SICUREZZA È LIBERTÀ

INTELLIGENCE
E CULTURA DELLA SICUREZZA
A DIECI ANNI
DALLA RIFORMA

GNOSIS. RIVISTA ITALIANA DI INTELLIGENCE

DIRETTORE
Mario Parente
DIRETTORE RESPONSABILE
Gianfranco Linzi

Coordinatore editoriale
Paolo Scotto di Castelbianco
Direttore della Scuola di formazione

Prima edizione dicembre 2017
Roma, Dat Donat Dicat srl 2017

SOMMARIO

Paolo Gentiloni
Un modello di intelligence moderna per le sfide dell'Italia 9-15

Alessandro Pansa
A dieci anni dalla legge 124/2007.
Un bilancio e uno sguardo al futuro 17-23

Giacomo Stucchi
Il sistema della sicurezza nazionale tra unitarietà,
partecipazione e nuove sfide 25-29

Mario Rasetti
Big Data e sicurezza nazionale 31-37

Gaetano Manfredi
Alleanza strategica tra intelligence e università 39-43

Franco Anelli
Università e analisi strategica. Lo studio di nuovi modelli
geostrategici 45-49

Paola Severino
Le garanzie funzionali degli appartenenti ai Servizi.
Un bilancio a dieci anni dalla legge 124/2007 51-57

Gianmario Verona
La definizione di interesse e sicurezza nazionale
economico-finanziaria in epoca digitale 59-63

Elda Morlicchio
Una nuova stagione di studi sull'Africa.
Partenariato tra intelligence e università 65-71

Massimo Bergami
Imprese e sicurezza nazionale 73-79

Francesco Profumo – Ettore Bompard
La sicurezza energetica nazionale.
Dimensioni, culture e strumenti 81-89

Donatella Sciuto
Internet of Things.
Rischi e opportunità per la sicurezza nazionale 91-97

Roberto Baldoni
Partenariato intelligence. Ricerca ai fini della sicurezza
cibernetica nazionale 99-105

Michele Colajanni
Evoluzione della minaccia cibernetica e delle relative capacità
di reazione e risposta 107-113

Antonino Alì
Evoluzione della normativa sulla sicurezza nazionale
a dieci anni dalla legge 124/2007 115-121

Alessandro Colombo
La tutela dell'interesse nazionale
nel nuovo sistema internazionale 123-129

Luciano Bozzo
La trasformazione delle metodologie di previsione strategica
e di costruzione di scenari 131-137

Lida Viganoni
Il ritorno della Geografia
nella prospettiva della sicurezza nazionale 139-143

Marina Brogi
Rischio cibernetico e sicurezza nazionale
nel sistema finanziario 145-151

Gustavo Piga
L'internazionalizzazione dei mercati e la tutela dell'interesse
economico-finanziario nazionale 153-159

Eugenio Lo Sardo
In un foglio l'evidenza 161-165

Mario Caligiuri
Il percorso evolutivo degli studi sull'intelligence in Italia 167-173

UN MODELLO DI INTELLIGENCE MODERNA per le sfide dell'Italia

Paolo Gentiloni

Un contesto temporale particolare, quello dei dieci anni dal varo di una legge che ha ridisegnato e razionalizzato in profondità l'assetto e il funzionamento dei Servizi segreti nazionali, offre l'opportunità di tracciare un bilancio su come e sino a che punto sia stato possibile avvalersi di uno strumento che è strategico per sua natura. Se non vi è dubbio che la componente informativa rappresenti sempre, insieme con il monopolio legittimo della forza, un elemento essenziale per salvaguardare l'indipendenza, l'integrità e la sicurezza dello Stato e la connotazione democratica delle nostre istituzioni, al contempo l'ambiente globale nel quale ci si trova a operare rende questa azione di presidio delicata e complessa.

Oggi quanto mai la sicurezza è una conquista quotidiana, non può in nessun momento essere data per scontata. La riflessione sul percorso compiuto in questi anni è pertanto molto opportuna per consolidare i risultati raggiunti e, allo stesso tempo, per attrezzarsi ad affrontare le incognite del futuro. Può essere svolta utilmente attorno a due concetti: i valori e le scelte.

Dott. Paolo Gentiloni, presidente del Consiglio dei ministri.

Dalla prospettiva che la nostra stessa identità nazionale ci detta, la nozione di «valore» si articola in tre dimensioni. Vi è, prima d'ogni altro, il valore supremo della democrazia che, nel nostro caso, comporta doveri che travalicano il compito, pur imprescindibile, della difesa delle istituzioni che la incarnano da possibili azioni ostili. Occorre continuare a mantenere l'Italia nella posizione, che la caratterizza, di grande equilibrio nel garantire assieme, come armoniose endiadi, sicurezza e libertà, sicurezza e privacy, riservatezza e trasparenza, senza mai cadere nella tentazione di scorciatoie illusorie e pericolose. Non è comprimendo la libertà dei cittadini che si contrasta efficacemente il terrorismo, non è sacrificando la protezione dei dati personali che si può perseguire la sicurezza cibernetica, non è con la segretezza fine a se stessa che gli Organismi informativi possono preservare gli interessi nazionali nel perimetro stabilito dall'ordinamento e in sintonico confronto con l'organismo parlamentare di controllo.

I «valori» vanno, altresì, riaffermati nella proiezione internazionale del nostro Paese. La costruzione di società democratiche, pluraliste, inclusive e aperte alla diversità rappresenta, oltre che un imperativo etico, anche la migliore garanzia di pace e stabilità e, in quanto tale, un tassello basilare di un più ampio esercizio di responsabilità volto a promuovere e ad assicurare una tutela efficace dei diritti umani e delle libertà fondamentali. Questa è l'architrave della nostra politica estera, alla quale siamo determinati a continuare a riferirci, anzitutto grazie a un forte, costante ancoraggio alla cornice e al sistema di rapporti delle Nazioni Unite, dell'Unione europea e della Nato. Che non va messo in discussione, ma non è in sé sufficiente, e non solo a causa della necessità di perseguire obiettivi divenuti oramai impellenti: riavvicinare il progetto comunitario alle menti e ai cuori degli europei, tornare a rendere cruciale il ruolo dell'UE nel mondo, corroborare la centralità dell'Alleanza Atlantica anche sul terreno del contrasto alle nuove sfide ibride.

La priorità italiana è infatti anche un'altra, in ragione della nostra geografia e della nostra storia: quella della stabilizzazione, dello sviluppo sostenibile e della crescita dell'area del Mediterraneo e del continente africano. È una priorità da perseguire con un'accorta combinazione di obiettivi immediati e strategie di più lungo periodo.

L'Italia è, in questo, facilitata dalle politiche di dialogo e cooperazione con tutti gli attori regionali, attuate e maturate nei decenni senza mai rinunciare alla sua fisionomia euro-atlantica. Nondimeno la stabilità dell'area Broader Middle East and Northern Africa rimane il più ambizioso fra i traguardi della politica estera nazionale, il cui raggiungimento postula anche un concorso informativo continuo da parte dell'intelligence, di elevatissima qualità operativa e analitica. Questo aspetto è peraltro essenziale per poter imbastire, con i nostri partner, rapporti di collaborazione leali e produttivi anche fra le

rispettive Agenzie di informazione e sicurezza, che è auspicabile siano sempre più intensi sul versante dell'info sharing. Vi è, infine, il «valore aggiunto» che il sistema Paese è in grado di esprimere per fronteggiare l'attuale forte competizione fra Stati sul terreno economico, che rammenta il dovere di proteggere la nostra comunità produttiva, di difendere gli assetti strategici e il patrimonio scientifico e tecnologico dai quali dipendono, oggi, il rafforzamento del ciclo di crescita economica e, in un domani tutt'altro che lontano, la capacità nazionale di muoversi lungo le frontiere più avanzate dell'innovazione industriale.

Se amici e partner sono anche concorrenti, ciò non vuol dire che si debba abdicare alla promozione del libero scambio e a politiche di convinta apertura a quegli investimenti esteri che generano occupazione e sviluppo. Né comporta che si debba essere partecipi di forme di nazionalismo aggressivo, nelle quali non ci riconosciamo e che non ci appartengono. Significa, piuttosto, che non possiamo farci trovare indifesi, che dobbiamo essere forti della nostra coesione sistemica sia sul piano informativo che dell'integrità delle nostre reti e dell'imprescindibile collaborazione fra istituzioni.

Nessuno di questi tre valori è nuovo per noi. Nel loro insieme essi sostengono quelle grandi scelte di fondo che disegnano il volto più autentico della nostra storia repubblicana. Eppure è l'idea di 'scelta' ad assumere oggi un significato duplice, poiché del tutto nuovi sono i termini nei quali si è indotti a declinare quei valori da un ambiente planetario che si contraddistingue per il suo essere sempre più imprevedibile e interconnesso.

Per rimanere fedeli alle nostre scelte fondamentali, dobbiamo ogni giorno assumere decisioni contingenti, molte volte ardue, ma sempre ineludibili per adeguarci alla continua mutevolezza degli scenari e a minacce globali per provenienza, trasversali per settori interessati e asimmetriche per attori ostili. La sfera nazionale e quella internazionale s'intrecciano in nodi sovente intricati e interdipendenti. Le minacce possono colpirci a casa nostra pur avendo origini lontane, possono essere interne ma riferirsi a fenomeni globali, assumono talvolta le fattezze apparenti di vulnerabilità circoscritte pur potendo comportare pericoli gravi per la tenuta dell'intero sistema Paese.

C'è un solo modo per rispondere alla grammatica della complessità: ragionare con la sintassi della conoscenza, essere informati a sufficienza per essere sicuri il più possibile.

Ed è precisamente questa la funzione dell'intelligence.

La forte instabilità del quadro geopolitico e le conseguenze sociali ed economiche della globalizzazione non impediscono di contribuire in maniera virtuosa ai processi di governance globale, ma a condizione che si disponga di strumenti analitici che permettano d'individuare in tempo utile le insidie, anche quelle non immediatamente percepibili.

La frammentazione delle catene globali del valore, la mobilità estrema del mercato dei capitali, la condivisione transnazionale delle infrastrutture strategiche non precludono la possibilità di puntare sull'innovazione e di ampliare le prospettive occupazionali per i nostri giovani, ma a patto di discernere con avvedutezza rischi e opportunità.
Non siamo affatto condannati a combattere il terrorismo al prezzo di somigliargli. Va tenuto presente che, di fronte al suo manifestarsi in maniera inedita e alla sua imprevedibilità, l'esperienza che abbiamo accumulato nei decenni è un bagaglio, sì, assolutamente prezioso, ma da sola non basta.
Occorre, in particolare dopo la sconfitta militare del Daesh, un costante supporto informativo che permetta di agire su tutti i necessari livelli di contrasto, a cominciare dai canali di diffusione della propaganda jihadista, dai processi di radicalizzazione, addestramento ed emulazione in internet, dalle fonti di finanziamento delle varie organizzazioni terroristiche. Devono essere incoraggiate forti sinergie fra intelligence e Forze di polizia che, nel caso italiano sono già consolidate e virtuose, ma che dovrebbero stabilirsi anche su scala più ampia. La cornice dovrebbe essere quella di una grande alleanza strategica, che coinvolga i Governi, le Agenzie di intelligence e di law enforcement, le Autorità giudiziarie, l'industria del web e la società civile. È la direzione verso cui l'Italia si è adoperata in questo anno di Presidenza del G7.
E, infine, ci si può comunque impegnare per cercare di governare grandi fenomeni epocali destinati a protrarsi nei decenni, come le migrazioni, purché essi siano conosciuti e compresi nelle cause prime e nei loro contorni reali. Serve, di conseguenza, che si lavori tutti assieme. E a tale scopo è necessario che, nel groviglio odierno di interessi e di insidie, ci si riesca ad accordare su quale sia l'interesse nazionale, ossia su ciò che debba essere difeso e promosso senza arrecare danno all'intera collettività.
Questo è il compito supremo della politica. Ma sarebbe illusorio pensare che il Governo – a fronte della novità e complessità dei problemi – possa da solo circoscrivere l'interesse nazionale, oltre che proteggerlo e sostenerlo. È agli Organismi informativi che spetta segnalare le criticità, fornire informazioni sostanziali, stimolare un continuo raffronto di prospettive e di idee, scandagliare senza sosta tutto quel che può mettere a repentaglio la nostra sicurezza.
Riletto oggi in questa luce, il provvedimento legislativo che dieci anni fa riformò l'intelligence nazionale può vantare, a buon diritto, una straordinaria modernità. E in effetti, pur in un panorama di minacce frattanto molto mutato per pervasività, novero e sofisticazione, il Paese può fare affidamento su uno strumento pienamente in grado di rispondere alle avversità del mondo in cui viviamo.
È una conquista preziosa, frutto del concorso di tre fattori.

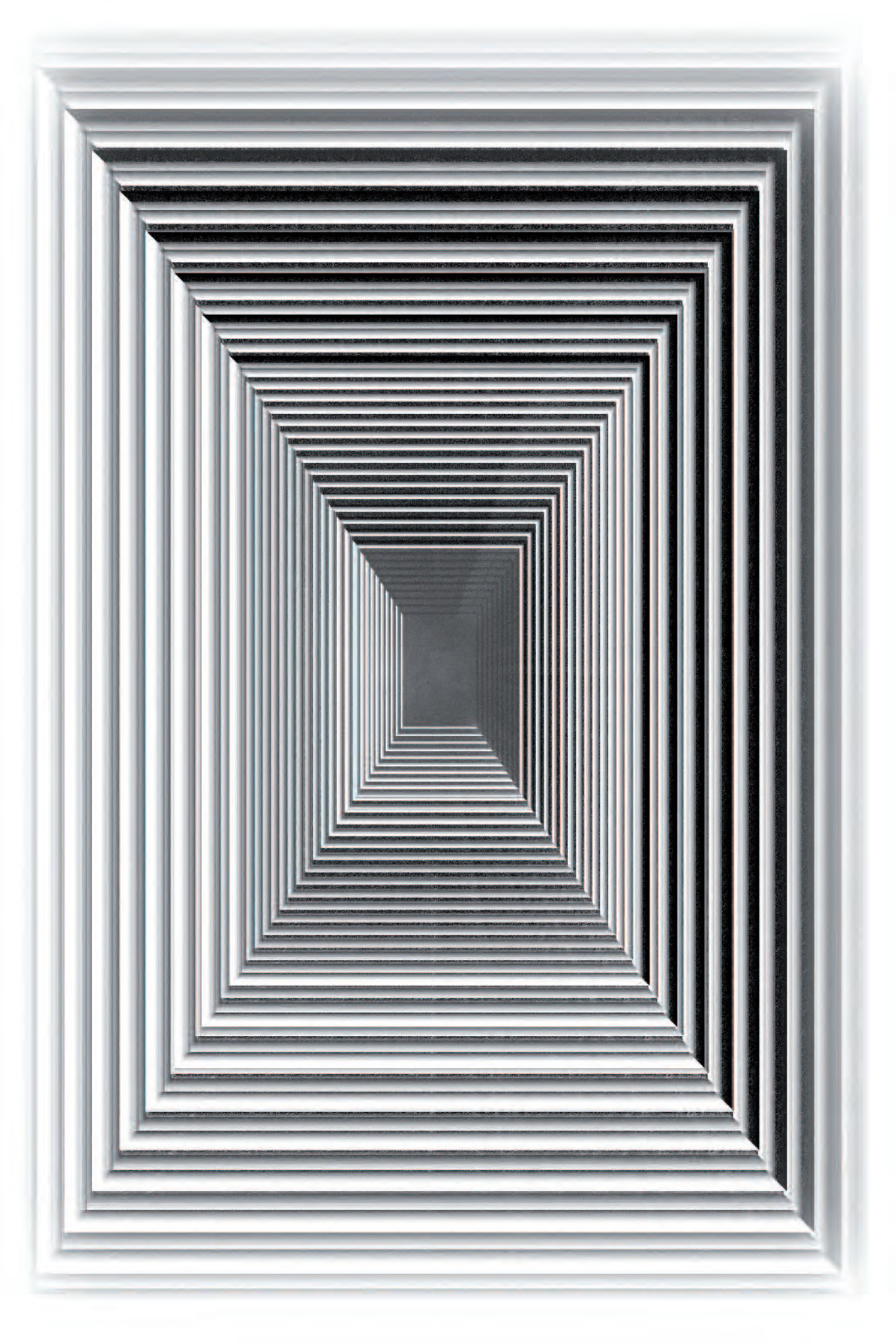
Lo si deve, anzitutto, all'abnegazione e alla professionalità straordinarie, di assoluta eccellenza, di tutto il personale del Dis, dell'Aise e dell'Aisi, dedito al suo servizio coltivando il valore della riservatezza, attitudine non facile e non scontata in questa temperie.
Lo si deve, certamente, alle decisioni legislative e regolamentari intervenute in questi anni, anche grazie all'impulso fruttuoso del Comitato parlamentare per la sicurezza della Repubblica (Copasir), che hanno aggiornato e migliorato la legge, ampliando altresì progressivamente il perimetro giuridico dell'azione dell'intelligence.
Lo si deve, prima ancora, alla validità perdurante dell'intuizione del Legislatore, che intervenne in profondità sull'architettura organizzativa e funzionale dell'intelligence, affinché i Servizi segreti potessero svolgere al meglio i loro peculiari compiti, che si articolano su due piani strettamente interconnessi.
L'uno prende corpo nell'abilità di anticipare le tendenze evolutive e le correlate minacce a tutti gli ambiti in cui si declina la sicurezza nazionale – dunque non solo quelli tradizionali, politico e militare, ma anche quelli economici, scientifici e industriali – analizzandoli e contestualizzandoli, allo scopo di consentire al Governo di agire in chiave preventiva. Va evitato che le sfide attuali si avvitino su se stesse e che, in avvenire, se ne configurino di ulteriori e più difficili. Devono essere gestiti i diversi frangenti di crisi e conflitto. Si deve stimolare, là dove necessaria, la coesione della comunità internazionale. Va riservata l'attenzione necessaria anche ai fenomeni di radicalizzazione interna, latenti ma che possono, tuttavia, essere spinti a riaffiorare da fattori di tensione sociale.
L'altro si sostanzia nell'azione sul campo, nel risolvere, con gli strumenti non convenzionali che dell'intelligence sono propri, specifiche situazioni critiche, in stretto raccordo con le Forze dell'ordine nel nostro territorio e, nei teatri di crisi, con le Forze armate, là dove sono presenti contingenti nazionali.
Centrale per l'assolvimento di queste funzioni, nell'assetto concepito dieci anni orsono, è il ruolo del Comitato interministeriale per la sicurezza della Repubblica (Cisr). Ha lavorato molto bene, anche in forza dell'attività svolta nel formato tecnico con il prezioso apporto del Dis, dell'Aise e dell'Aisi.
È stato possibile avvalersi in maniera straordinariamente feconda della visione olistica dei problemi di cui il Comitato è naturale detentore per la messa a punto delle priorità e delle linee di indirizzo, e per innescare sui dossier di sicurezza una logica di sistema e di convergenze.

Peraltro, in virtù di una modifica della legge 124/2007 che ha individuato, per l'appunto, nel Cisr l'organismo deputato alla gestione delle emergenze di sicurezza nazionale, nonché delle importanti novità intervenute nella normativa comunitaria, si è operato per rimodulare in maniera radicale e innovativa l'architettura per la protezione cibernetica e la sicurezza informatica nazionali, che costituiscono precondizioni fondamentali per lo sviluppo del nostro Paese. Il Dpcm, a mia firma, del febbraio scorso, è da considerarsi l'esito, sin qui culminante, di un processo riformatore snodatosi nel decennio, improntato a principi di coordinamento, raccordo, sinergia e collaborazione internazionale. È stato per di più costante, nel contesto complessivo, lo sforzo di affinamento delle attività di formazione della comunità intelligence. Non si è trattato di un impegno fine a se stesso, piuttosto di una componente assai qualificante per la costruzione di collaborazioni strutturate con il mondo dell'Università e della ricerca, utili per l'arricchimento reciproco sul terreno della conoscenza.

Va quindi reso pieno merito ai Vertici della nostra intelligence e a tutte le donne e gli uomini che con loro collaborano, ai professionisti di lungo corso e ai talenti più giovani reclutati in questi anni, di aver assolto sino in fondo il mandato loro affidato: non soltanto negli ambiti della raccolta informativa e della sua valorizzazione analitica, ma pure nella politica di apertura verso la società civile e nei partenariati con gli attori privati.

L'istituzione si è così guadagnata la fiducia dell'opinione pubblica, facendo della trasparenza un obiettivo concreto e della promozione della cultura della sicurezza uno strumento importante per indurre nei cittadini e nelle imprese la percezione corretta della portata delle sfide che bisogna affrontare.

Il modello di intelligence sul quale l'Italia può contare è esattamente quello di cui ha bisogno.



