuno di questi corrisponde un ufficio in Nigeria presso il quale le somme "affidate" in Italia possono essere incassate dopo ventiquattro ore. All'utente che spedisce il denaro viene rilasciata una ricevuta riportante una *password*, comunicata al destinatario per il ritiro del contante in Patria. I gestori dei centri di raccolta in Italia provvedono poi a trasferire i soldi in Africa attraverso porta valori della stessa nazionalità.

che realtà si sono rivelati funzionali a circuiti di illegalità. Esemplificativo, al riguardo, il caso dell'Afghanistan, dove la sussistenza di un sistema bancario poco sviluppato ha favorito il radicamento di una fitta rete di operatori "informali" (agenzie di *money exchange* e *hawaladors*) strettamente interconnessa con il narcotraffico, primaria fonte di sostentamento dei gruppi insorgenti, nonché con omologhi circuiti informali operanti nei Paesi contermini e in *hub* finanziari internazionali che fungono da vere e proprie "stanze di compensazione" per numerosi operatori provenienti dall'area afghano-pakistana.

In altri casi, si osserva come i flussi finanziari "illeciti" vengano veicolati attraverso gli stessi circuiti bancari con l'adozione di tecniche di "frazionamento" che consentono di polverizzare il volume delle transazioni, ovvero mediante l'interposizione di soggetti "terzi", i cui profili non presentano particolari "anomalie" o palesi collegamenti con le liste "antiterrorismo".

2. *Cyber threat*

Di potenziale impatto sul sistema Paese e sulla stessa sicurezza nazionale, la minaccia cibernetica (vds. box 6) si conferma una sfida crescente per le politiche di sicurezza degli Stati, e sollecita pertanto il diretto coinvolgimento degli apparati d'intelligence, la massima sinergia tra settori pubblici e privati e la più ampia collaborazione internazionale.

Box 6

Con la dizione di ***CYBER THREAT*** si intende genericamente il complesso delle attività controindicate condotte tramite reti e sistemi ICT (*Information and Communication Technology*) e/o contro di essi da una gamma diversificata di attori.

A seconda delle finalità (criminali o *lato sensu* politiche) e degli attori (statuali o meno) gli attacchi cibernetici vengono poi classificati come atti di cibercriminalità, di ciberterrorismo ovvero di vera e propria guerra cibernetica (*cyber warfare*).

Si tratta di una minaccia che, sebbene riferita al mondo intangibile del *cyber space*, presenta ormai tratti di estrema concretezza. Il settore ICT ha infatti assunto negli anni un peso crescente per l'economia e la società, registrando una crescita esponenziale sia delle apparecchiature fisse e mobili che si connettono ora alla rete in *wireless*, sia del volume e della sensibilità delle informazioni scambiate.

Tale settore ha la peculiare caratteristica di costituire un'infrastruttura critica in sé e di rappresentare, al contempo, il nervo portante delle altre infrastrutture critiche.

La diffusione delle reti di comunicazione e informazione digitali conferisce poi una "dimensione cibernetica" anche a settori di attività che siamo abituati a pensare slegati dal *cyber space*, ampliando il novero degli ambiti esposti alla minaccia.

È significativo, al riguardo, che le attività digitali rappresentino talvolta anche strumenti impiegati dai regimi per reprimere il dissenso, acquisendo una spiccata valenza ai fini della politica estera internazionale.

le preoccupazioni della NATO

Non è un caso che il nuovo concetto strategico della NATO, adottato in novembre a Lisbona dai Capi di Stato e di Governo dell'Alleanza Atlantica, impegni i Paesi membri a potenziare la capacità di prevenire, individuare, difendersi e riprendersi ("*recover*") da attacchi informatici, ritenuti potenzialmente in grado di minacciare la prosperità, la sicurezza e la stabilità nazionale ed euroatlantica.

le iniziative del Governo

In linea con gli impegni assunti a Lisbona e in conformità alle raccomandazioni espresse in luglio dal Comitato Parlamentare per la Sicurezza della Repubblica, l'Autorità di governo – che agli

inizi dell'anno ha posto la *cyber threat* tra gli obiettivi prioritari dell'attività informativa – ha promosso una serie di iniziative, incluso un apposito esercizio interministeriale, allo scopo di approfondire i molteplici aspetti della minaccia e pervenire alla più adeguata strategia di prevenzione e contrasto.

gli attori della minaccia

Tra gli aspetti peculiari della *cyber threat* figura l'ampio e diversificato *range* di soggetti da cui può provenire un attacco informatico: non più solo singoli *hacker* ma anche gruppi terroristici e criminali, mentre il vero dato emergente è la riconosciuta aggressività, per quanto sovente indiretta, di attori statuali.

cyber space e *cyber war*

L'aumentata consapevolezza, a livello globale, delle potenzialità e dei rischi della rete informatica si è accompagnata alla diffusa percezione dello spazio cibernetico quale possibile "campo di battaglia" (in questo senso si parla di "militarizzazione" della rete).