A DIECI ANNI DALLA LEGGE 124/2007

UN BILANCIO E UNO SGUARDO AL FUTURO

Alessandro Pansa

È orientamento largamente, se non unanimemente, condiviso quello di valutare in termini molto positivi il bilancio dei dieci anni trascorsi dal varo della legge 7 agosto 2007, n. 124 che ha riformato l'intelligence nazionale. Lo si deve anzitutto al fatto che in tale provvedimento trovò espressione una grande scelta culturale, prima ancora che legislativa: quella di emancipare i Servizi segreti dall'alveo angusto della cultura della segretezza, per consentire loro di operare in un mondo che non si esauriva più nel planisfero delle frontiere fisiche e che richiedeva una nuova cultura della sicurezza diffusa e partecipata a tutti i livelli, dal circuito istituzionale al tessuto produttivo e imprenditoriale, dalla comunità scientifica e accademica alla società civile.

Fu una scelta rivoluzionaria. Che è cosa ben distinta da una rivoluzione. A compiersi nel 2007 fu, piuttosto, una cesura fondamentale in un lungo processo riformatore che ha abbracciato decenni di storia repubblicana ed è proseguito sino a oggi, senza che mai – è bene ricordarlo – si sia fermata la macchina operativa, sempre evitando che i tempi di messa a regime delle trasformazioni di volta in volta intervenute stingessero sulla prontezza di risposta.

Non si ripudiò l'eredità dell'assetto precedente né si disconobbe il suo portato valoriale. Al contrario, si ripartì dai risultati che si erano nel frattempo consolidati e si cambiò come era necessario fare, cioè radicalmente.

Pref. Alessandro Pansa, direttore generale del Dis.

Sotto questo profilo, l'intelligence nazionale è uno degli esempi meglio riusciti di apprendimento esperienziale, ossia della capacità di rispondere al cambiamento col cambiamento, di agire per miglioramenti progressivi e perfezionamenti successivi, allo scopo, nel nostro caso, di fornire un servizio sempre diverso perché sempre adeguato a esigenze che sono mutevoli per natura. Un cammino che merita di essere ripercorso, non come esercizio fine a se stesso, ma per meglio comprendere dove siamo, nonché per fissare nuovi traguardi, ispirati all'opportuna combinazione di ambizione e realismo.
La sicurezza nazionale è infatti un bene supremo e immateriale in evoluzione continua, del quale si avverte sino in fondo l'importanza solo quando viene a mancare. Di conseguenza, in una democrazia i Servizi segreti devono 'servire' a vigilare costantemente sulla società aperta e a difendere le condizioni dalle quali dipende il suo sviluppo. Il grimaldello della vigilanza è la conoscenza. Non v'è, del resto, virtù pubblica o privata che non origini dalla conoscenza, e ciò vale a più forte ragione per quell'istituzione che è chiamata precisamente a ottemperare al dovere cruciale di trasformare le informazioni in conoscenza. In tal senso, molto v'era stato di proficuo nell'ordinamento che per un trentennio e sino al 2007 aveva retto l'intelligence. Era stato stabilito – grazie a una rafforzata linea giurisprudenziale costituzionale – il suo indispensabile collegamento diretto con il decisore politico, che fino al 1977 era mancato. Era stato sancito, sul piano legislativo e organizzativo, che il suo compito deve consistere non soltanto nella ricerca, ma anche: nella lettura dei fenomeni; nell'analisi delle informazioni non altrimenti disponibili e utili al processo decisionale dell'Esecutivo in materia di sicurezza nazionale; nel contributo alla definizione di strategie di contrasto adeguate.
Dieci anni fa i tempi erano però maturi per scrivere una nuova pagina, per mettersi al passo con l'evoluzione della minaccia. Le strutture sino allora operanti non avevano nel loro Dna l'abilità di agire nell'era della globalizzazione. All'epoca in cui quelle Agenzie erano nate e si erano formate ed evolute, la globalizzazione non esisteva e non aveva ancora esercitato il suo impatto dirompente non solo sulla tecnologia e sulle professioni, ma anche sul modo di pensare degli individui, sulla cultura, sulla postura strategica delle Nazioni, sul significato dell'interesse cruciale e sul concetto stesso di sicurezza nelle sue varie accezioni, perciò anche sulla sicurezza nazionale. Si era passati dalla visione geopolitica dei localismi a quella dei globalismi, sino ad arrivare all'inedita dimensione *glocal*, mentre il terrorismo internazionale andava assumendo fattezze e dinamiche nuove, con un'evoluzione che dal punto di rottura dell'11 settembre sarebbe culminata nel pericolo inusitato posto dal Daesh, che ha insanguinato anche il suolo europeo. Il carattere globale delle minacce e delle incognite non era, in sé, una novità né positiva né negativa: era molto differente dal passato e, come tale, andava affrontato con strumenti rinnovati

e risposte adeguate. Esigeva, soprattutto, coerenza e unitarietà nel discernimento dei rischi per la sicurezza come nella prevenzione e nella reazione. Tanto che la forte convergenza sia politica che tecnica, nella quale si tradusse la volontà di cambiamento, ci fa comprendere nitidamente come la nozione di unitarietà del Comparto non fosse semplicemente una costruzione organizzativa, ma una precisa volontà del potere legislativo, rispondente alla consapevolezza maturata. Una nozione allora nuova, oggi patrimonio acquisito e proiettato nel futuro.

Le architravi della legge 124 concepite dieci anni fa sono riassumibili in due parole chiave: il «sistema», perno ingegneristico e interpretativo vuoi dell'impianto, vuoi delle successive direttrici attuative della riforma; il «controllo», a garanzia di trasparenza e di legittimità democratica.

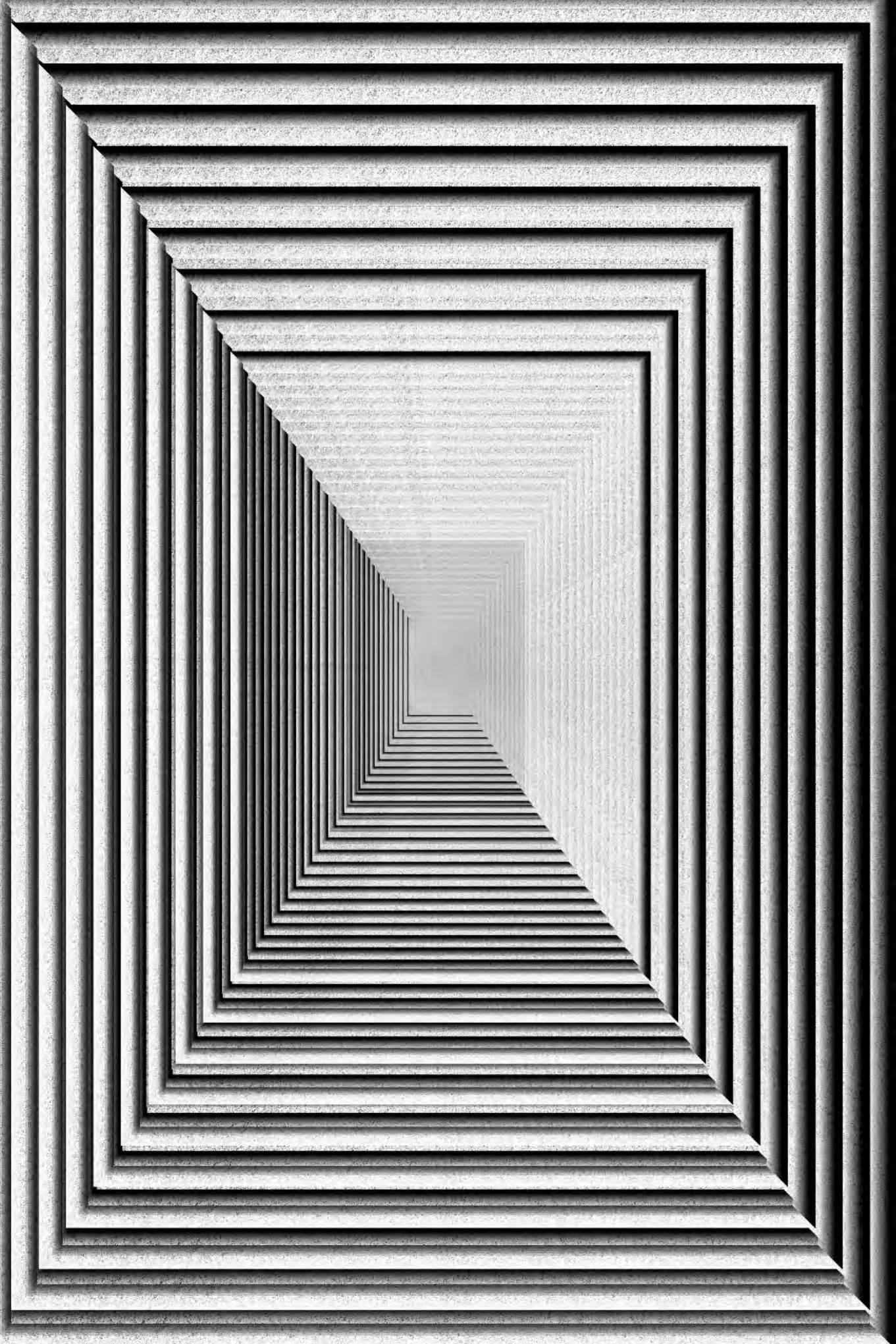
Quanto alla prima, la gittata del provvedimento è misurabile con l'ampia elencazione d'interessi alla cui tutela l'intelligence è stata chiamata a concorrere fornendo al Governo il suo supporto informativo. Le finalità delle attività di ricerca attribuite ad Aise e Aisi hanno visto ampliarsi il loro spettro, non più limitato alla difesa dell'indipendenza, dell'integrità e della sicurezza interna ed esterna della Repubblica e delle sue istituzioni democratiche, ma esteso agli interessi economici, industriali e scientifici del Paese. È stata in tal modo sanzionata la prima declinazione legislativa dell'interesse nazionale in un perimetro ampio, riferibile non più alla mera difesa degli elementi costitutivi dello Stato Ordinamento, bensì allo Stato-comunità, a uno spazio nel quale si muovono soggetti pubblici e privati.

Incaricata di proteggere il sistema Paese, l'intelligence si è per prima fatta sistema. Nella sua architettura organizzativa e nella sua catena di comando: due Agenzie con finalità e missioni separate e circoscritte su base non più tematica ma geografica, e un coordinamento forte in capo al Dis. Nel modus operandi: volto, appunto, a 'mettere a sistema', ad assicurare coerenza e fruibilità a tutte le informazioni disponibili, essendo compito principale dei Servizi segreti quello di organizzare nella sequenza corretta i dati, per poi riscontrarli, ponderarli e decifrare in anticipo e con rapidità le intenzioni e le strategie degli attori ostili. Nel tessuto connettivo delle sue relazioni: il Sistema di informazione per la sicurezza della Repubblica quale Pubblica amministrazione, collegata con le altre e, come le altre, tenuta a operare rigorosamente in base alla legge pur svolgendo attività non convenzionali, in una quotidianità fatta di stretta collaborazione con le Forze di polizia e le Forze armate e di vicinanza alla magistratura.

Parimenti, a salvaguardia dello Stato-comunità, l'intelligence non è più solo un 'apparato', ma anche una comunità di tre Organismi fra loro integrati che lavorano in maniera coesa e unitaria, un insieme di parti che si muovono in armonia fra loro per conseguire il fine comune.

Il controllo è stato il secondo muro maestro dell'edificio riformatore, poiché concepito e articolato in termini assai più estesi rispetto al quadro normativo precedente. È stato previsto nel Comitato parlamentare per la sicurezza della Repubblica (Copasir) un soggetto di alto livello politico-istituzionale impegnato nella verifica rigorosa e continuativa della rispondenza dell'attività degli Organismi informativi al dettato costituzionale e legislativo e all'esclusivo interesse della Repubblica. È nel Copasir che la riprova quotidiana dell'equilibrio fra sicurezza e libertà, imprescindibile in ogni democrazia, trova il suo alveo naturale.
A specifici obblighi di comunicazione nei confronti del Comitato corrispondono funzioni consultive e incisivi poteri di controllo. Basti il dato delle oltre 180 audizioni svoltesi nella presente legislatura a significare tanto il clima di leale collaborazione e sintonia instauratosi negli anni, quanto l'intensità dei rapporti, caratterizzati dalla virtuosa congiunzione fra il rigore nell'azione di vigilanza e lo spirito costruttivo e propositivo.
È su questi due pilastri che gli altri concetti cardine della riforma hanno potuto prendere forma concreta e hanno potuto improntarsi ai principi di trasparenza e di legittimità democratica: la responsabilità politica, accentrata nel vertice di Governo; la collegialità, assicurata dal Comitato interministeriale per la sicurezza della Repubblica (Cisr); la temporalizzazione del segreto di Stato, poiché se è all'interesse nazionale che 'i Servizi servono', i segreti possono rimanere tali per un periodo, non per sempre; il criterio della 'doppia chiave' per lo svolgimento di condotte illecite, che da allora richiede l'assunzione di responsabilità del potere esecutivo e insieme la verifica del potere giudiziario; la promozione della cultura della sicurezza; una politica di selezione del personale rivolta non solo ai quadri della Pubblica amministrazione ma anche ai giovani talenti; un vero e proprio patto con l'Accademia, bacino indispensabile per la contaminazione dei saperi e, al contempo, per mettere in campo le professionalità migliori.
La legge 124 è stata sin da subito messa alla prova e lo è stata nella sua essenza, vale a dire nell'idea di approccio integrato alle diverse minacce alla sicurezza nazionale. E, se vi è una dimensione che più delle altre presuppone una risposta organica, è quella della sicurezza cibernetica, che pertanto ha sostanziato, giocoforza, l'ambito naturale di verifica della riforma, in particolare su due terreni: da una parte, il binomio fra solidità e flessibilità al cambiamento dell'impianto legislativo; dall'altra, l'amalgama di strumenti, professionalità e sinergie istituzionali che tale impianto postulava. Elementi entrambi irrinunciabili, in un mondo dove gli avanzamenti tecnologici pongono problemi che si rivelerebbero ingovernabili qualora non si investisse adeguatamente in cybersicurezza.

Quanto al primo aspetto, lungo un sentiero attuativo marcato da un altissimo tasso di condivisione delle decisioni legislative e regolamentari, che ha visto il Copasir svolgere il suo ruolo consultivo in maniera straordinariamente feconda, tappa cruciale è stata quella di metà percorso, allorché il provvedimento del 2007 è stato affinato e completato, addirittura all'unanimità in ambo le Camere, al fine di rafforzare le attività di informazione a tutela delle infrastrutture critiche e della sicurezza informatica.
Grazie alla pietra miliare rappresentata dalla legge 7 agosto 2012, n. 133 già l'anno dopo è stato possibile disegnare una prima architettura nazionale, con un decreto del presidente Monti al quale vanno ascritti meriti importantissimi, specie in termini di accrescimento, oltre che della capacità di risposta, della consapevolezza diffusa, nel quadro della Pubblica amministrazione e al di fuori della sua cornice, circa la portata della minaccia cyber.
Da quella esperienza si è ripartiti per mettere a punto, quest'anno, un nuovo decreto col quale il presidente Gentiloni ha disposto l'ulteriore, ampio ammodernamento della filiera di reazione, dettato dalle travolgenti evoluzioni intervenute nel frattempo, che hanno reso abnorme l'asimmetria tra la facilità di accesso alla rete e l'onerosa difficoltà della sua difesa.
Il nuovo provvedimento ha rafforzato il ruolo del Cisr e ha disposto che il Nucleo sicurezza cibernetica, ora ricondotto all'interno del Dis, assicuri la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale in raccordo con tutte le strutture dei ministeri competenti in materia.
Questi sono gli importanti risultati raggiunti sinora. Eppure la velocità delle trasformazioni è destinata a costituire la cifra più autentica del futuro che ci attende. Ed è la seconda pietra di paragone del testo normativo varato dieci anni orsono. Già oggi siamo alle prese con scenari sino a poco tempo fa impensabili: solo nel 2016, le informazioni caricate in internet hanno superato in dimensione la quantità di conoscenza trasmessa dall'inizio dell'umanità sino al 2015, mentre è nelle banche dati di privati che viene detenuto il sapere digitale del mondo intero.
Dovremo muoverci lungo confini nuovi e sconosciuti che, verosimilmente, arriveranno a riplasmare i nostri paradigmi culturali e, forse, persino i principi alla base del diritto positivo.
Merita frattanto evidenziare che, per rispondere a dinamiche di questa magnitudine, il connubio fra l'uomo e la tecnologia è certamente essenziale, ma a condizione di non dimenticare mai che il fattore umano sarà quello decisivo, quello che farà davvero la differenza. Vinta la scommessa della riforma, la vera sfida per i Servizi segreti del futuro sarà quella di adeguarsi alla velocità del cambiamento. Se la flessibilità è la chiave di volta per interpretare gli imperativi dell'avvenire, il capitale più importante per l'intelligence è quello umano, quello che nel gergo specialistico si definisce Humint.



Gli investimenti in tecnologia rimarranno fondamentali, ma spetterà ai professionisti degli Organismi informativi avvalersene con il dovuto bagaglio di competenze e abilità. Servirà sempre di più, allo scopo, un sapere trasversale e multidisciplinare, utile a decrittare trend globali che vedranno la digitalizzazione, oramai intrinseca al pensare e all'agire umano, incidere sugli equilibri planetari, sui rapporti di forza, sui vantaggi competitivi e sulla distribuzione internazionale dei fattori di produzione.

Cambierà la tecnologia ma, come accaduto più volte sin dall'89, muterà anche la geopolitica, che già oggi ci disorienta, segnata com'è da continue crisi. Se, per un verso, una sorta di rivincita della geografia fa riemergere antiche linee di frattura, per altro verso nuovi moltiplicatori di instabilità – riconducibili a scelte politiche, tensioni sociali, fattori religiosi, cambiamenti climatici – tendono a ridisegnare le frontiere e le costruzioni sovranazionali o, comunque, a metterle seriamente in discussione.

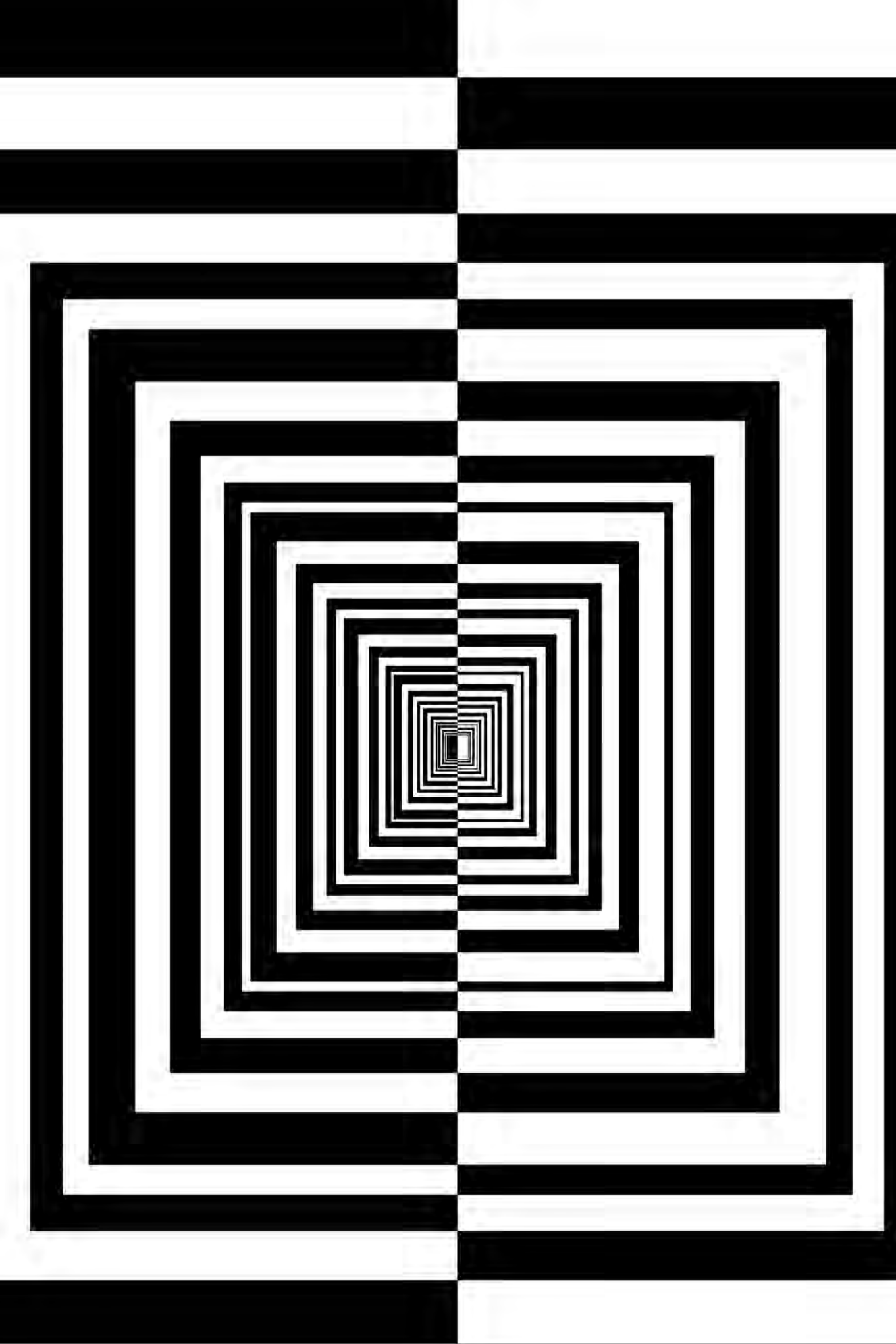
L'uomo, dunque, al centro di tutto, a cominciare dal nostro impegno costante su un duplice versante: la formazione e la promozione di una cultura della sicurezza generalizzata e sempre più matura. È, questa, una priorità irrinunciabile, sin qui perseguita con risultati notevoli, ma che adesso, nell'era del web e dei social media, va modernizzata e ripensata.

Occorre che anche l'intelligence faccia la sua parte rivolgendosi al terreno più fertile: quello delle menti dei giovani, ai quali la blogosfera offre una sconfinata prateria di libertà. La vivono, giustamente, come terreno d'elezione del loro essere 'cittadini digitali', come grande conquista del nostro tempo, dalla quale dipenderà il loro domani, e dalla quale non si torna indietro. I giovani devono essere incoraggiati nella loro fame di futuro, che spetterà comunque ai 'nativi digitali' costruire. Allo stesso tempo, è fondamentale che essi siano utenti consapevoli delle nuove tecnologie, che sviluppino autonome capacità di giudizio e anche, quando necessario, di autodifesa. A tale scopo, il Dis si accinge a lanciare una nuova iniziativa: la prima campagna nazionale cyber rivolta ai giovani.

In definitiva, se è chiaro dove eravamo prima e dove siamo potuti arrivare grazie alla riforma, è altrettanto chiaro dove dobbiamo andare ora.

L'imperativo, per le donne e gli uomini dell'intelligence, è quello di proseguire con coerenza e determinazione nel cammino che ieri li ha visti gestori di segreti, oggi li vede professionisti della sicurezza, domani, e più che mai, li dovrà vedere cittadini del mondo.

Questa è la fisionomia dell'intelligence sulla quale la Nazione dovrà, e sicuramente potrà, continuare a riporre pieno affidamento e convinta fiducia.



IL SISTEMA DELLA SICUREZZA NAZIONALE TRA UNITARIETÀ, PARTECIPAZIONE E NUOVE SFIDE

Giacomo Stucchi

Ai tempi di James Bond il mondo era più facile. Una scacchiera fatta di bianco e nero, con una visione 'a blocchi' che riconduceva tutto al registro amici / nemici. Oggi l'intelligence si confronta con realtà complesse e scenari fluidi che sollecitano resilienza, flessibilità, competenze accresciute in settori nuovi e sfidanti, approcci multidisciplinari e capacità di fare squadra. Occorre campo lungo per analizzare e processare una molteplicità di dati e affrontare le multiformi sfide globali alla sicurezza nell'era dei Big Data.

La questione non è solo prevenire ma dove *mettere muro* rispetto a minacce asimmetriche che provengono da avamposti senza confini. La bruciante attualità dei fenomeni migratori e della minaccia terroristica e cibernetica esige che gli apparati securitari facciano *sistema*, per trovarsi un passo avanti rispetto a essi. Per aggiornare il Governo sui potenziali target di manovre aggressive è indispensabile lavorare nei segmenti più avanzati, come l'analisi economico-finanziaria e la protezione cibernetica.

Sen. Giacomo Stucchi, presidente del Copasir.

Se le risposte sono state finora pronte e puntuali, lo si deve alla riorganizzazione del Comparto intelligence operata dalla legge 3 agosto 2007, n. 124, che si è espressa in termini di *sistema della sicurezza*. Le 'uova del Drago' impiegano tanto tempo a schiudersi ma poi danno vita a qualcosa di unico. Anche per riformare i Servizi segreti c'è voluto un lungo lavoro, ma i risultati hanno premiato l'impegno.
I 46 articoli che compongono la l. 124/2007 hanno dato nuovo volto e ossatura all'intelligence italiana, superando così la l. 801/1977. Pubblicata nella Gazzetta Ufficiale n. 187 del 13 agosto 2007, la norma istitutiva del Sistema di informazione per la sicurezza della Repubblica traccia una vision precisa, stabilendo come l'attività istituzionale dell'intelligence tuteli l'interesse nazionale. Il Comparto intelligence – strumento non convenzionale ma necessario per difendere i confini (non solo fisici) della nostra democrazia – si muove in un framework strategico e operativo profondamente incardinato nella normativa.
Le novità introdotte dalla l. 124/2007 hanno ricondotto la responsabilità politica e l'alta direzione al presidente del Consiglio ma anche al Comitato interministeriale per la sicurezza della Repubblica (Cisr). Hanno incardinato il coordinamento in capo al Dipartimento delle informazioni per la sicurezza (Dis), disegnando la mission dell'Agenzia informazioni e sicurezza esterna (Aise) e dell'Agenzia informazioni e sicurezza interna (Aisi), secondo un criterio di riparto territoriale. Nel nuovo terreno di lotta, l'intelligence lavora con specifica attenzione ai settori più moderni e, con la l. 124, ha aperto un dialogo con i cittadini: dalla cultura della segretezza si è passati alla cultura della sicurezza, in cui assume centralità il ruolo del Dis, al quale l'art. 4 affida, appunto, le «attività di promozione e diffusione della cultura della sicurezza».
In tale solco è stata istituita la Scuola di formazione del Comparto, che si occupa di aggiornamento, addestramento specialistico e tecnico-operativo del personale già in servizio presso Dis, Aise e Aisi anche attraverso collaborazioni con analoghe istituzioni della Pubblica amministrazione, università, centri studi, think net e think tank, sia in Italia sia all'estero. La Scuola degli 007 è un racconto d'intelligence moderna, ma anche il mondo universitario si è rivelato un alleato strategico, creando una rete in grado di migliorare la capacità di proiezione degli operatori della sicurezza. Dalle università, inoltre, sono state assunte risorse qualificate.
L'intelligence raccoglie informazioni e sostiene decisioni, ma la legge ne fa anche uno dei fattori di sviluppo della Nazione, ponendola a protezione degli interessi scientifici, industriali e strategici dell'Italia, come pure del know how delle sue imprese.

L'aggiornamento della l. 124 – non 'un tagliando' ma un'opportuna modifica – è arrivato con la l. 7 agosto 2012, n. 133 che, tra le altre disposizioni, all'art. 1 della l. 124 ha aggiunto il comma 3-bis: «Il Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali». Da notare anche l'art. 10, che modifica l'articolo 40 della l. 124 in materia di tutela del segreto di Stato, stabilendo che «Il Presidente del Consiglio dei Ministri, su richiesta del Presidente del Comitato parlamentare (Copasir), espone, in una seduta segreta appositamente convocata, il quadro informativo idoneo a consentire l'esame nel merito della conferma dell'opposizione del segreto di Stato». Un'altra sfida aperta è il web. La rete, espressa in forum jihadisti, blog e soprattutto social network, è diventata ovunque il mezzo più importante di diffusione e di comunicazione nel circuito jihadista. Per i terroristi che combattono in maniera asimmetrica sul web, Facebook, Twitter, Telegram e altri siti d'informazione sono «the Lifeblood of Daesh», linfa vitale. Il *jihad della parola*, tramite i processi mediatici, favorisce il proselitismo e la diffusione di messaggi per il potenziamento del *brand del terrore*. La strategia mediatica jihadista mira ad attivare dibattiti e creare U*mma virtuali*, sia in lingua araba che in altre lingue. Oggi obiettivi, modus operandi e mire di addestramento sono diversi dal pur recente passato. Le minacce vanno dai network terroristici ai lupi solitari, dall'uso di esplosivi al ricorso a coltelli e veicoli lanciati sulla folla, fino alla pratica e allo sfruttamento degli incendi. Scegliendo azioni low cost, che non necessitano di alcun tipo di formazione specifica, coloro che sono ispirati dai messaggi jihadisti che popolano la rete sono esortati a compiere azioni individuali ovunque si trovino e con qualunque mezzo. In tale contesto il web è ormai diventato un *virtual training camp* dove gli aspiranti jihadisti ricevono una preparazione interattiva, trovano suggerimenti e ispirazioni per azioni di terrorismo 'fai-da-te'. La Cyberwar contro il Daesh è fondamentale per evitare l'*attraversamento della linea* da parte di altri cyber-reclutati alla causa della bandiera nera. Appare strategico il ricorso a una *intelligence analisys on social profiles*. Negli appelli in rete, infatti, il Daesh parla anche al singolo jihadista che, non avendo la possibilità di recarsi nei territori controllati dal califfato, viene esortato a compiere ugualmente «una piccola azione nel cuore della loro terra» dal momento che «è più importante e più efficace che una grande azione in Medio Oriente». A prescindere dalle sigle e dai brand, la galassia jihadista sta assumendo la connotazione di un magma ispirato a una visione fondamentalista disposta ad attacchi soft e continui (la strategia dei mille tagli), pur di potenziare l'effetto terrore per destabilizzare gli equilibri dell'Occidente.

Se, da una parte, l'ambiente digitale offre possibilità alla radicalizzazione e all'offensiva terroristica, dall'altra, esso consente all'operatore della sicurezza di ricostruire le tracce della possibile eversione, risalendo la corrente del web: è qui che si apre anche il campo della Social Media Intelligence (Socmint) e la frontiera dei Big Data.

Da tempo il dibattito su questo nuovo spazio per la raccolta di informazioni rilevanti coinvolge due aspetti della questione, i contenuti e le relazioni, che portano a ricomprendere l'uso dei social nel ciclo di intelligence, magari con un passo in più proposto da studiosi quali Marco Lombardi: «Vanno dunque fuse la Socmint e la Humint, favorendo la nascita della loro sintesi in una nuova disciplina: la Digital Humint»[1].

Nel cyberspazio, la battaglia da vincere è quella della crittografia. Perché se è vero che il Daesh perde terreno a seguito di operazioni militari, la sconfitta della cyber propaganda jihadista richiederà un tempo più lungo e rinnovata capacità per prevenire e rispondere operativamente alla potenza di una minaccia che non ha confini né termine.

La sicurezza è il *primo valore* e dunque anche l'impiego delle garanzie funzionali per gli operatori dei Servizi è mirato alla sua tutela. In forza di tale *speciale causa di giustificazione*, di cui all'art. 17 della l. 124, non sono punibili gli agenti dell'Aise e dell'Aisi che, in presenza di determinati presupposti e in base a una specifica procedura autorizzatoria che fa capo al presidente del Consiglio o all'Autorità delegata, ove istituita, pongano in essere condotte astrattamente previste dalla legge come reato. Prima della l. 124, l'inchiostro del Legislatore – la legge era la n. 801/1977, per trent'anni la 'Magna Carta' dei Servizi – non aveva previsto questo tipo di tutela. Qualcuno potrebbe obiettare che per gli operatori dell'intelligence esisteva lo 'scudo' del segreto di Stato, ma la svolta – in termini di indirizzo politico e strategico per uno strumento non convenzionale come l'intelligence – è arrivata solo con la l. 124. La condotta delle donne e degli uomini dell'intelligence nazionale, che operano con «autorizzazione» del decisore politico, viene scriminata in funzione delle esigenze operative. Due i criteri fondamentali che reggono l'architettura delle garanzie funzionali e il loro ambito di applicazione: l'indispensabilità e la proporzionalità delle condotte al conseguimento degli obiettivi dell'operazione non altrimenti perseguibili.

Ogni operazione – che viene attivata dopo la dovuta previsione di possibili ipotesi di condotta di reato – è preliminarmente autorizzata. Ciò significa che le garanzie non sono poste in campo perché gli 007 facciano il bello o il cattivo tempo, ma per obiettivi istituzionali. Qui non c'entrano storie da *black rain* ma la capacità di agire 'in dinamico', come si dice nelle Agenzie.

1. M. Lombardi et al., *Dalla Socmint alla Digital Humint. Ricomprendere l'uso dei Social nel ciclo di intelligence*, in *Sicurezza, Terrorismo e Società*, «International Journal» 2 (2015), p. 100.

Oltre ad allungare il campo dell'operatività, questi strumenti consentono infatti di 'portare a casa' – e in sicurezza – dati e risultati, in un piano d'azione nel quale il fattore umano resta la vera chiave del successo. E il perimetro delle garanzie per i cittadini è assolutamente rispettato. Nessun agente ha – o potrà mai avere – 'licenza di uccidere' o potrà «ledere la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone».

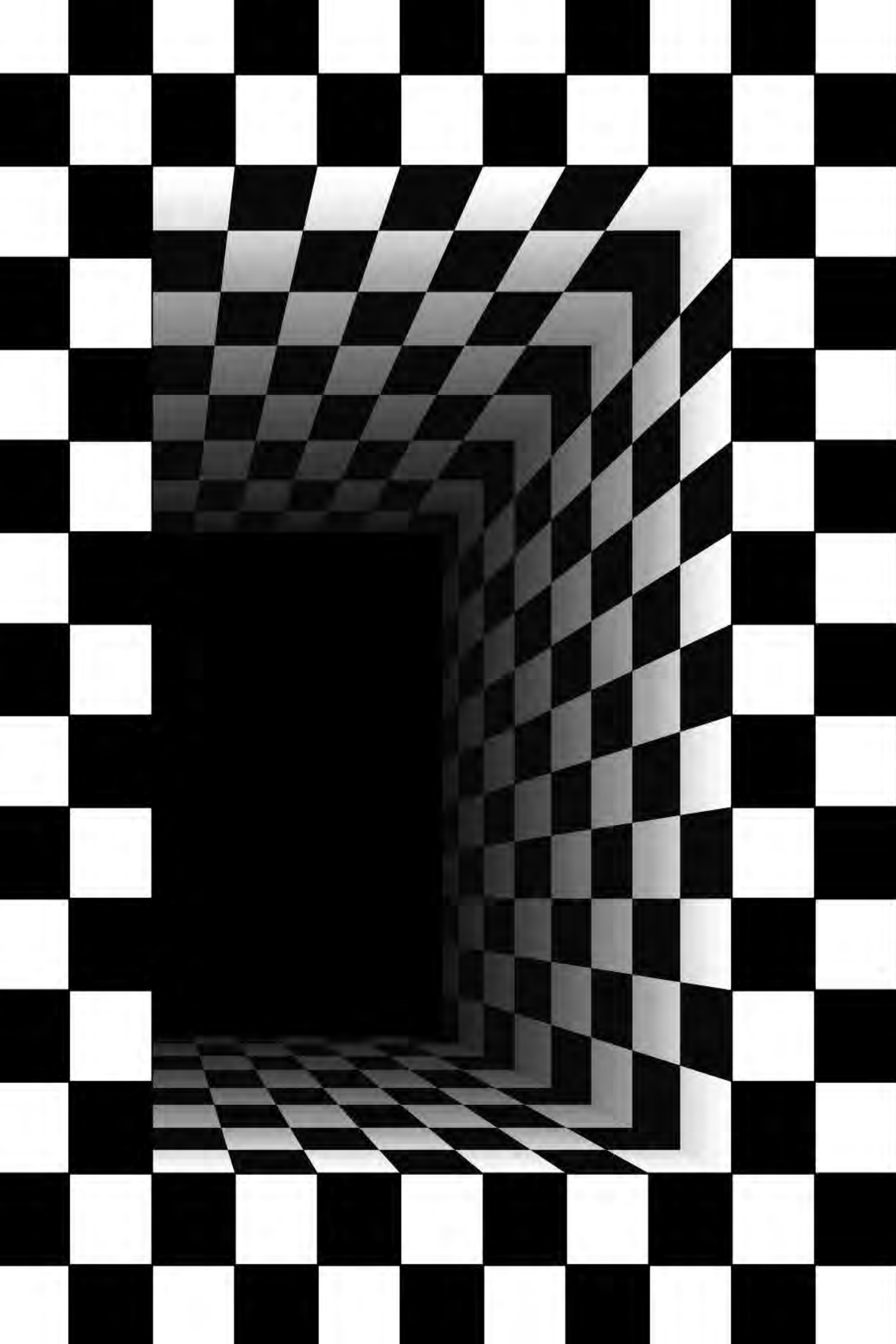
Il controllo parlamentare – attraverso il Copasir – assicura che non ci siano 'diversioni'. L'art. 33 della l. 124 dispone che, nella Relazione semestrale, il Copasir sia informato sulle operazioni condotte dai Servizi di informazione per la sicurezza nelle quali siano state poste in essere condotte previste dalla legge come reato. La dimensione sfidante dell'intelligence resta una: cambiare le cose sul terreno. Le garanzie sono strumenti nel kit degli *intelligence officer* che sono – e devono restare – persone equilibrate, in quanto professionisti della sicurezza che si muovono sempre in una logica di servizio.

Il successo della sicurezza è la *partecipazione*: la nuova intelligence è partner credibile di imprese e università. L'omega delle conclusioni dice apertura di un mondo, reti di senso, nessi di comunità.

La Relazione sulla politica dell'informazione per la sicurezza 2016 spiega che l'intelligence è passata – agli occhi degli italiani – da «apparato» a «comunità». Una realtà dinamica e pensante, capace di tenere il passo a sfide di lungo termine. Non servono aspettative, occorrono obiettivi raggiungibili e verificabili, prima di spostare nuovamente i confini e trasformare le difficoltà in sfide.

Fa parte del gioco dell'essere «resistere al fulmine che governa ogni cosa», scriveva Eraclito. L'obiettivo è sempre disambiguare la minaccia, lavorando sul campo. Lavorando insieme. Se vince la sicurezza, vince il Paese.

Vinciamo tutti.



Big Data
e sicurezza nazionale

Mario Rasetti

C'è una rivoluzione in corso, la *rivoluzione digitale*, da cui tutti siamo travolti per lo tsunami d'informazione cui essa dà vita. La quantità di dati che produciamo raddoppia ogni anno: nel 2016 abbiamo generato tanti dati quanti ne erano stati prodotti nell'intera storia dell'umanità fino al 2015. Ogni minuto nel mondo si effettuano centinaia di migliaia di ricerche su Google e di 'post' su Facebook, che contengono informazione, la quale rivela cosa facciamo, proviamo e pensiamo: chi siamo. Con lo sviluppo dell'Internet delle Cose entro meno di dieci anni avremo 150 miliardi di dispositivi e sensori, 20 volte più numerosi degli uomini sulla Terra, connessi tra loro e con le persone in un'immensa rete globale. Allora la quantità di dati raddoppierà ogni 12 ore. E tutto potrà, almeno in linea di principio, diventare più 'intelligente'; presto avremo non solo smart phones ma smart homes, smart factories, smart cities, smart cars; e la domanda è: sapremo noi umani essere più smart?

Prof. Mario Rasetti, presidente della Fondazione Isi, Torino – New York.

L'umanità sarà sempre più costituita da individui che, di fatto, non sono semplici esseri umani, ma umani con 'protesi' – cellulari, iPhone, laptop… – pezzi di tecnologia che consentono di comunicare, scambiare informazione, accedere a nuove conoscenze, fare operazioni intelligenti in modi nuovi, che estendono a dismisura i sensi, la velocità, la comprensione del mondo circostante. Infatti, in parallelo con la nostra capacità di generare dati, trasmetterli e riceverli, l'intelligenza artificiale (IA) sta compiendo – attraverso l'analisi dei dati e l'abilità nell'estrarne con efficienza il valore – progressi mozzafiato. L'IA non si programma più riga per riga, ma è ormai capace di imparare e automigliorarsi. Sono già attivi algoritmi in grado di riconoscere la scrittura manuale e i pattern, di descrivere il contenuto di fotografie e video, di completare un gran numero di compiti che richiedono *intelligenza*, meglio degli uomini. Oggi il 70% di tutte le transazioni finanziarie è effettuato da algoritmi e il contenuto delle News è, in buona parte, generato automaticamente; e fra breve toccherà alla medicina, alla Pubblica amministrazione, ai trasporti, alle banche…

Tutto questo colloca la rivoluzione digitale allo snodo di tre diverse strade, con caratteristiche e prospettive diverse. La prima: quella digitale è una rivoluzione paragonabile all'invenzione della stampa. Non c'è dubbio che i bit faranno molto più di quanto i caratteri mobili di Gutenberg abbiano fatto in oltre cinque secoli e mezzo in termini di spostamento degli equilibri del potere, di trasferimento della conoscenza dalle mani di pochi a comunità sempre più allargate, di nascita di nuove categorie di attività umane. Sarà avviato un percorso analogo a quello che ha pavimentato la strada che dal Rinascimento, attraverso l'Illuminismo, ci ha portati alla rivoluzione industriale e dai manoscritti su pergamena ci ha fatti arrivare all'E*ncyclopédie* di Diderot e d'Alembert e via via fino a Wikipedia.