Il *cyber space* è, infatti, sempre più considerato – dopo terra, mare, cielo e spazio – il "quinto dominio" della difesa militare. Va evidenziata la potenziale gravità del pericolo al quale risulterebbe inevitabilmente esposta, nell'eventualità di un attacco informatico, la struttura economico-produttiva (per sua stessa natura "aperta" verso l'esterno) dei vari Paesi tecnologicamente più avanzati. Ciò in considerazione della "dipendenza informatica" di questi ultimi, che sono capaci di sviluppare e gestire strutture informatiche complesse ma, proprio per questo, sono inevitabilmente esposti a gradienti di rischio direttamente proporzionali al livello di informatizzazione raggiunto. Non può essere sottaciuto, al riguardo, l'accelerato sviluppo di strumenti di attacco sempre più moderni ed efficaci. Esemplificando, una nuova frontiera sembrerebbe costituita dai *virus* "asintomatici", di origine tuttora ignota, che sono in grado di cancellare le proprie tracce e di creare con estrema rapidità *botnet* (reti di computer infettati). Analoga capacità offensiva avrebbe l'ancor più recente "*Stuxnet*", definito da molti il "primo *super-virus* di classe *malware* completamente nuova", una sorta di "missile cibernetico cerca e distruggi".

i nuovi *virus*

La "militarizzazione" delle reti informatiche si presenta, in sintesi, come un processo nel cui ambito vanno già delineandosi due diverse strategie di utilizzo che assumono – di volta in volta ed a seconda delle necessità – carattere difensivo o offensivo.

le strategie di utilizzo

L'iniziativa di maggior sostanza operativa appare, al momento, quella adottata dagli Stati Uniti con la costituzione di un apposito Ente, dedicato esclusivamente alla materia, il *Cyber Command*. La struttura ha un vasto organico ed è stata attivata definitivamente il 1° ottobre. Nel quadro della generale revisione di *policy* recentemente disposta dall'Amministrazione statunitense, è previsto il coinvolgimento di tutte le forze armate del Paese, in base al principio che

gli USA e il *Cyber Command*

individua "in ogni militare un futuro combattente cibernetico" e che non esclude la possibilità, ove necessario, di "attacchi preventivi".

La messa in moto di questa imponente macchina organizzativa potrebbe rappresentare un importante riferimento per tutti gli altri Stati dell'Alleanza Atlantica e il monitoraggio dei suoi sviluppi operativi costituisce un imprescindibile punto di partenza per la definizione delle molteplici questioni, anche di ordine politico e diplomatico, connesse all'impiego delle tecnologie informatiche.

la vicenda *Google*

Vicende, come quella di *Google* in Cina, destinate ad alimentare un acceso confronto all'interno dell'opinione pubblica internazionale e del più vasto ambiente dei cibernauti, rimandano alle difficoltà di contemperare l'esigenza, da un lato, di difendere gli interessi della Comunità nazionale e internazionale riconoscendo un ruolo più incisivo alle entità statuali; dall'altro, di continuare a garantire la libertà e la riservatezza degli utenti sul *web*.

Seppure non propriamente inquadrabile tra le ipotesi di attacco informatico, analogo dibattito potranno innescare gli sviluppi del caso *Wikileaks*, ove il *know how* tecnologico si è coniugato con la capacità di incunearsi tra le maglie di una rete di comunicazione avvalendosi, verosimilmente, del concorso attivo di individui interni alla stessa rete.

L'entusiasmo travolgente con il quale la società moderna, ad ogni livello di applicazione, ha deciso di affidare all'informatica l'evoluzione della propria capacità di comunicazione quando non addirittura gli strumenti di analisi della realtà circostante, lascia ben celata la minaccia intrinsecamente contenuta in un universo tecnologico del quale soggetti ostili sembrano aver compreso appieno le enormi potenzialità offensive. La sempre più vasta letteratura specializzata e la stessa crescente casistica delle violazioni valgono a testimoniare il particolare attivismo di alcuni attori nello sviluppare sistemi in grado di penetrare il patrimonio di conoscenze e di *know how* organizzativo degli altri Paesi.

una sfida da raccogliere

Conclusivamente, è ragionevole ritenere che per l'immediato futuro la sfida più impegnativa sul piano della prevenzione e del contrasto sarà rappresentata proprio dalla minaccia cibernetica, che verosimilmente continuerà ad "evolvere", anche in relazione alla sua capacità di concretizzarsi in maniera efficace, selettiva, anonima, senza limiti di tempo e di distanza.

Tale scenario, che può comprendere anche attacchi su larga scala, sollecita una risposta mirata, tempestiva, integrata e multisettoriale.

Per quanto riguarda il nostro Paese, non possono non richiamarsi le citate raccomandazioni del Comitato Parlamentare per la Sicurezza della Repubblica, che ha sottolineato la necessità di una pianificazione strategica a livello nazionale e di un impianto organizzativo che assicuri "il coordinamento tra gli attori interessati", anche attraverso la "ridefinizione delle attività delle strutture esistenti" ed una "rimodulazione delle attuali competenze e responsabilità".