Il secondo aspetto è ancora culturale; la scienza dei dati, per antonomasia il *digitale* e l'IA, la nuova frontiera che fa convergere scienza e tecnologia nel sogno comune di concepire e sviluppare sistemi di calcolo e di manipolazione dell'informazione capaci di eseguire compiti che normalmente richiedono l'intelligenza umana, dopo cinquant'anni di sforzi e di miliardi di dollari spesi in ricerca, stanno infine riuscendo a decifrare il codice (*crack the code*) dell'intelligenza umana, quanto basta per trasferirne una parte alle macchine. Significa che l'uomo sarà spodestato dalla sua posizione di supremazia nella società? Certamente no: il cervello umano non è riproducibile da nessuna macchina che non sia un cervello umano molto più evoluto. L'irresistibile leggerezza dell'IA è, in realtà, nel groviglio composito della nostra intelligenza con i nostri valori di uomini, perché i metodi dell'intelligenza artificiale sono lo strumento naturale per affrontare i sistemi complessi.

Il terzo snodo è di natura sociale e dunque etica. È incontrovertibile che mentre questi progressi non potranno che portare in prospettiva a una lunga epoca di prosperità, benessere e tempo libero, di conoscenza senza precedenti, il transitorio a questo stato felice può essere lungo e brutale se non avremo la forza di adattare a esso la nostra economia, le politiche sociali, i comportamenti collettivi.

L'alternativa è una nuova forma di luddismo di reazione al digitale, che potrebbe – come quello nell'Inghilterra del XVIII secolo, seguito alla rivoluzione industriale indotta dall'invenzione della macchina a vapore – portare a un vero e proprio bagno di sangue. Davvero rischiamo un periodo di drammatici scontri sociali a livello globale, perché in pochi anni oltre la metà dei lavori che oggi conosciamo non saranno più svolti da uomini ma da macchine dotate di IA, e non solo lavori manuali, ma lavori che comportano lo sviluppo di processi intelligenti. Sarà una grande crisi, non della classe operaia ma dei colletti bianchi.

Proprio l'innovazione digitale sta all'origine della più aggressiva delle diseguaglianze; quella che spinge oggi il ceto medio alla protesta, al populismo, all'intolleranza (gli «scartati» di papa Francesco). Occorreranno investimenti enormi e globali su istruzione, creatività, riqualificazione degli espulsi dall'asset produttivo nonché nuove modalità di formazione, che non siano limitate ai giovani ma si estendano a chi ha un patrimonio ancora condivisibile di esperienza professionale alle spalle. Non si tratta semplicemente di ridistribuire la ricchezza, ma di creare nuove fonti di conoscenza, per generare nuovo 'sapere' e reinserire nella macchina sociale chi è stato espulso dal mondo del lavoro. E creare nuovo lavoro con nuovi lavori.

I grandi progressi delle tecnologie dell'informazione (IT) trasformeranno le società e le relazioni fra cittadini e governanti; l'impatto dell'automazione, della robotica e dell'intelligenza artificiale sulle economie, sulla distribuzione del lavoro e della ricchezza e, soprattutto, sull'equità sociale farà sì che i Big Data diventino presto un fattore chiave della competizione e dello sviluppo, ponendosi alla base e alla guida di nuove ondate di crescita della produttività e dell'innovazione. Tutto ciò, però, solo a condizione che le corrette politiche decisionali e i necessari incentivi vengano messi in opera con equilibrio. La rivoluzione digitale influirà sul modo in cui si distribuisce il potere nel mondo. Siamo preparati ad affrontare il significativo cambio delle regole che strutture cardine di società, economia e politica vedranno fra oggi e il 2035? Anche la scienza non sarà esente da queste domande e dovrà trovare la sua collocazione in tale quadro articolato e difficile, per non mancare al suo ruolo di guida, etica e concettuale, di una società sempre più smarrita di fronte ai contrasti che la tecnologia, spesso, pare più creare che dirimere.

Nei prossimi 50 anni i supercomputer sorpasseranno di ordini di grandezza, in molti settori, le capacità umane, potenziandole e aumentandole al di là di quanto ora riusciamo a immaginare. E quella dei Big Data – oggi considerata una rivoluzione dell'Information Technology, la quinta dopo i grandi computer, i pc, internet e il web 1.0, i cellulari e il web 2.0, una rivoluzione dovuta allo tsunami di dati che sempre più travolge questo mondo dove tutto quello che facciamo lascia una traccia digitale – ci farà sorridere, quando il numero di byte generati sarà più grande di quello di atomi e molecole nella materia del mondo che ci circonda.
L'ardua sfida dei Big Data è riuscire a estrarre la grande quantità d'informazione che fluisce dentro e fuori dai sistemi complessi con cui conviviamo ed entro cui viviamo. Anche se essi hanno una varietà di caratteristiche diverse; se, ad esempio, sono relativi alla scienza, ben strutturati e controllati, o alla società, più difficili da analizzare ma capaci di fornire una vera e propria *tomografia* della società stessa e rendere possibili 'predizioni' fino a ora quasi impensabili; quello di trasformare i dati in informazione; l'informazione in conoscenza e, infine, la conoscenza in 'sapere' è uno dei più difficili problemi mai affrontato dalla scienza. È il *data mining*; estrarre valore dai dati, come un minatore estrae minerali preziosi dal terreno.
C'è un aspetto inquietante nel quadro che sto dipingendo: il *digital warfare*. Il termine fa riferimento alle nuove strategie, virtuali, di warfare – credo di usare il termine inglese per una sorta di pudore; mi spaventa dire «guerra» – che vedono il coinvolgimento e l'intreccio delle nuove tecnologie IT in sempre più profonde e drammatiche implicazioni sociali e politiche.
Computer hacking (chi non ha sentito parlare di hacker e li ha guardati magari con simpatia, immaginando ragazzini un po' discoli, ma con un'intelligenza molto vivace, capaci di mettere in crisi, giocando, i giganti della tecnologia e della politica) così come *data corruption* sono ormai tecniche centrali del digital warfare. Anche nell'era digitale, per i conflitti – quelli veri, dove nessuno gioca – il cervello conta più dei muscoli. Nel campo di battaglia digitale tuttavia, sia esso militare o civile, l'IT opera solo come amplificatore di forze, mentre la dinamica della superiorità fra chi attacca e chi è bersaglio viene definita con metriche diverse: l'accesso alle reti, ormai pandemico, cambia i differenziali di potere tradizionali, a tutti i livelli della società, e determina come valutare gli equilibri di forza.
Nel digital warfare un ruolo sempre più dominante spetta alla *deception*, l'inganno, che può trasformare l'informazione (e dunque il controllo dei dati e della loro forma e struttura) sia in «arma», nella fase offensiva, sia in «bersaglio», e dunque debolezza, nella difesa. La centralità che l'informazione ha rispetto a quello che ne è il veicolo, l'IT, fa sì che sia la capacità di 'influenzare' a diventare il fattore critico di un conflitto, la cui natura è per-

ciò in continuo divenire. Per questo una qualche forma di controllo sulle comunicazioni di massa diventa prioritaria per governi e Forze armate. Qui si apre un baratro etico: è possibile salvaguardare la riservatezza dell'individuo e al tempo stesso la sicurezza della società nel suo insieme? Perché con la rilevanza crescente della deception, che sempre più è parte integrale delle comunicazioni di un Governo, la manipolazione dell'informazione diventa, nel bene e nel male, funzione essenziale di difesa e di offesa.

Nella società, d'altra parte, l'uso – e la dipendenza! – da internet crescono con modalità ormai più che esponenziale; così la *cybersecurity* sta rapidamente evolvendo da disciplina puramente tecnica, basata su metodologie di analisi e inferenza dai dati, a concetto strategico geopolitico, che richiede il sostegno di strumenti di intelligenza estesi all'intero compound socio-economico e politico, perché gli attacchi cyber minacciano ora in toto la prosperità, la sicurezza e la stabilità nazionale e internazionale.

I decisori della sicurezza nazionale devono giocare nel cyberspazio una complessa partita in difesa dei nostri valori, e per loro una chiave di successo starà nella disponibilità di scenari affidabili e completi, perché solo così potranno colmare la distanza fra strategia e tattica, muovendosi a tutti i livelli del processo cyber. Dunque, anche nel caso digitale si ripete una narrativa nota: la sicurezza delle infrastrutture critiche nazionali deve avere meta-livelli strategici, come deterrenza e controllo, basati su una rappresentazione globale della struttura e delle sue relazioni interne in termini di data science, crittografia, inferenza non lineare per l'individuazione d'intrusioni e su metodi avanzati d'intelligenza artificiale per decifrare la strategia dell'avversario.

In questo quadro sono cruciali le tecniche di *encryption* per garantire la confidenzialità dei dati nei processi di comunicazione e immagazzinamento. Esse richiedono nuovi strumenti di processamento dei linguaggi – sia naturali sia artificiali – specialmente in situazioni critiche, come la necessità di delegare i processi di analisi a macchine non sempre affidabili. La difficoltà è che uno schema efficiente di encryption deve essere coerente, il risultato decriptato deve cioè essere uguale a quello che si otterrebbe se l'analisi fosse effettuata sui dati originali: una sfida matematica, logica e computazionale senza precedenti.

Varie soluzioni complesse sono già in opera per casi specifici: condivisione d'informazioni segrete, dimostrazioni di conoscenza zero, *oblivious transfer*, anonimato, privacy, voto elettronico, aste elettroniche, protocolli di lotterie, protezione di agenti mobili, computazione *multiparty* ecc., ma la partita rimane aperta, con una sfida che è al contempo scientifica e politica, entrambe di straordinaria difficoltà.

Una diversa declinazione di questa stessa problematica è la versione che tocca la società in senso lato, non solo nella prospettiva della sicurezza ma anche in quella più ampia dei valori e della cultura. Essa nasce dal fatto che oggi siamo incredibilmente vulnerabili alla manipolazione delle nostre opinioni, preferenze, credenze e dei nostri sentimenti mediante la disinformazione digitale. Lo strumento è quell'insieme di *bias* – sociali, cognitivi, economici, algoritmici – cui siamo sottoposti attraverso la rete. Questo ha generato un terribile meccanismo sociale di autodifesa, che consiste nel fidarsi soltanto dei segnali provenienti dal nostro 'circolo sociale' e rifiutare ogni informazione che contraddica l'insieme di convinzioni – non necessariamente basate sull'esperienza – del nostro gruppo di riferimento. La logica di questo atteggiamento è scritta in profondità nel nostro Dna, perché ci è stata utile nel processo di evoluzione, quando la specie si adattava per sfuggire ai predatori! La densità del web è così alta che la disinformazione si propaga quasi istantaneamente entro un gruppo e, al contempo, così segregata da riuscire con difficoltà a passare da un gruppo all'altro, in modo che sempre più i membri del gruppo sono esposti selettivamente a un'informazione allineata solo con convinzioni già acquisite; uno scenario, questo, che non favorisce certo lo sviluppo di un salutare senso critico!

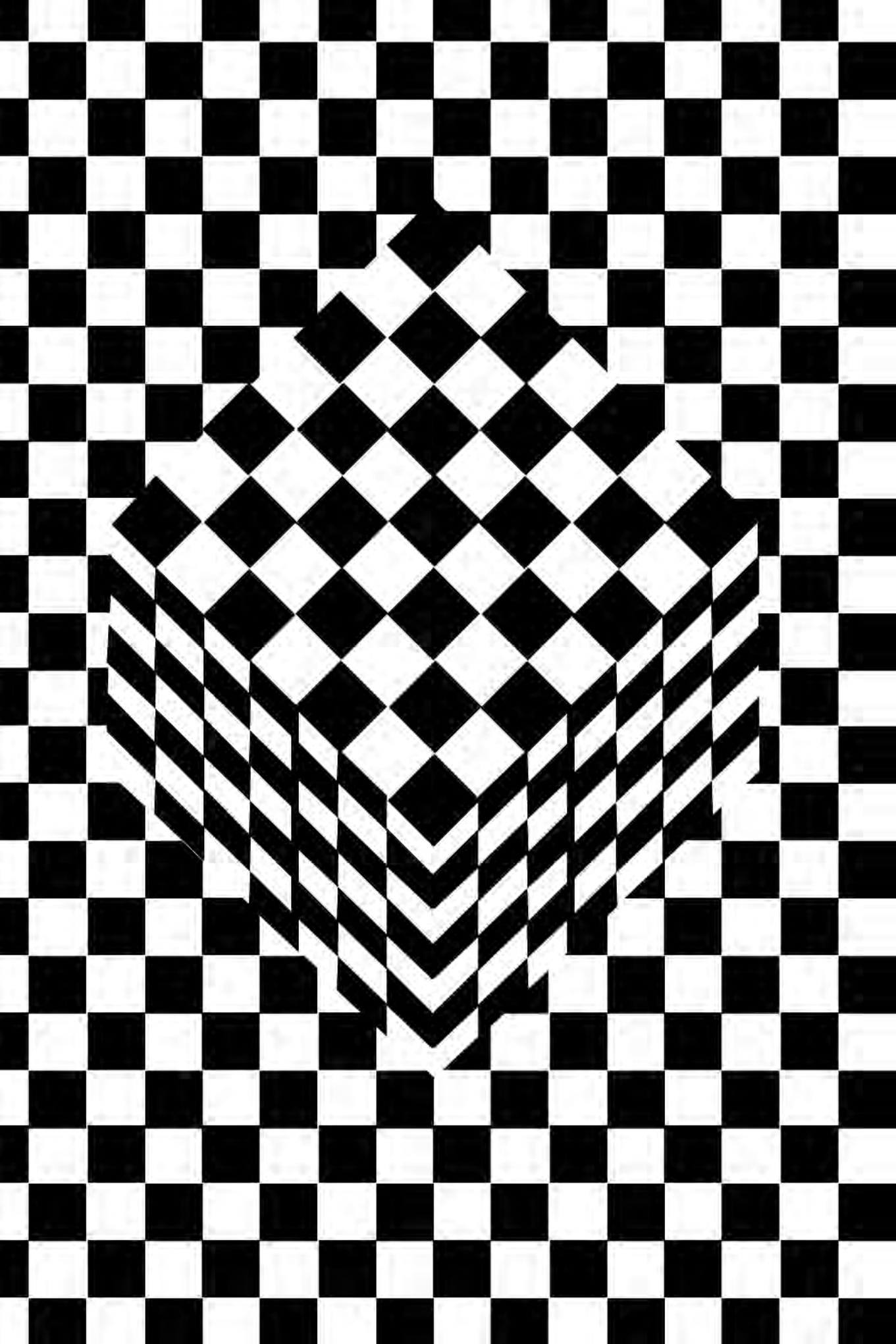
Il rapporto con i media è significativo: il pregiudizio ci porta ormai a condividere o meno un titolo senza neppure leggere l'articolo. Si vedono già i primi tentativi di costruire motori di ricerca mirati a questo fine, basati sulla capacità di distinguere – con parole chiave e algoritmi – *fake news* e *true news*, ma sono molto deboli. La loro debolezza sta nel fatto che la distinzione manichea fra «vero» e «falso» dipende soprattutto, tautologicamente, da quali fonti sono considerate affidabili e non dall'oggettiva veridicità del testo. Ancora una volta è la scienza a essere chiamata in causa: è necessario un *truth algorithm* efficace e affidabile e, soprattutto, indecifrabile.

Si aggiunga il fatto che in alcune loro istanze i dati sono addirittura incomputabili per i nostri computer e ci si chiede di andare oltre a quella straordinaria costruzione concettuale che è alla base di tutto il nostro bagaglio di metodi e strumenti di analisi: la macchina di Turing.

E i valori? Che ne è in questo quadro di riferimento di etica, categoria profitti-salari-lavoro, solidarietà, salvaguardia delle risorse e della natura, salute e benessere? E cosa ne sarà?

Coniugarli con obiettivi, metodi e necessità della scienza, della tecnologia e della sicurezza implica trovare equilibri, tanto delicati quanto difficili. La nostra attenzione ai valori fondanti della civiltà democratica, cui siamo approdati dopo tanti secoli di storia travagliata, non deve conoscere sosta, perché il rischio è di essere travolti da una tecnologia fine a se stessa e dover cedere pezzi preziosi della nostra umanità.

Il mondo moderno nasce solo circa 400 anni fa con l'Illuminismo. Ci fa sorridere pensare come l'incitamento di Immanuel Kant nel parlare di Illuminismo: «Sapere aude! – Abbi il coraggio di servirti della tua intelligenza!» suoni quasi come un ossimoro, se accostato a quell'altrettanto appassionato di Steve Jobs, «Stay hungry, stay foolish!», per spingerci a osare sempre di più per innovare. Illuminismo e rivoluzione scientifico-tecnologica: è con essi che nascono capitalismo, democrazia, commercio globale, potenza industriale. Oggi, la crescita e la diffusione senza precedenti delle reti e della connettività stanno creando un nuovo tipo di ordine, con nuove e diverse sorgenti di forza. Il potere è allo stesso tempo più distribuito, ma anche più concentrato, come mai prima d'ora, mentre tutti i valori, da quelli economici e finanziari a quelli di conoscenza e morali, tradotti in una miriade d'impulsi sembrano fragili, perché le scale di tempo sono sempre più brevi e quelle spaziali più globali, e il profondo cambiamento nei poteri nazionali sarà messo in ombra da un cambiamento ancora più profondo e fondamentale: quello della natura del potere attivato dalle tecnologie di comunicazione.
È in questo scenario, un po' apocalittico (ma quanto reale!), che la scienza del digitale, dei dati, dei sistemi complessi, dell'intelligenza artificiale può e deve giocare il suo ruolo cruciale; ma questo lo potrà fare solo se saprà da subito dotarsi proprio di una forte piattaforma di valori etici che siano universali, condivisi e non particolari; ispirati al benessere collettivo e alla qualità della vita di tutti. Dobbiamo – e, anche in questo, quella dettagliata tomografia della società che i dati ci consentono di mettere a punto sarà strumento fondamentale – concepire un nuovo modello sociale che si adegui ai cambiamenti che il digitale comporta, sapendo coniugare la ridotta necessità di lavoro, con salari adeguati e sicurezza.



ALLEANZA STRATEGICA TRA INTELLIGENCE E UNIVERSITÀ

Gaetano Manfredi

Il Comparto dell'intelligence italiano ha avviato da tempo una stagione di cambiamento e di apertura verso la società civile che ha contribuito a rilanciarne la visione; oggi l'intelligence è ampiamente percepita come una struttura al servizio dello Stato e a difesa della democrazia, capace di affrontare le complesse esigenze di sicurezza che sono poste dall'articolata situazione internazionale. E quest'apertura non è affatto un'operazione di sola immagine ma coincide, invece, con un concreto cambiamento di approccio alla funzione d'intelligence, che passa anche attraverso la costruzione di una solida e fattiva collaborazione con il mondo delle università. Tante sono oggi le iniziative congiunte con singoli atenei italiani, legate ad azioni di formazione e di ricerca, mentre l'architettura della partnership con il mondo accademico vuole essere di sistema e di ampio respiro. A riprova di ciò va sicuramente ricordato il programma 'Intelligence live', un lungo roadshow del Sistema di informazione per la sicurezza della Repubblica attraverso il quale l'intelligence italiana ha fatto visita in diverse tappe a numerosissimi atenei, potendosi confrontare con studenti e ricercatori di

Prof. Gaetano Manfredi, rettore dell'Università Federico II di Napoli e presidente Crui.

provenienza culturale diversa, potendo raccontare i propri obiettivi, le proprie criticità, le nuove sfide poste dalla complessa situazione internazionale e dall'evoluzione tecnologica in atto. Si è trattato di incontri tutti stimolanti, che hanno attratto numerosi studenti e ricercatori affascinati dal mondo dell'intelligence ed entusiasti nell'apprendere quanto il loro contributo possa essere utile a cogliere e affrontare con successo le nuove sfide per la sicurezza. I rapporti tra il mondo dell'intelligence e quello universitario sono da alcuni anni una realtà già in diversi Paesi, tra cui Stati Uniti e Regno Unito, e il grande impegno che si sta profondendo in Italia per costruire con successo questa sinergia pone il nostro Paese all'avanguardia.

L'esigenza di avvicinare il mondo universitario e della ricerca all'organizzazione dell'intelligence è dettata da due aspetti fondamentali: da un lato, la necessità di garantire sempre alti livelli di sicurezza in un ecosistema tecnologico comunque in continua evoluzione, dove utilizzi malevoli delle nuove tecnologie sono inevitabilmente l'altra faccia della medaglia di tantissime innovazioni tecnologiche, che si impongono in modo dirompente, inevitabili e necessarie; dall'altro lato, la complessità delle crisi politiche, delle tensioni interne ed esterne al nostro Paese, rafforzata dalla globalizzazione e dalle trasformazioni della società, impone un approccio articolato e multidisciplinare alla sicurezza, con l'urgente necessità di competenze plurime, per affrontare con successo i numerosi rischi che si generano.

Innanzitutto, quindi, la vorticosa rivoluzione tecnologica cui assistiamo con ritmi sempre più rapidi pone continuamente nuovi fronti su cui operare per garantire la sicurezza dello Stato, della società e della democrazia, in Italia come ovunque nel mondo. La nebulosa di nuove tecnologie, digitali e non, cresce e matura a una velocità impressionante, si fonde in nuovi sistemi e rapidamente è in grado di entrare nella vita quotidiana, scalzando sistemi preesistenti che velocemente diventano obsoleti. Si tratta di rivoluzioni grandi e piccole, che impattano in maniera più o meno significativa diversi aspetti della nostra società e del nostro modo di vivere, dal lavoro, all'istruzione, alla salute, alla comunicazione. Siamo ormai abituati agli annunci di imminenti rivoluzioni, dovute all'introduzione di questa o quella tecnologia, che ormai non ne veniamo quasi più impressionati, e ci limitiamo a subirne le conseguenze, in questo o in quell'aspetto della nostra vita, e ad adattarci alla nuova novità. Quest'approccio da utenti è totalmente opposto a quello che sono obbligati ad avere gli operatori della sicurezza, ai quali non è permesso abbassare la guardia nel vortice d'innovazioni tecnologiche tutte potenzialmente capaci d'impattare sulla sicurezza di una società in continua trasformazione, che fa del rinnovamento tecnologico ormai un equilibrio dinamico, non più una semplice opzione ma una necessità. E l'esempio emblematico e attuale si chiama Industria 4.0.

Si tratta dell'ultima annunciata rivoluzione digitale che sta trasformando il mondo della produzione, non solo di oggetti ma anche di servizi, informazioni e conoscenza. Etichettata come la quarta rivoluzione industriale, con Industria 4.0 non s'intende una singola innovazione tecnologica, ma un ecosistema di nuove tecnologie (numerose liste redatte per descrivere il fenomeno Industria 4.0 ne individuano molte decine), che integrandosi e interagendo in infinite combinazioni, promettono di incidere su numerosissimi aspetti della nostra vita e della nostra società. Dietro il fenomeno Industria 4.0 si sono l'Internet of Things, la stampa 3D, la robotica, le interazioni machine-to-machine, l'Intelligenza artificiale, le tecnologie di analisi dei Big Data e tante altre grandi e piccole tecnologie che stanno generando trasformazioni incredibili nel modo di lavorare, di produrre, di informarsi, di comunicare, di creare. Immaginare il mondo a valle di queste trasformazioni e cercare di prevedere come comunicheremo, ci sposteremo e lavoreremo, anche solo tra dieci anni, è praticamente impossibile.

La peculiarità del fenomeno Industria 4.0 è la pluralità di tecnologie che hanno raggiunto quasi in contemporanea una maturità tale da impattare il mondo industriale. Le innovazioni sono quindi capaci di andare in risonanza tra loro e amplificare in modo imprevedibile il loro effetto sulla società e sulla sicurezza. Questo ecosistema di tecnologie rappresenta, quindi, il punto di partenza di un percorso d'innovazione inevitabile che trasformerà profondamente la nostra vita, anche se non possiamo immaginare come esattamente ciò avverrà. Tutto ciò è elettrizzante se ci poniamo come utenti finali delle tecnologie, come abitanti del mondo che non vedono l'ora di approfittare dei vantaggi che queste nuove tecnologie forniranno semplificando e migliorando la vita. Purtroppo, però, non è mai solo questo il nostro punto di vista. Le trasformazioni in arrivo promettono di essere così pervasive da incidere anche sulla nostra privacy e sulla nostra sicurezza. Adeguarsi alle innovazioni aggiornando il modo in cui viene gestita la sicurezza diventa quindi un obbligo per la nostra società e l'intelligence è in prima linea in questa sfida.

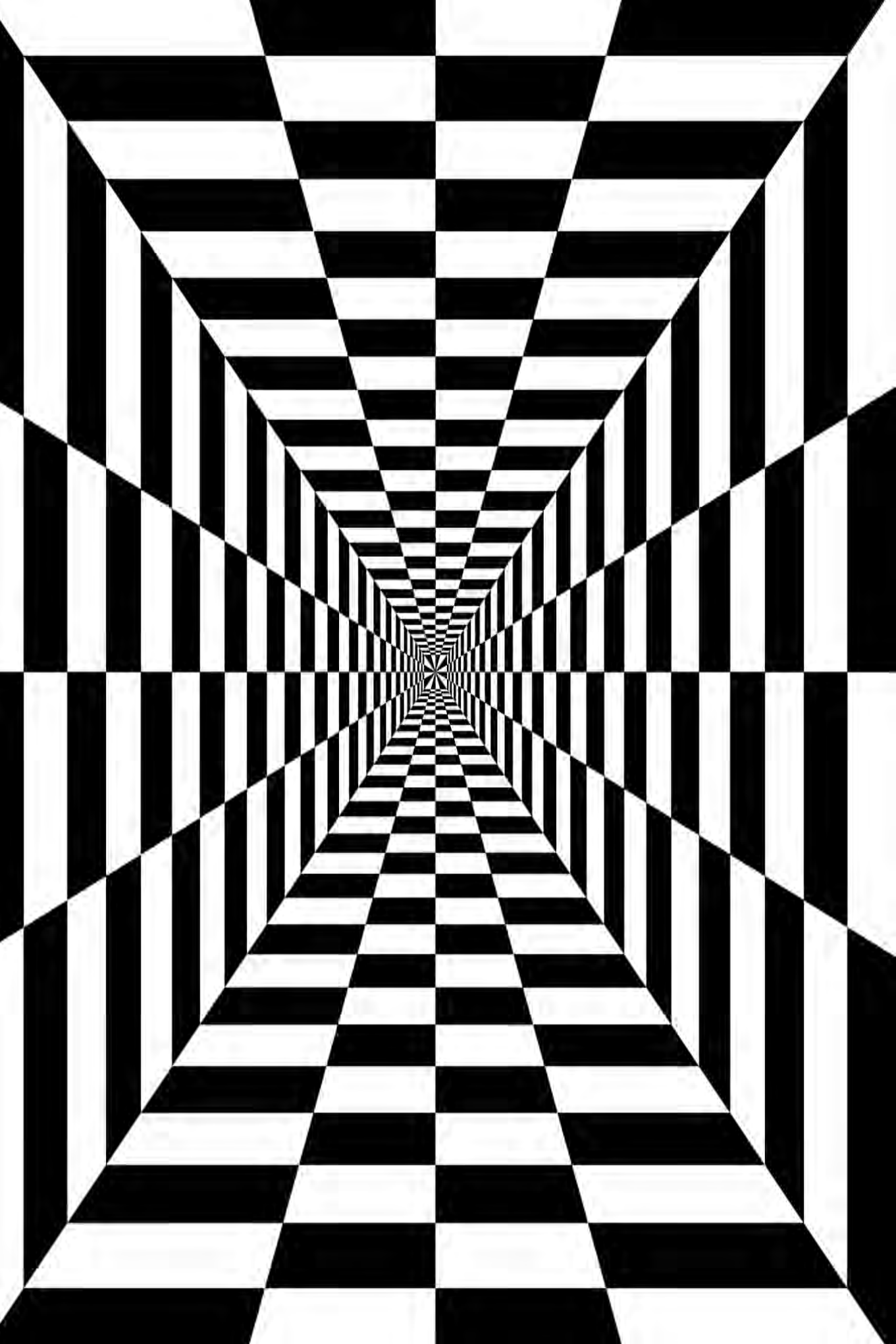
D'altra parte, la rivoluzione tecnologica a cui assistiamo è caratterizzata da un aspetto fondamentale: la grande accessibilità delle nuove tecnologie che, per quanto spesso potentissime, sono comunque disponibili a molti soggetti. Ciò rappresenta una caratteristica che contribuisce ad accelerare la stessa innovazione tecnologica. I soggetti che fanno ricerca sono infatti numerosissimi, dagli hacker ai colossi digitali, alle piccole imprese e alle università, e traggono grande vantaggio dalla condivisione di idee, innovazioni e sviluppi; ma, al contempo, il facile accesso alle tecnologie eleva i rischi legati a un loro utilizzo malevolo e le rende potenziali punti di attacco alla sicurezza e alla privacy dei singoli e delle comunità.

Ecco quindi evidente la grande utilità di una partnership strutturata tra la realtà dell'intelligence e quella universitaria. L'università italiana, che sa esprimere grandi qualità e grandi eccellenze negli ambiti disciplinari legati alle tecnologie, rappresenta nel nostro Paese la prima sentinella delle trasformazioni e delle innovazioni in atto e può costituire un partner essenziale, fornendo supporto nell'analisi delle nuove tecnologie, nella valutazione dei rischi a esse collegate, nella previsione delle evoluzioni tecnologiche in atto, nell'utilizzo delle tecnologie stesse per mitigarne i rischi e nello sviluppo di specifiche applicazioni tecnologiche con finalità di sicurezza.
L'altro aspetto, che dà ampia giustificazione della necessità di una partnership forte tra intelligence e università, riguarda la complessità e il carattere articolato che assumono le questioni internazionali e nazionali trattate dall'intelligence. La globalizzazione, l'innovazione tecnologica, le grandi questioni internazionali, le nuove reti di comunicazione e i social network sono solo alcuni degli ingredienti di questa complessità, che ridisegnano il profilo di competenze e conoscenze richiesto per gli operatori dell'intelligence.
Una multidisciplinarità molto particolare, che va dalla conoscenza di culture diverse, alla storia contemporanea, alle tecnologie Ict, all'economia, alle scienze giuridiche. Apporti disciplinari molto differenti, che possono essere riuniti insieme con successo solo attraverso il contributo accademico e di tutte le sue anime culturali e disciplinari. Un'analisi sicuramente parziale delle competenze plurime oggi necessarie include una conoscenza profonda delle questioni politiche e storiche contemporanee, cui possono sicuramente contribuire i validissimi storici dell'accademia italiana. Le eccellenze dell'ingegneria e della fisica presenti in numerosi atenei possono aiutare ad affrontare le questioni connesse alle innovazioni tecnologiche, per quanto già ampiamente discusso in precedenza. La sicurezza relativa ai nuovi strumenti economici e finanziari, anche legati alle nuove tecnologie, richiede una conoscenza approfondita cui possono contribuire le valide scuole di economia. E, ancora, tutte le questioni giuridiche sul piano nazionale e internazionale, anche legate alle nuove esigenze di privacy e sicurezza digitale, possono essere affrontate con il supporto delle scuole di giurisprudenza.
In dettaglio, quindi, il contributo universitario può essere duplice. Da un lato, l'università può rispondere all'esigenza di una formazione specialistica per gli operatori della sicurezza che preveda percorsi peculiari, costruiti attraverso l'apporto di diverse discipline, per formare un profilo professionale idoneo a operare nella complessità delle questioni che l'intelligence si trova ad affrontare oggi. Dall'altro lato, l'intelligence può rinnovarsi attingendo proprio al mondo universitario, anche con nuove modalità di reclutamento di operatori, dotati di un profilo professionale diverso da quello convenzionale, ovvero non provenienti dalle Forze di sicurezza, con lo scopo di arric-

chire e completare la comunità degli esperti. Ben vengano, quindi, sia iter professionalizzanti per studenti universitari (significative esperienze sono già condotte in molti atenei), per formare nuove figure, sia percorsi compiuti nelle convenzionali strutture formative dell'intelligence, ovvero la Scuola di formazione del Comparto intelligence, con il supporto della comunità accademica. Ben vengano anche nuove forme di collaborazione che vedano i ricercatori universitari impegnati a supporto di specifiche questioni specialistiche e peculiari.

Per tutto quanto esposto, l'alleanza tra il mondo universitario e quello dell'intelligence rappresenta sicuramente un punto cardine irrinunciabile della politica per la sicurezza nazionale. Le grandi questioni che l'intelligence italiana si trova ad affrontare per garantire la sicurezza dello Stato insieme alle trasformazioni culturali, tecnologiche, politiche e sociali, in atto a livello globale, pongono nuove esigenze che richiedono un approccio nuovo e un nuovo alleato: l'università.

E l'università italiana, con il proprio bagaglio di competenze specialistiche e generalità culturali, si è mostrata da subito pronta a rispondere a questa esigenza, con entusiasmo e senso del dovere, per contribuire fattivamente al bene dello Stato, della democrazia e alla sicurezza della nostra gente.



UNIVERSITÀ E ANALISI STRATEGICA

LO STUDIO DI NUOVI MODELLI GEOSTRATEGICI

Franco Anelli

«Geography is about power», scrive Gearóid Ó Tuathail, nel suo celebre *Critical Geopolitics*[1]. Dal punto di vista geopolitico, la mappa del mondo non è un prodotto naturale, bensì il risultato di un'incessante lotta lungo la storia per il potere di amministrare, controllare e sfruttare lo spazio fisico. E negli ultimi decenni, chiusa la lunga parentesi del confronto bipolare – che aveva, per così dire, 'ingabbiato' questa lotta in una rigida prospettiva dicotomica – il sistema internazionale si è dovuto nuovamente confrontare con una geografia complessa e dai contorni mutevoli, ridisegnati da un'inaspettata confusione geopolitica. Abbiamo così assistito a una colossale redistribuzione del potere e del prestigio a livello internazionale, a guerre locali e regionali, alla frammentazione di Stati, all'impetuosa crescita della visibilità dei cosiddetti *Non-State Actors*, alla polarizzazione violenta delle società caratterizzate da una pluralità identitaria etno-religioso-culturale, alle spinte centrifughe nella stessa Europa.

Prof. Franco Anelli, rettore dell'Università Cattolica del Sacro Cuore di Milano.

1. Ó Tuathail 1996, p. 1.

L'aumento della complessità dello scenario internazionale, che tende sempre più alla multipolarità, ha portato a una progressiva obsolescenza dei principi di analisi strategica a cui eravamo abituati (unicità della minaccia, sostanziale staticità strategica dei macro-scenari, *Zero Sum Game Theory*, schema binario *amicus / hostis* ecc.), evidenziando, al contempo, le difficoltà nell'aggiornare dottrine e metodologie d'analisi, come dimostrato dalla tentazione ricorrente a reinterpretare il contesto internazionale in chiave criptobipolare (si pensi, ad esempio, all'architettura della 'guerra al Terrore').
Ancora durante il periodo della Guerra fredda, il politologo Ciro Zoppo sottolineava i rischi del ritardo fra il mutamento del quadro di riferimento strategico e l'evoluzione delle «mappe cognitive» correlate[2]. Ritardo che esponeva al rischio di non comprendere i meccanismi delle nuove matrici strategiche. Queste vischiosità cognitive e organizzative si sono andate sommando alla bassa capacità predittiva dimostrata nei decenni dalle scienze sociali e alla tendenza a leggere in forme semplificate i contesti regionali o subnazionali ove esplodevano crisi di sicurezza.
Per quanto la propensione al conservatorismo dei criteri di analisi – sia da parte dei decisori che degli studiosi – appaia come una conseguenza naturale del rapido mutamento politico-sociale e dell'innovazione tecnologica, il sistema universitario ha senza dubbio accolto la sfida della crescente complessità del sistema delle relazioni internazionali. Ne è una testimonianza l'incremento quantitativo negli atenei italiani degli insegnamenti di studi strategici, di geopolitica e geoeconomia, ma anche delle neuroscienze applicate alle relazioni sociali e al comportamento in contesti di emergenza, che hanno via via affiancato i tradizionali insegnamenti giuridici, storici, economici, politologici e sociologici nell'ambito dei corsi di studio dedicati alle relazioni internazionali. Particolarmente rilevante è stata la riscoperta della geopolitica come disciplina accademica e quale utile strumento di comprensione delle dinamiche internazionali, sia a livello micro sia macro, grazie soprattutto alla scuola francese, in particolare al geografo Yves Lacoste e al Laboratoire de stratégie théorique creato presso la Fondation pour les Études de Défense Nationale in Francia. Il successo di questo termine e delle riviste che s'ispiravano alla riflessione geopolitica (si pensi a «Hérodote» in Francia o a «Limes» in Italia) ha permesso di superare la *damnatio memoriae* subita dalla geopolitica classica all'indomani della fine della Seconda guerra mondiale, dato che essa era stata ingiustamente collegata alle ideologie più nefaste di quel periodo. Al contrario, l'analisi geopolitica si è rivelata uno strumento indispensabile per comprendere le

2. Cfr. Zoppo – Zorgbibe 1985.

radici profonde delle tante crisi locali che andavano esplodendo nel mondo, così come la sovrapposizione – spesso conflittuale – della proiezione degli interessi nazionali dei singoli attori locali regionali e internazionali coinvolti[3]. Come noto, infatti, l'instabilità e l'apertura di nuove aree di conflittualità sono potenti magneti che attirano gli interventi esterni e incrementano la permeabilità dei sistemi di sicurezza regionali. In termini geostrategici, sono le cosiddette *shatterbelts* individuate dal geopolitologo statunitense Saul Bernard Cohen: le linee di faglia e di frattura in cui si scaricano le tensioni internazionali[4].

L'Università Cattolica del S. Cuore ha cercato, in particolare, di approfondire – da una prospettiva marcatamente pluridisciplinare e interdisciplinare – la riflessione sui mutamenti in atto nel sistema internazionale e nella capacità di comprendere le dinamiche politico-sociali, securitarie e identitarie di micro-scenario, collocandole nel più ampio quadro del mutamento geostrategico internazionale. Un cambiamento che giunge spesso imprevisto agli stessi esperti o che appare così composito e mutevole da sfuggire a ogni tentativo di sistematizzazione. Eppure, è proprio la difficile leggibilità della dinamica internazionale contemporanea e l'interrelazione dei suoi effetti che ci spingono a un'analisi che non sia meramente reattiva, ma anche previsionale e proattiva.

John Mainard Keynes soleva ironicamente ricordare che «l'inevitabile non accade mai. L'imprevisto sempre». Ma la limitatezza e la fallibilità di ogni tentativo previsionale non possono far desistere dallo sforzo d'immaginare le principali linee di possibile evoluzione geopolitica, sociale, economica, ecologica e tecnologica; né dall'ipotizzare quali possano essere i principali attori locali, regionali e internazionali nei diversi quadranti strategici e come proseguirà la redistribuzione del potere fra gli Stati avviatasi negli ultimi vent'anni. Da questo punto di vista, le metodologie per l'elaborazione di modelli strategici previsionali, di breve, medio e lungo periodo rappresentano un importante strumento che può e deve accompagnare tanto l'analisi scientifica quanto la fase decisionale politica e l'elaborazione di politiche di sicurezza. È in questa prospettiva che va inquadrata la collaborazione avviata con la Scuola di formazione del Sistema di informazione per la sicurezza della Repubblica, supportata dalle disposizioni recate dalla legge 3 agosto 2007, n. 124 che ha incoraggiato l'avvicinamento fra università, enti di ricerca e il mondo dell'intelligence. Una collaborazione che si esplicita in una pluralità di progetti comuni di aggiornamento e approfondimento sul mutamento degli scenari regionali.

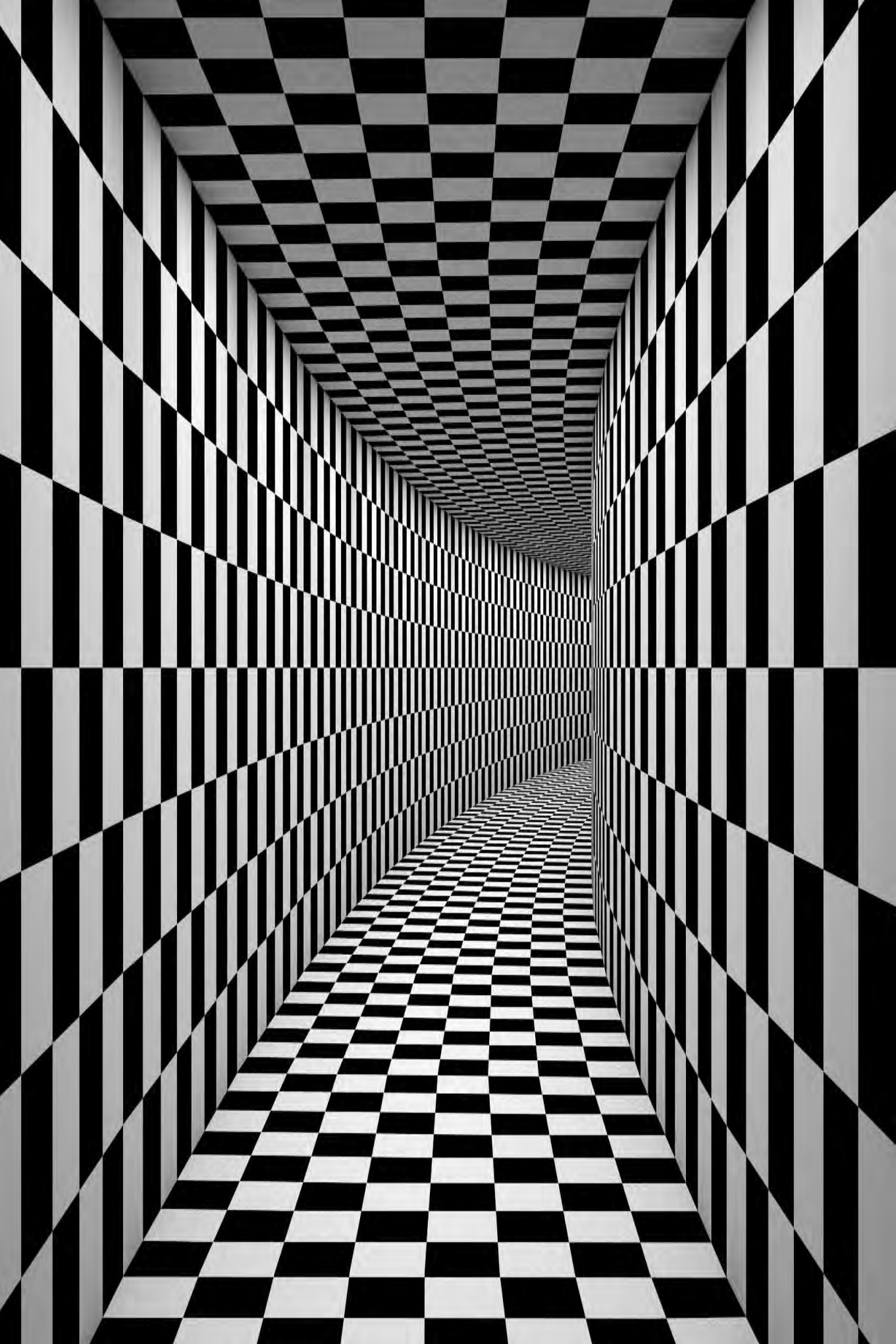
3. Cfr. Lacoste 2006.
4. Cohen 2008.

Al primo filone appartengono percorsi di aggiornamento su diversi quadranti geopolitici mondiali e su temi connessi alla sicurezza, con l'organizzazione di seminari e lezioni specialistici. A essi si è aggiunto un corso di formazione permanente specificamente dedicato alle sfide dell'analisi strategica e al ruolo delle tecniche di analisi più moderne e strutturate, che offrono un valido strumento per formulare ipotesi e scenari, limitando al massimo i *bias* cognitivi e favorendo la messa a sistema delle diverse *expertise* e conoscenze.
Il già ricordato quadro internazionale impone, infatti, di andare oltre la riflessione dei singoli esperti, creando gruppi di lavoro basati su metodologie sia qualitative sia quantitative aperte alla *cross-fertilization* e all'innovazione dei modelli interpretativi.
Quanto al secondo filone, può essere ricordata la recente iniziativa M*editerraneo* 2035. L*a trasformazione degli scenari geopolitici*. Si tratta di un progetto sfociato, nel giugno scorso, in un convegno organizzato presso il campus di Roma dell'Università Cattolica, a cui hanno partecipato alcuni fra i maggiori esperti italiani di relazioni internazionali, sicurezza, economia, Medio Oriente, mutamenti ecologici, demografici e tecnologici, alla presenza dei vertici del Comparto sicurezza. Obiettivo primario del convegno è stato quello di offrire una riflessione sull'evoluzione del bacino del Mediterraneo e delle aree prospicienti, evidenziando il ruolo dei diversi attori regionali e internazionali (sia statuali sia sub-statuali) e cercando di immaginare le possibili criticità future. Dopo anni di apparente marginalità, infatti, il Mediterraneo sembra oggi ritornato al centro della scena politica internazionale; tuttavia si tratta di una centralità più subita che desiderata, provocata dall'esplosione di fenomeni fortemente destabilizzanti quali il terrorismo jihadista, la crescita incontrollata del fenomeno delle migrazioni, la frammentazione statuale violenta lungo la sponda sud e la polarizzazione etno-settaria. Questo stato di forte conflittualità rende il sistema regionale penetrabile e permeabile alle interferenze esterne, facendo aumentare notevolmente il numero di variabili. A tutti questi già complessi fattori si vanno aggiungendo fenomeni di lunga durata come il mutamento climatico, demografico e delle relazioni economiche.
Il risultato è la crescita della complessità di ogni possibile modello geostrategico previsionale, tanto più che da tempo – a livello macro-internazionale – si vanno indebolendo i principi su cui si è cercato di fondare l'ordine post bipolare, come il multilateralismo e l'approccio cooperativo. Se durante tutto il XX secolo le dinamiche internazionali sono state capaci di agire come dei 'regolatori' dell'assetto di questo bacino, oggi la dimensione regionale sembra prendere il sopravvento,

con una diminuzione della capacità d'intervento calmierante esterno. Si crea così un sistema instabile, fortemente competitivo e dominato, da un lato, dall'enfasi sulla sicurezza e, dall'altro, dalle alleanze polarizzate.
Dinanzi a un tale scenario appare ineludibile l'esigenza di rafforzare e rendere maggiormente efficace la nostra capacità di lettura e di comprensione delle dinamiche contemporanee e delle possibili proiezioni future. Un tentativo che deve necessariamente essere il più possibile olistico e interdisciplinare, che spinge a una collaborazione crescente fra il mondo dell'alta formazione e della ricerca, le strutture istituzionali e decisionali e il sistema per la tutela della sicurezza dello Stato.

BIBLIOGRAFIA

S. Cohen, *Geopolitics. The Geography of International Relations*, Rowman & Littlefield Publishers, Lanham 2008².
Y. Lacoste, *Géopolitique: La longue histoire d'aujourd'hui*, Larousse, Paris 2006.
G. Ó Tuathail, *Critical Geopolitics*, Routledge, London 1996.
C. Zoppo – Ch. Zorgbibe (eds.), *On Geopolitics: Classical and Nuclear*, Martinus Nijhoff Publishers, The Hague 1985.



LE GARANZIE FUNZIONALI DEGLI APPARTENENTI AI SERVIZI

UN BILANCIO A DIECI ANNI DALLA LEGGE 124/2007

Paola Severino

Il tema delle garanzie funzionali degli appartenenti ai Servizi di sicurezza (Aise e Aisi) si colloca al crocevia di due interessi di sicuro rilievo e di evidente spessore costituzionale: da un lato, l'idea alla base di ogni sistema democratico della trasparenza dell'agire dei pubblici poteri e del controllo sul loro operato, nel cui ambito, dal nostro specifico angolo visuale, si inserisce quello esercitato dall'Autorità giudiziaria a fronte di fatti integranti reato; dall'altro, la necessità, allorché a venire in gioco sia la protezione della sicurezza nazionale, che gli operatori dei Servizi, per il perseguimento delle finalità istituzionali, possano contare su uno scudo protettivo che li ponga al riparo dal rischio penale connesso alle condotte poste in essere.
Si tratta di un quadro di interessi da tempo delineato dalla nostra Corte costituzionale che, sin dalle note sentenze n. 82 del 1976 e n. 86 del 1977[1] in materia di segreto di Stato, ha identificato nel «supremo interesse della sicurezza dello Stato [...], cioè l'interesse dello Stato-comunità alla propria integrità territoriale, alla propria indipendenza e, al limite, alla sua stessa sopravvivenza», il bene in grado di legittimare un arretramento dei principi sopra evocati.

Prof.ssa Paola Severino, rettore della Luiss Guido Carli di Roma.

1. Corte cost., sentenza 6 aprile 1976, n. 82, Pres. Oggioni, Rel. Crisafulli; Corte cost., sentenza 24 maggio 1977, n. 86, Pres. Rossi, Rel. Roehrssen.

Si è in presenza, prendendo in prestito le parole della Consulta, di un valore che, in quanto connesso alla salus rei publicae, non può che prevalere su ogni altro e che trova copertura normativa nell'art. 52 Cost. laddove qualifica la difesa della Patria come sacro dovere del cittadino[2]. Da notare come, a partire da quelle fondamentali decisioni, non a caso il dialogo con il Legislatore si sia piuttosto spostato sui limiti del segreto e sulle modalità di verifica della correttezza dell'esercizio del relativo potere in capo all'Esecutivo.
La logica è dunque quella del bilanciamento tra interessi contrapposti, alla ricerca di un soddisfacente punto di equilibrio che, nella consapevolezza della centralità della sicurezza dello Stato, non comprima eccessivamente le esigenze di giustizia[3].
Uno schema analogo non può che valere per le garanzie funzionali la cui previsione deve passare, in uno Stato di diritto, per un'espressa disposizione legislativa e per la fissazione di precise condizioni al cui ricorrere l'autore del fatto possa andare esente da pena.

IL LUNGO CAMMINO VERSO L'INTRODUZIONE DELLE GARANZIE FUNZIONALI PER I SERVIZI DI SICUREZZA

Il vero nodo delle garanzie funzionali è stato rappresentato, a differenza del segreto di Stato, dal silenzio sul punto serbato per lunghi anni dal Legislatore. Nessuna menzione di cause di esclusione della pena a favore dei dipendenti dei Servizi di sicurezza era contenuta nella legge 24 ottobre 1977, n. 801 che, tradizionalmente, ha costituito il punto di riferimento normativo in materia. Era sì presente, come autorevolmente osservato, un cenno al tema nella parte in cui, dopo aver stabilito l'obbligo dei direttori dei Servizi «di fornire ai competenti organi di polizia giudiziaria le informazioni e gli elementi di prova relativi a fatti configurabili come reati», si ammetteva la possibilità, su disposizione del Ministro competente con l'esplicito consenso del presidente del Consiglio, di ritardare siffatta comunicazione «quando ciò sia strettamente necessario per il perseguimento delle finalità istituzionali dei Servizi». Ma nulla più di questo[4].
Il dibattito rimaneva confinato all'ambito teorico nonché all'interno delle aule parlamentari e dei lavori delle commissioni di riforma che, nel tempo, hanno cercato di porre rimedio all'evidente lacuna[5].

2. Corte cost., sent. nn. 82/1976, 86/1977, citata nota 1.
3. Sull'argomento, cfr. Spirito 1979, pp. 581-592. Più di recente sul punto, in connessione al tema delle garanzie funzionali, cfr. Bonetti 2008, pp. 45-55.
4. Grevi 1987, pp. 555 ss.
5. Sul punto, cfr. Fioravanti 1991, pp. 448-475; Grevi 1987, p. 557.

Né la situazione si è modificata allorché nel nostro sistema sono iniziate a fiorire, sino al riordino operato dalla legge 16 marzo 2006, n. 146, le figure di agente provocatore, riguardanti protagonisti e condotte di taglio diverso, ma la cui regolamentazione da parte del Legislatore è una spia dell'importanza di offrire soluzioni normative ad hoc[6].
Il risultato è stato quello del ricorso al segreto di Stato quale meccanismo di supplenza rispetto alla mancata presa di posizione del Legislatore[7]; segreto di Stato che, nel frattempo, aveva ricevuto uno statuto di disciplina sensibile agli ammonimenti rivolti dalla Corte costituzionale, quantomeno per quanto attiene alla previsione di limiti – il richiamo ai fatti eversivi dell'ordine costituzionale quale barriera invalicabile – e alla titolarità del potere di apposizione e opposizione attribuita al vertice dell'Esecutivo, il presidente del Consiglio.
Si trattava però di uno strumento non adeguato: da una parte, la diversa ratio del segreto – che è quella di sottrarre alla pubblicità notizie, atti, documenti ecc. la cui diffusione potrebbe arrecare grave pregiudizio alla sicurezza della Repubblica – faceva sì che esso non potesse indirizzarsi a coprire il fatto di reato in sé ma esclusivamente riferirsi a ciò che doveva rimanere confinato negli arcana imperii[8]. L'effetto, spiegato dal segreto, di tutela degli appartenenti ai Servizi era dunque indiretto, potendo inibire l'accertamento dell'Autorità giurisdizionale limitatamente agli elementi da esso coperti, sancendone l'inutilizzabilità quali fonti di prova, avuto riguardo all'eventuale integrazione di ipotesi criminose degli agenti nell'esercizio delle loro funzioni; dall'altra, la legge del 1977 fissava verso l'alto il confine del segreto – peraltro con una formula piuttosto elastica (quella dell'eversione dell'ordinamento costituzionale) – ma non disciplinava in modo articolato, sempre per richiamarsi all'insegnamento della Corte costituzionale, quale fosse il «ragionevole rapporto di mezzo a fine» in grado di legittimare il ricorso al segreto medesimo[9].
Insomma, una protezione degli appartenenti ai Servizi che si giocava tutta sul piano processuale e senza un itinerario chiaro, scandito da definiti passaggi legislativi, in grado di fungere da guida per l'autore del fatto.

6. Si fa riferimento, in particolare, all'art. 9 – rubricato 'Operazioni sotto copertura' – della legge 16 marzo 2006, n. 146 (a sua volta modificata dalla legge 13 agosto 2010, n. 136), sulla ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001. Tale disposizione, infatti, ha provveduto a introdurre nel nostro ordinamento una regolamentazione organica, a livello sostanziale e procedurale, delle diverse operazioni sotto copertura e dei c.d. agenti provocatori, sino ad allora disciplinati dal nostro Legislatore in differenti disposizioni normative – quali, ad esempio, l'art. 14 della l. 269/1998 in materia di turismo sessuale in danno dei minori, o l'art. 4 del d.l. 374/2001 recante disposizioni per il contrasto al terrorismo internazionale – abrogate dall'articolo in parola. In dottrina, sul punto, cfr. Amato 2011.
7. Guccione in Illuminati 2010, p. 266.
8. Sull'argomento, cfr. Corte cost., sentenza 10 aprile 1998, n. 110, Pres. Granata, Rel. Contri, con nota di Santoriello 1999, pp. 797-798. Secondo il giudice delle leggi, infatti, «... l'opposizione del segreto di Stato da parte del Presidente del Consiglio dei Ministri non ha l'effetto di impedire che il pubblico ministero indaghi sui fatti di reato cui si riferisce la 'notitia criminis' in suo possesso, ed eserciti se del caso l'azione penale, ma ha l'effetto di inibire all'Autorità giudiziaria di acquisire e conseguentemente di utilizzare gli elementi di conoscenza e di prova coperti dal segreto».
9. Corte cost., sent. n. 110/1998, citata nota 8.

È questo lo scenario in cui irrompe il Legislatore del 2007 che con la l. 124 ha finalmente dettato, insieme a una disciplina rinnovata del segreto di Stato, un'apposita regolamentazione delle garanzie funzionali.
La soluzione elaborata si pone nel solco della migliore dottrina che aveva evidenziato come essa dovesse essere rintracciata sul piano del diritto penale sostanziale, nell'universo delle cause di non punibilità, affiancandosi poi una scansione procedurale costruita sulla falsariga di quella sperimentata sul versante del segreto di Stato[10].
Il punto di approdo è rappresentato da una causa di giustificazione che pertanto, al ricorrere di determinate, stringenti condizioni, rende lecito il fatto di reato posto in essere dall'agente dei Servizi.
E nella configurazione dei presupposti di tale scriminante si rintraccia parimenti larga eco delle indicazioni provenienti dall'ambito teorico: l'esigenza di fissare paletti oggettivi all'operatività dell'esimente rispetto a determinate forme di aggressione; la necessità che la scriminante sia «tipicizzata in termini di proporzionalità fra i beni e gli interessi in gioco»; l'importanza di assicurare una documentazione della procedura autorizzativa e di prevedere adeguate sanzioni in caso di abusi[11].
L'insegnamento offerto dalle esperienze maturate sul fronte del segreto di Stato consigliava poi di affidare al livello più alto dell'esecutivo la 'gestione' del nuovo meccanismo ideato e di stabilire un chiaro percorso di controllo parlamentare delle decisioni adottate in questo delicato settore, nonché, infine, di contemplare un controllo giurisdizionale, per così dire di ultima istanza, attribuito anche qui alla Corte costituzionale.
Ha preso in questo modo corpo la speciale causa di giustificazione di cui all'art. 17 della citata l. 124/2007 che, per sua espressa previsione, va ad aggiungersi a quella generale di cui all'art. 51 c.p.[12].
Il perimetro 'esterno' della causa di giustificazione è delimitato dal Legislatore facendo ricorso a una tecnica opposta rispetto a quella sperimentata, ad esempio, nel settore delle operazioni sotto copertura. In luogo della previsione di singoli reati autorizzati, si è preferito far riferimento, in chiave però negativa, alla tipologia di bene giuridico escluso: si assiste così a un elenco piuttosto articolato che va dalla vita, all'integrità fisica, alla personalità individuale, dalla libertà personale a quella morale, alla salute o all'incolumità di una o più persone, all'amministrazione della giustizia, con alcune specificazioni. Residuano alcune ipotesi, questa volta identificate in base al richiamo a specifiche disposizioni incriminatrici, det-

10. Fioravanti 1991, p. 466.
11. Flick 1999, pp. 1103-1104; Fioravanti 1991, p. 467; Grevi 1987, p. 566; Pisa 2001, pp. 1457-1459.
12. Per un'analisi complessiva della novella, cfr. Bricchetti et al. 2007, pp. 60-67; *Commento*... 2007, pp. 716-855; Mosca et al. 2008, pp. 243-280; nonché i contributi in Illuminati 2010.

tate però dall'esigenza di coordinamento con lo spettro applicativo del segreto di Stato. I requisiti 'interni' della causa di giustificazione rispecchiano, come accennavo, l'esigenza che la condotta sia: connessa all'esercizio delle attribuzioni funzionali degli appartenenti ai Servizi; indispensabile e proporzionata al conseguimento degli obiettivi dell'operazione, non altrimenti perseguibili; frutto di una specifica comparazione degli interessi pubblici e privati in rilievo; realizzata in modo da arrecare il minor danno possibile agli interessi lesi. Tutte valutazioni che, in linea di principio, sono affidate al presidente del Consiglio, cui compete l'autorizzazione delle condotte e delle operazioni di cui sono parte, secondo la procedura descritta all'art. 18 della l. 124/2007. Rispetto a esse è istituito un penetrante controllo parlamentare affidato al Comitato parlamentare per la sicurezza della Repubblica (Copasir), destinatario, ai sensi del successivo art. 33, co. 4, entro trenta giorni dalla conclusione delle operazioni medesime, di specifica informativa da parte del capo del Governo, il quale trasmette, altresì, a quell'organismo una relazione semestrale avente a oggetto l'attività dei Servizi e altri dati di particolare rilievo (tra cui, ad esempio, l'andamento della gestione finanziaria del Dis e delle due Agenzie nel periodo di riferimento).

Il Copasir può altresì, ai sensi dell'art. 34, richiedere al presidente del Consiglio, laddove elementi acquisiti nell'esercizio delle proprie funzioni lo inducano a procedere all'accertamento della correttezza delle condotte poste in essere da appartenenti o ex appartenenti ai Servizi, di disporre lo svolgimento di inchieste interne, i cui esiti dovranno essere trasmessi al Comitato medesimo.

Assolvono a una sorta di funzione di norme di chiusura del sistema le previsioni di cui all'art. 20, che sanziona in modo severo l'illegittima preordinazione, a opera dei dipendenti dei Servizi, delle condizioni per il rilascio dell'autorizzazione, e all'art. 39, comma 1 bis, che vieta l'apposizione del segreto su «fatti, notizie o documenti concernenti le condotte poste in essere da appartenenti ai Servizi di informazione per la sicurezza in violazione della disciplina concernente la speciale causa di giustificazione».

Per il resto, si istituisce invece un parallelo, quanto a modalità del controllo giurisdizionale, tra segreto e garanzie funzionali: in entrambi i casi, giudice ultimo sarà, allorché sia sollevato dall'Autorità giudiziaria conflitto di attribuzione, la Corte costituzionale alla quale, per la materia di nostro interesse, non potrà essere opposto il segreto.

Infine, la novella introdotta con la legge 7 agosto 2012, n. 133 ha posto rimedio a un possibile profilo di frizione della disciplina dettata dalla legge del 2007 rispetto al tema delle intercettazioni preventive poste in essere dai Servizi[13], opportunamente procedendo alla riformulazione dell'art. 4 del d.l. 27 luglio 2005, n. 144, convertito nella l. 31 luglio 2005, n. 155, che ha esteso la possibilità di utilizzare tale strumento operativo a tutti i settori di attività dei Servizi ex artt. 6 e 7 della l. 124/2007, concentrando nel contempo la potestà autorizzatoria in capo al Procuratore generale presso la Corte di appello di Roma, secondo uno schema ispirato alle esperienze di altri ordinamenti.

13. Aveva sottolineato tale criticità, prima delle modifiche operate nel 2012, Bonetti 2008, p. 50.

NOTE CONCLUSIVE

L'economia di questo lavoro non consente di analizzare più in dettaglio l'articolata disciplina oggi vigente. Il quadro delineato permette tuttavia di svolgere alcune, necessariamente cursorie, riflessioni.

Vorrei muovere da un primo indubbio merito da ascrivere alla legge del 2007: quello di aver fatto uscire il tema delle garanzie funzionali dalla zona grigia in cui era confinato e di averlo, pur con gli opportuni collegamenti, distinto da quello del segreto di Stato.

Sappiamo bene che l'operatività degli appartenenti ai Servizi di sicurezza può comportare anche l'integrazione di fatti di reato e siamo altresì consapevoli che questa attività, a certe condizioni, è non solo fisiologica ma necessaria per salvaguardare la sicurezza della nostra Repubblica.

La l. 124/2007, preso atto di tale realtà, l'ha collocata nella giusta prospettiva, quella delle cause di giustificazione e dunque del bilanciamento tra interessi contrapposti: dobbiamo essere consapevoli che si tratta di condotte lesive di certi beni giuridici – pensiamo anzitutto alla riservatezza nelle sue diverse forme di manifestazione – ma che devono essere considerate lecite in virtù della prevalenza del controinteresse in gioco, che – è bene sempre ricordarlo – ha a che vedere con l'esistenza stessa dell'ordinamento democratico. La legge in parola non assolve però a un compito altrettanto importante, ovverosia quello di definire con precisione chirurgica lo spazio di liceità. L'obiettivo è perseguito dal Legislatore, come si è visto, attraverso la previsione di beni giuridici destinati a prevalere nel bilanciamento; tecnica normativa che è da apprezzare nella misura in cui indica aree per definizione sottratte alla 'licenza di commettere reati' da parte degli agenti dei Servizi – vita, integrità fisica, libertà individuale e morale e così via procedendo – ma che sconta in primo luogo le difficoltà connesse alla precisa identificazione dello spettro di protezione delle singole fattispecie di volta in volta in questione. Ed è emblematico sul punto il dibattito originatosi, già all'indomani della riforma, con riguardo a talune figure criminose la cui ricostruzione in chiave plurioffensiva rimette fatalmente all'interprete la selezione degli interessi in rilievo e, di riflesso, gli spazi di operatività della scriminante[14].

Su altro versante, la scelta compiuta non consente di plasmare la soluzione sulla base delle concrete modalità di azione poste in essere dagli operatori dei Servizi: così si è giustamente rilevato come ben potrebbero darsi casi in cui a un fatto di furto, come tale scriminabile in quanto offensivo del solo patrimonio, si associ una condotta violenta realizzata per assicurarsi il possesso della cosa sottratta, con la relativa qualificazione in termini di rapina impropria[15]. Il saldo finale sarebbe quello di un'esclusione dall'ambito di copertura dell'art. 17 – venendo in rilievo una lesione dell'integrità fisica e/o della libertà morale – di una condotta che sembrerebbe in effetti ragionevole far ricadere al suo interno. Né soccorre il ricorso alla prassi applicativa, atteso che l'esigua giurispru-

14. Sul punto, cfr. in particolare Pisa 2007, pp. 1432 ss.; Bonetti 2008, p. 49.
15. Pisa 2007, p. 1433.

denza sul punto[16] – destinata a rimanere tale, finendo con l'interessare profili patologici o comunque casi in cui sia controversa l'applicazione della scriminante – difficilmente potrà assolvere a un ruolo di orientamento efficace, pur fornendo qualche indicazione in merito. Si potrebbe allora ragionare se, sulla scia della disciplina relativa all'agente provocatore, non sia preferibile invertire l'approccio al tema e indicare in positivo l'elenco delle ipotesi di reato per le quali ammettere la speciale causa di giustificazione. In ogni caso, al di là della verifica operata, in sede di autorizzazione, dal presidente del Consiglio, è e deve rimanere ferma la necessità che sia assicurato, con trasparenza ed efficacia, un controllo capillare in sede parlamentare[17], in grado di offrire ai cittadini una chiara e completa visione delle attività poste in essere dai nostri Servizi di sicurezza.

16. Sul tema delle garanzie funzionali degli appartenenti ai Servizi di sicurezza esiste un unico precedente nella giurisprudenza di legittimità – si tratta della sentenza n. 38356/2014, Traviglia, della sesta sezione della Corte di cassazione – ove il Supremo Collegio, con riferimento a delle condotte di illegittima detenzione e trasporto in luogo pubblico di esplosivi (ex. artt. 10 e 12, l. 497/1974), si è limitato a sancire il principio dell'applicabilità retroattiva della speciale esimente di cui all'art. 17 della l. 124/2007 (sussistendone, ovviamente, tutti i predetti presupposti) anche alle operazioni di intelligence precedenti all'entrata in vigore della novella normativa in commento.

17. I compiti e le funzioni di controllo del Comitato parlamentare per la sicurezza della Repubblica (Copasir) sono disciplinati in modo puntuale dal Capo IV ('Controllo parlamentare') della l. 124/2007 (artt. 30-38). Peraltro, la l. 133/2012, recante alcune modifiche alla legge del 2007 sul riordino dei Servizi, ha notevolmente rafforzato i compiti del Copasir, attribuendogli poteri di controllo maggiormente incisivi sul sistema dei Servizi di sicurezza e diverse funzioni consultive, imponendo altresì al presidente del Consiglio specifici obblighi di comunicazione nei confronti del Comitato.

BIBLIOGRAFIA

Commento articolo per articolo – L. 3.8.2007, *n*. 124, «Leg. Pen.» (2007).

G. Amato, L*e garanzie funzionali per gli 'operatori' di* I*ntelligence*, «Gnosis» (2011) 3.

P. Bonetti, P*rofili costituzionali delle garanzie funzionali per gli agenti dei* S*ervizi di informazione per la sicurezza*, «Percorsi Costituzionali» (2008) 1.

R. Bricchetti et al., G*aranzie funzionali agli* '007', «Guida al diritto» 40 (2007).

L. Fioravanti, L*inee di un nuovo statuto penale degli appartenenti ai* S*ervizi segreti*, «Riv. it. dir. e proc. pen.» II (1991).

G.M. Flick, P*rincipi di legittimità e legalità nell'attività degli* O*rganismi di intelligence anche con riferimento alle norme di diritto penale e processuale penale*. (L*e garanzie funzionali*), «Per aspera ad veritatem» 15 (1999).

V. Grevi, S*punti e variazioni in tema di rapporti tra segreto di stato e servizi di sicurezza*, «Politica del Diritto» 4 (1987).

G. Illuminati (a cura di), N*uovi profili del segreto di* S*tato e dell'attività di intelligence*, Giappichelli, Torino 2010.

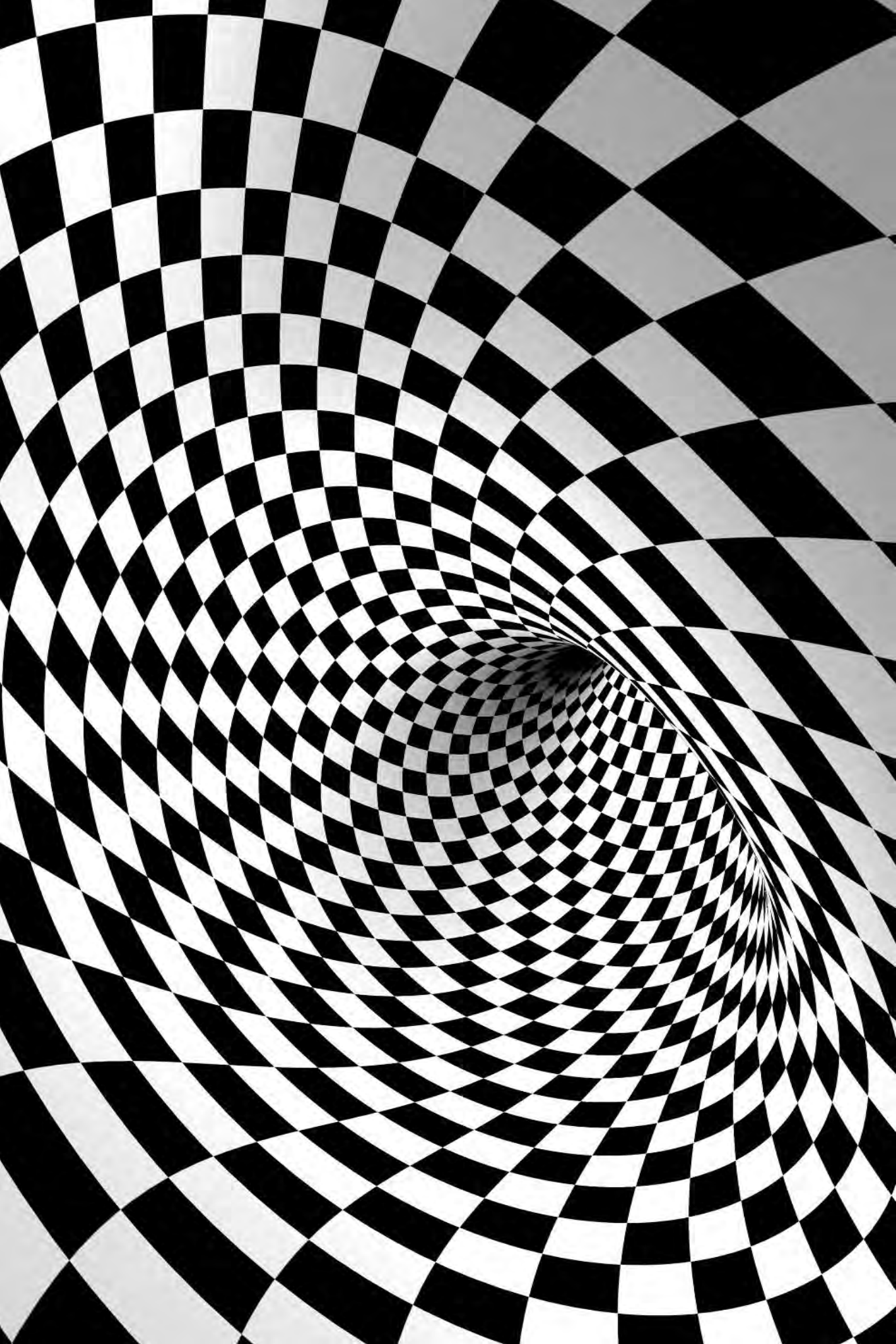
C. Mosca et al., I S*ervizi di informazione e il segreto di* S*tato*, Giuffrè, Milano 2008.

P. Pisa, S*ervizi segreti e* S*tato di diritto*, «Diritto penale e processo» XII (2001).

P. Pisa, L*e garanzie funzionali per gli appartenenti ai* S*ervizi segreti*, «Diritto penale e processo» XI (2007).

C. Santoriello, L*a sentenza costituzionale n*. 110 *del* 1998 *in tema di opposizione del segreto di* S*tato e poteri dell'autorità giudiziaria*: *una pronuncia con molte luci e qualche ombra*, «Giur. It.» IV (1999).

D. Spirito, S*egreto di* S*tato e funzione giurisdizionale*: *bilanciamento o prevalenza di interessi*?, «Riv. it. dir. e proc. pen.» II (1979).



LA DEFINIZIONE DI INTERESSE E SICUREZZA NAZIONALE ECONOMICO-FINANZIARIA IN EPOCA DIGITALE

Gianmario Verona

Il presente contributo intende semplicemente porre alcuni quesiti, ancora privi di risposta, che tuttavia vengono alimentati da due importanti traiettorie evolutive che caratterizzano la società del XXI secolo in ogni angolo del mondo, indipendentemente dai singoli Paesi e dai rispettivi governi. Ci si riferisce alla crescente importanza dell'economia nella vita individuale e sociale e all'impatto innovativo della tecnologia digitale, in progressivo aumento.

Di seguito verranno illustrate e, in conclusione, si porranno una serie di domande che evidenziano il ruolo dei sistemi d'interesse e di sicurezza nazionale, destinato a diventare non solo sempre più cruciale e centrale, ma anche più evoluto dal punto di vista dei processi e dei contenuti.

Prof. Gianmario Verona, rettore dell'Università commerciale Luigi Bocconi.

Una delle tante eredità del secolo che ci siamo lasciati alle spalle è legata al peso sempre più rilevante dell'economia nella società. Seppur sia difficile trovarne una definizione univoca e onnicomprensiva, essa è quella disciplina che si preoccupa di comprendere e studiare gli effetti dell'allocazione di risorse tra attori che sono parte di un sistema e ha come oggetto le transazioni, che includono processi che contemplano attività quali la produzione, il consumo e il relativo finanziamento, quest'ultimo tipico delle economie sviluppate.

Come si può ben intendere da questa descrizione approssimativa, essa non pertiene al novero delle cosiddette scienze 'dure', ovvero le scienze naturali, essendo invece categorizzata nel novero delle scienze 'deboli' e, in particolare, di quelle sociali, che studiano il comportamento dell'essere umano nell'ambito della società. Sono 'deboli' in quanto faticano a identificare regole solide che siano cristallizzabili in modelli. Infatti, l'interazione tra le variabili è così complessa e dipendente da fattori contingenti da richiedere molteplici studi per poter assurgere a teoria. Ciononostante, l'economia ha un impatto indiscusso sul comportamento umano.

Seppur dalla nascita dell'umanità abbia ricoperto un ruolo cruciale – il baratto è una delle prime forme di transazione rappresentate nei libri di storia e le guerre raccontate dagli stessi libri sono spesso causate dall'intento di controllare risorse naturali che hanno un valore economico singolare – nel corso del XX secolo essa è divenuta un perno della società, in cui le persone esercitano il proprio ruolo in qualità di consumatori, risparmiatori, lavoratori e imprenditori. L'evoluzione della società e la sua complessità portano, anzi, i singoli individui a manifestare aspettative crescenti rispetto ai ruoli economici che vanno in essa a rivestire. Il sociologo Maslow le ha ben espresse, enfatizzando come esse vadano a cogliere obiettivi che, da materiali, divengono sempre più introspettivi e legati al ruolo che l'individuo ricopre nella società. Analogamente, le organizzazioni, siano esse *not for profit*, o imprese che producono beni (industriali o servizi), o istituzioni di vario genere, in aggiunta a un loro ruolo sociale presentano sempre una componente economica di rilievo, la cui importanza si è ampliata nel corso del tempo.

Col passare degli anni, l'economia ha assunto una funzione nevralgica anche nei sistemi d'interesse e di sicurezza nazionale, che non possono prescindere dagli equilibri – sociali, politici e militari – che la macroeconomia dei Paesi e la microeconomia dei settori producono in ogni istante della vita quotidiana. Tale impatto è ulteriormente sostenuto dall'avvento della tecnologia digitale, fondata su una serie di innovazioni degli anni Novanta: dalla convergenza degli sviluppi delle telecomunicazioni con il mainframe e personal computer, alla diffusione della rete internet, evolutasi in un sistema che permette la dematerializzazione della memoria in quello che oggi viene definito

cloud. Le sfaccettature che essa assume, sino a oggi sconosciute, presentano proprietà incommensurabili con altre tecnologie, tra cui l'orizzontalità, la globalità e la natura *disruptive*.

Al pari dell'energia elettrica che ha rivoluzionato la vita e le fabbriche del secolo scorso, essa ha una natura orizzontale rispetto ai settori cui si applica: è definibile come una *general purpose technology*, una sorta di tecnologia generalista. Infatti – a differenza di altre che insistono su singole industrie – impatta in modo trasversale sui settori di ogni economia. Diversamente da altre tecnologie che pure hanno un general purpose quali, ad esempio, le macchine a vapore e l'energia elettrica, è anche 'evolutiva', presentando una spinta di graduale miglioramento che la rende progressivamente più innovativa. Dalla diffusione di internet alla produzione delle app degli smartphone dell'inizio di questo millennio, all'industria 4.0 che fa intravedere la robotica e l'intelligenza artificiale applicata nelle fabbriche e nei servizi, la tecnologia digitale sta irreversibilmente occupando spazi sempre maggiori nei singoli settori, ridisegnandone le logiche di produzione, di distribuzione e di consumo. Oltre a essere globale, in quanto ha modificato le dinamiche sottostanti il processo di espansione internazionale, è analitica e capillare, atteso che la diffusione di internet e dei social media ha dato vita a una nuova forma di personalizzazione molecolare, che consente a imprese e singoli individui livelli d'interazione che fino a non molti anni addietro erano accessibili solo alle grandi organizzazioni, con tempi e costi ridottissimi rispetto al passato e destinati ulteriormente a diminuire. La peculiarità di tale tecnologia è, però, la sua natura, spesso definita disruptive. A differenza di altre, la sua forza risiede nell'attivazione di un percorso a due vie, in cui la domanda riveste un ruolo cruciale. In questo, è foriera di stimoli d'interazione che investono i singoli cittadini e che mai, sino a oggi, la vita economica e industriale aveva conosciuto. Essa, cioè, mette l'individuo al centro dell'interazione e, in quanto tale, genera processi di scambio sinora impensati.

Ne è stato rivoluzionato il nostro modo di comunicare e sono state trasformate le industrie che si occupano d'informazione e di comunicazione (dai giornali fisici alla televisione). Ha inciso anche sul modo in cui acquistiamo i prodotti (con l'avvento dell'e-commerce ha varcato la percezione del rilievo dei punti di vendita). Ma la cosa più importante è che la tecnologia digitale sta innovando le modalità in cui ci informiamo e apprendiamo (si pensi a quanto sta accadendo al settore dell'istruzione, che è sul punto di essere rivoluzionato dai nuovi canali digitali) e quelle in cui alimentiamo la nostra fiducia nei confronti di terze parti, per non parlare delle irreversibili novità nel modo in cui lavoriamo.

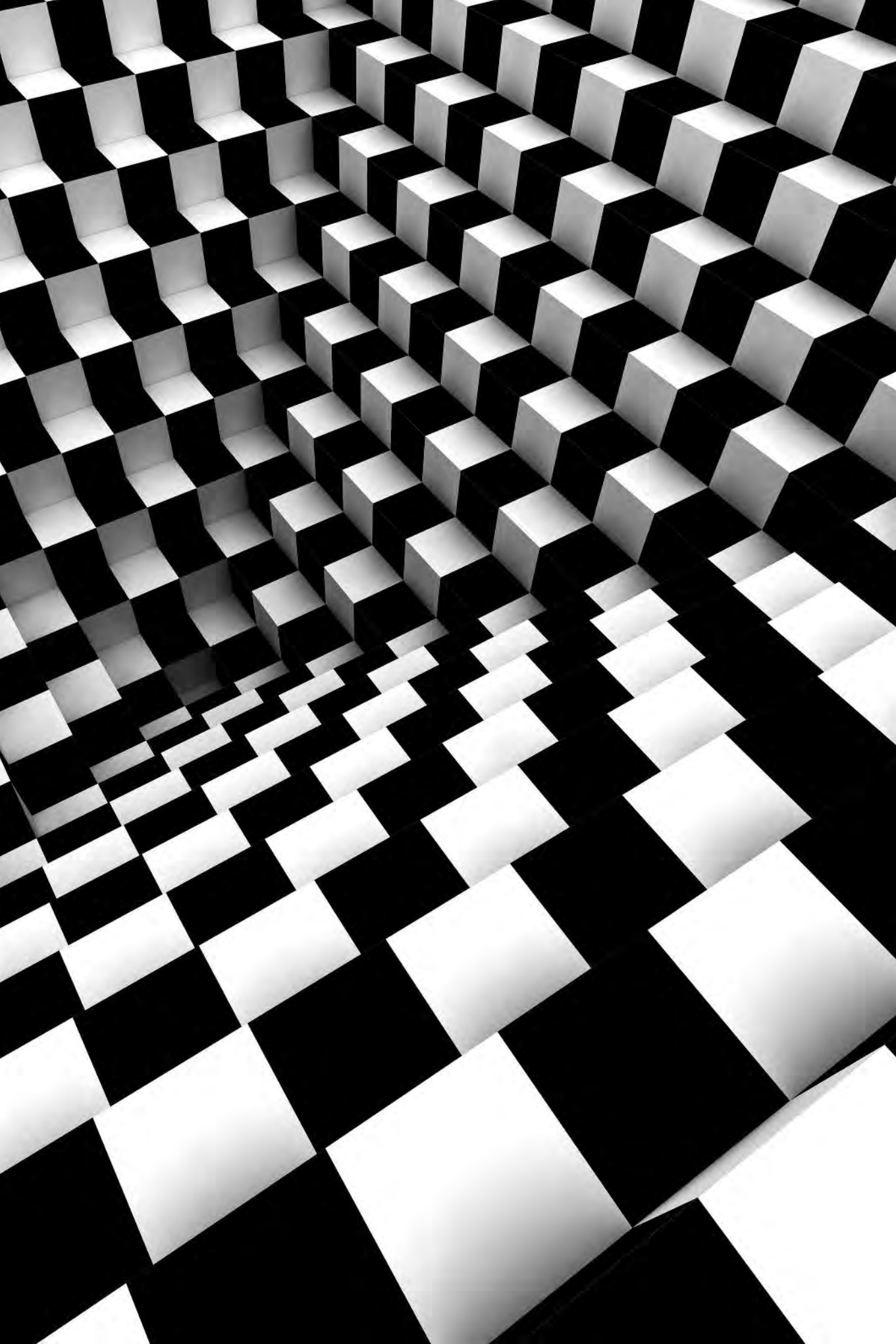
Se questa trasformazione profonda apre nuove opportunità per le organizzazioni e per i singoli individui, è evidente che a essa si legano altrettanti rischi che devono essere costantemente monitorati.
A livello micro pensiamo, ad esempio, alla cybersecurity, alla tutela dei consumatori e dei cittadini nonché della loro privacy, che vengono minate in modo drastico, tradendo la loro libertà individuale. Pensiamo all'intento consumeristico di soggetti che si connettono a siti per alimentare un desiderio di svago o per finalizzare una transazione economica e la cui identità viene violata. Pensiamo alle conseguenze di un classico fenomeno teorico bancario, ovvero 'la corsa agli sportelli' (*bank run*) che, nel caso della finanza on line, può avvenire in nano-secondi.
Naturalmente la dimensione economico-finanziaria è solo una parte del problema, ben più ampio. Consideriamo le implicazioni drammatiche nel campo delle cosiddette fake news con riferimento alle recenti elezioni politiche statunitensi, che sembrano aver inciso direttamente sull'elettorato americano. Ma poniamo mente anche a fenomeni d'informazione immediata che hanno un risvolto non negativo, quali la Primavera araba o l'allerta di fronte a eventi terroristici.
L'avvento dei Big Data dischiude opportunità incredibili dal punto di vista della comprensione dei meccanismi di funzionamento della società ma, allo stesso tempo, rende sempre più deboli i nodi del sistema sociale interconnesso dalla rete. Sorgono infinite domande, che riflettono l'esigenza di un approfondimento delle implicazioni che economia e dati digitali pongono alle società del XXI secolo. Tra le tante, alcune hanno priorità:
– quali sono i diritti degli operatori della rete?
– come possono tali diritti essere coniugati con i principi di libertà individuale, alla luce dei quali sono sottostimate le implicazioni del comportamento nella rete dei singoli cittadini?
– quali sono i diritti degli operatori che regolano le attività economico-finanziarie dei cittadini e che sono amplificati nell'ambito della rete?
– che tipo di controllo è opportuno esercitare per evitare la violazione dell'interesse della libertà individuale e nazionale?
– che tipo di interazione deve sussistere tra sistemi d'interesse e sicurezza nazionale di diversi Paesi?
– quali meccanismi di coordinamento consentono di prevenire problemi di natura globale?

Queste sono banali domande la cui risposta è complessa, postulando conoscenze giuridiche, sociologiche, economiche e politiche, che vanno ben oltre le competenze dell'autore di questo scritto.

L'epoca che stiamo vivendo è straordinaria: tutti i principali macro parametri danno evidenza a una traiettoria evolutiva rispetto alle generazioni che ci hanno preceduto (numero di guerre, vita media delle persone, reddito medio degli individui ecc.). Abbiamo, inoltre, l'opportunità di valorizzare ulteriormente questo progresso, facendo leva su quanto economia e tecnologia permettono di ottenere. Ciononostante, permangono plurimi quesiti che necessitano di una risposta, che può rappresentare una soluzione per favorire un percorso di crescita lineare e coerente con quanto l'umanità, sin dalla sua origine, ha dimostrato di produrre.

BIBLIOGRAFIA

D. Besanko et al., *Microeconomic*, John Wiley & Sons Inc, New York 2008[3] (International Student Version).
O. Blanchard et al., *Macroeconomics*. A *European Perspective*, Pearson, UK 2017.
E. Brynjolfsson et al., *The Second Machine Age*: *Work*, *Progress*, *and Prosperity in a Time of Brilliant Technologies*, MIT Press, Cambridge 2014.
R.M. Grant, *Contemporary Strategy Analysis*, Ninth Edition, Wiley, UK 2016.
J. Manyika et al., *Digital globalization*: *The new era of global flows*, McKinsey Global Institute, New York 2016.
P. Milgrom et al., *Economia Organizzazione e Management*, il Mulino, Bologna 1994.
E. Prandelli et al., *Vantaggio competitivo in rete*. *Dal web* 2.0 *al cloud computing*, McGraw-Hill, Milano 2011.
J. Tirole, *The Theory of Corporate Finance*, Princeton University Press, Princeton and Oxford 2006.
J. Tirole, *Economics for the Common Good*, Princeton University Press, Princeton and Oxford 2017.
E. Von Hippel, *Democratizing Innovation*, MIT Press, Cambridge 2005.
World Economic Forum, *The Future of Jobs*: *Employment*, *Skills and Workforce Strategy for the Fourth Industrial Revolution*, Global Challenge Insight Report 2016.



UNA NUOVA STAGIONE DI STUDI SULL'AFRICA

PARTENARIATO TRA INTELLIGENCE E UNIVERSITÀ

Elda Morlicchio

Con la legge istitutiva del Regio Istituto Orientale del 1888 l'offerta formativa di lingue del Mediterraneo e dell'Africa aumentò, proprio mentre prospettive coloniali italiane si materializzavano per Libia e Corno d'Africa. Tra le discipline principali si annoveravano varie lingue del Mediterraneo allargato (arabo volgare, turco volgare, amarico, persiano, armeno) mentre tra le complementari figurava «legislazioni dell'Asia e dell'Africa e loro condizioni storiche ed economiche rispetto all'Europa e specialmente all'Italia».

Dopo la guerra italo-turca fu creato il ministero delle Colonie, con competenza sui quattro governatorati africani: Eritrea, Somalia italiana, Tripolitania e Cirenaica. Nel 1911 fu avviato un riordino del Regio Istituto Orientale con lo scopo di creare quadri coloniali sia nel settore amministrativo che in quello linguistico. La legge 19 giugno 1913, n. 800 pose l'Istituto «alla dipendenza del ministero delle Colonie» e stabilì che rilasciasse diplomi di «cultura coloniale», miranti a «una completa e pratica conoscenza delle Colonie italiane», e diplomi di «interprete» per il perfezionamento nel Paese della lingua studiata.

Prof.ssa Elda Morlicchio, rettore dell'Università L'Orientale di Napoli.

Anche se la dipendenza dal ministero delle Colonie durò meno di un decennio, per l'Orientale segnò una svolta importante e comportò un notevole ampliamento dell'offerta formativa, in parallelo con il rafforzamento delle ambizioni coloniali italiane. Nel 1918 erano attive varie discipline attinenti al bacino mediterraneo e all'Africa orientale: albanese, amarico, arabo, berbero, turco.
Nel 1923, su proposta del nuovo ministro delle Colonie, Luigi Federzoni, il Regio Istituto Orientale tornò alla dipendenza del ministero della Pubblica istruzione; successivamente, con il Regio d.l. del 15 agosto1925, n. 1603 fu riconosciuto il grado di Istituto di studi superiori all'Orientale che, tuttavia, continuava a rilasciare «diplomi d'interprete» agli «interpreti e dragomanni per i servizi dei ministeri degli Esteri e delle Colonie». Tra il 1925 e il 1935 nell'Istituto si sviluppò molto il settore dell'etiopistica, in cui spiccava la figura di Francesco Beguinot, ordinario di berbero dal 1914, non ignaro di arabo e lingue del Corno d'Africa. Nel settore arabistico aveva ancora influenza Carlo Alfonso Nallino, sebbene questo settore fosse guardato con sospetto dopo che studiosi come Leone Caetani e Giorgio Levi Della Vida avevano lasciato l'Italia o si erano rifiutati di prestare giuramento.
L'amministrazione ordinaria dell'Orientale, condotta da Alberto Geremicca per un decennio (1926-1935), si concluse con la nomina dell'onorevole Bernardo Barbiellini Amidei a commissario straordinario, le cui competenze, concentrate soprattutto sul Caucaso, erano il presupposto di un piano molto ambizioso, presumibilmente studiato con Galeazzo Ciano, ministro della Stampa e della propaganda dal 1935. Il piano prevedeva la trasformazione dell'Orientale in una centrale di propaganda antibritannica e antisovietica. Nel contrasto alla Gran Bretagna, a suo giudizio, si doveva utilizzare l'arma delle lingue nazionali; poiché la Gran Bretagna, per estendere la sua influenza nei Balcani pubblicava il mensile «Balkan Herald», l'Orientale avrebbe dovuto promuovere «un mensile balcanico redatto nelle lingue dei principali Paesi di quella regione». Inoltre, siccome la Gran Bretagna aveva mandato su Iraq, Giordania e Palestina, Barbiellini Amidei proponeva di riprendere la pubblicazione dell'«Avvenire Arabo» per risvegliare l'orgoglio nazionale arabo. Perfezionò, inoltre, un piano di accerchiamento linguistico dell'Unione Sovietica con l'attivazione dell'insegnamento di tutte le lingue parlate nei Paesi con essa confinanti (ugrofinniche, baltiche, balcaniche, caucasiche), ciò che rimase – nel complesso – patrimonio dell'Orientale. Barbiellini fu rimosso dall'incarico di commissario il 16 luglio 1938: il giorno stesso fu sostituito da Michelangelo Guidi. All'Orientale le autorità del regime avevano deciso di assegnare il ruolo di avamposto degli studi africanistici italiani, sgombrando il campo da chi, invece, ne chiedeva il declassamento a sezione di un'erigenda, grande «Università coloniale». Nel 1940 Guidi fu nominato accademico d'Italia e direttore dell'Istituto in sostituzione di Francesco Beguinot.

Il Regio decreto 24 ottobre 1941, n. 1616 sanzionava la posizione privilegiata dell'Orientale come centro di formazione della burocrazia coloniale: presso il corso di laurea in Scienze coloniali, fiore all'occhiello del regime, era istituita la Scuola di perfezionamento e alti studi coloniali e l'Orientale appariva allora come un ateneo con impronta più africanistica che orientalistica. La disfatta italiana nel Corno d'Africa causò lo scioglimento della Scuola; con la caduta di Tripoli (gennaio 1943) anche la Libia era perduta e l'Italia non aveva più colonie. La laurea in scienze coloniali, pertanto, non aveva più senso ma, nonostante il drastico calo degli iscritti, il corso di laurea resisteva, strenuamente difeso da comitati di docenti e di studenti.
Tuttavia, i tempi erano cambiati e, con il nuovo direttore Leone Pacini Savoj, nel 1957 furono aboliti sia il corso di laurea sia l'annessa Scuola di perfezionamento e, nello stesso anno, l'Orientale diventava ateneo statale. Un successivo decreto del presidente della Repubblica (20 settembre 1966, n. 926) introduceva la laurea in «Scienze politiche per l'Oriente», destinata al reimpiego dei docenti di materie giuridiche del corso di laurea in Scienze coloniali. Agli inizi degli anni Settanta (rettore Gherardo Gnoli), l'Istituto divenne un ateneo con più facoltà e si ampliò il versante umanistico degli studi delle culture africane. Accanto a discipline introdotte allora per la prima volta (egittologia, antichità libico-berbere, archeologia dell'Etiopia) e al rafforzamento degli studi etnografici, antropologici e religiosi rivolti all'Africa, si allargò notevolmente lo spettro dello studio scientifico delle lingue africane, che arrivò a comprendere, tra le altre, somalo, swahili, zulu, hausa, ge'ez. In tale quadro di rinnovamento venne creato il Dipartimento di studi e ricerche su Africa e Paesi arabi, l'unico in Italia che recasse questo continente nel proprio nome. Quando nel 2012 furono abolite le facoltà, gli studi africanistici si concentrarono nel nuovo grande Dipartimento Asia, Africa e Mediterraneo, il maggiore di siffatta tipologia nelle università italiane.

SPUNTI DI ANALISI

Analisi politiche, economiche e sociali indicano che l'Africa diventerà, entro i prossimi vent'anni, un polo geopolitico e geoeconomico di primaria importanza nei mutevoli equilibri globali. Vaste zone del continente saranno sempre più al centro di flussi economici e d'interscambi di beni e persone. Attualmente il Sudafrica è una delle cinque principali economie emergenti del globo, mentre del gruppo delle 15 Eagles (E*merging and growth-leading economies*) fanno parte Egitto e Nigeria. È previsto che dell'elenco dei Paesi che nel prossimo decennio avranno un forte sviluppo del Pil facciano parte anche Algeria, Libia (se la situazione interna si stabilizzerà), Marocco, Etiopia e Mozambico.

Le profonde trasformazioni che coinvolgeranno il continente porteranno sia opportunità che rischi. In particolare, l'Africa settentrionale sarà probabilmente caratterizzata, nel prossimo quinquennio, da instabilità politica causata dal difficile rapporto tra élite e popolazione – che potrebbe indurre in alcuni Paesi un ulteriore indebolimento delle istituzioni nazionali – e dal peggioramento delle condizioni economiche. Inoltre, i rischi di crisi ambientali connessi anche ai cambiamenti climatici rimarranno particolarmente elevati in tutto il continente e incideranno negativamente sulla disponibilità di risorse idriche e alimentari a favore di una popolazione sempre più urbanizzata. Tutto ciò potrebbe causare, indirettamente, anche l'esplosione di crisi di natura sanitaria. È però prevedibile che fenomeni d'instabilità riguarderanno anche altri Paesi dell'Africa sub-sahariana, alimentando conflitti armati che si aggiungeranno a quelli in atto, i quali – a loro volta – avranno effetti diretti (distruzioni, saccheggi e morti) e indiretti (flussi di profughi nei Paesi vicini) che aggraveranno ulteriormente la situazione economica e le condizioni di vita.

Gli strumenti usualmente adoperati dalle élite locali per gestire il malcontento saranno limitati a causa di vari fattori economici, quali la riduzione nei prezzi del greggio e il graduale passaggio di molte industrie manifatturiere e di settori del terziario a nuove tecnologie automatizzate, che causerà profondi cambiamenti nell'impiego della manodopera, anche nei maggiori Paesi industrializzati. Attualmente risulta già evidente che nell'Africa sub-sahariana la chiusura di impianti minerari e di fabbriche ha causato il ritorno ad attività agricole.

È possibile identificare alcuni principali *drivers* di cambiamento. In sintesi:

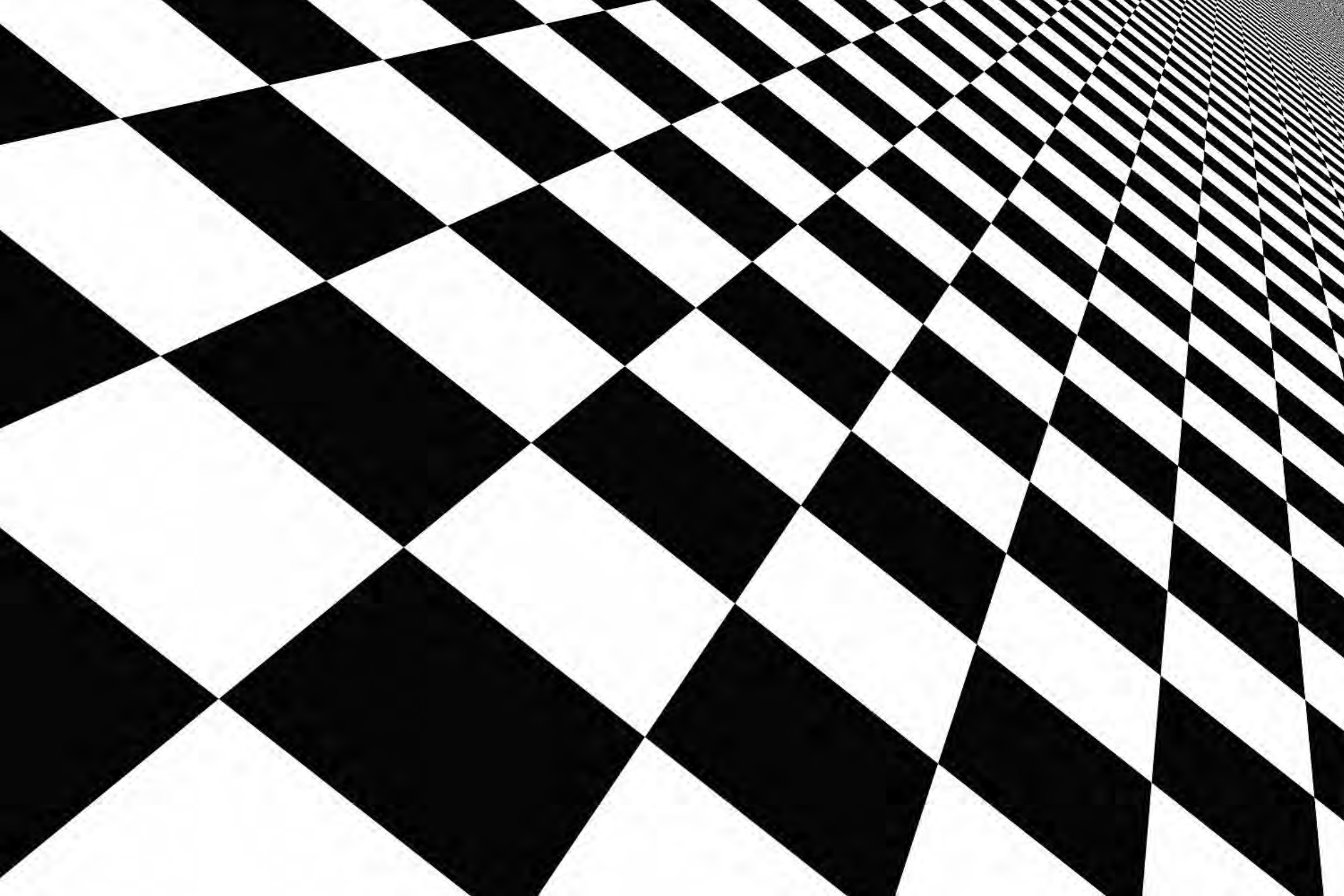
- esplosione demografica;
- cambiamenti climatici e connessa riduzione di disponibilità idrica e di produzione di cibo in varie zone del continente;
- veloce cambiamento delle classi dirigenti in alcuni Paesi del continente e, per converso, estrema resilienza da parte di altre;
- utilizzo spregiudicato di strumenti estremi di mobilitazione socio-politica quali rivalità etniche o claniche ed estremismo religioso;
- sviluppo economico ineguale e conseguente aumento delle già gravi disuguaglianze;
- rivoluzione tecnologica;
- utilizzo intensivo dei terreni agricoli e, più in generale, delle risorse naturali.

Sia per la prossimità al territorio nazionale che per i rapporti esistenti con il sistema Paese, l'Africa costituisce una delle aree di maggiore importanza per gli interessi italiani. Un dato da sottolineare è la complessità delle realtà racchiuse nella definizione di «Africa», che fanno sì che non si possa

parlare di una realtà unica. Oltre al Nordafrica troviamo, scendendo verso sud e passando per l'Africa sub-sahariana, contesti molto diversi con problematiche ereditate dal passato e dall'età coloniale – rese in molti casi ancora più gravi dalle evoluzioni recenti – né vanno dimenticate altre parti del mondo in fase di crescita con grandi chances dal punto di vista economico, sociale e politico. Va ancora ricordato che la complessità si sposa con un processo di revisione dei confini e con il fenomeno migratorio: quest'ultimo sia 'tra Sud e Sud' – cioè tra diversi Paesi africani – sia da sud verso il Nordafrica o verso l'Europa. In tale ottica, è fondamentale conoscere il più possibile le origini storiche e culturali dei potenziali fattori di frammentazione e le direttrici di ricomposizione delle entità politiche.

IL RUOLO DELLE UNIVERSITÀ ITALIANE INSIEME ALLE ALTRE ISTITUZIONI DEL PAESE

Nonostante il passato coloniale, l'Italia dispone di un enorme potenziale. I rapporti economici indicano chiaramente che pur senza i mezzi di altri Paesi europei / occidentali il sistema Italia è in grado di parlare con le diverse realtà e di spendere un patrimonio culturale che non è in genere percepito come compromesso con politiche (neo-)coloniali (ad esempio, francesi, inglesi, statunitensi, attualmente cinesi). In tale ottica non va tralasciata la futura importanza degli immigrati provenienti dalle varie regioni dell'Africa e ora residenti in Italia e/o cittadini italiani. Costoro, e ancor di più i loro figli (cresciuti e, spesso, anche nati in Italia) costituiranno in futuro un ulteriore fattore di relazione prezioso e, quindi, uno strumento virtuoso nei rapporti tra Italia e Paesi africani. Poter contare su questi nuovi cittadini e avere un rapporto privilegiato con quelle diverse situazioni – l'emigrazione in Italia è variegata e non è ridotta che a poche nazionalità – può essere un fattore importante per la nostra presenza in Africa. In questo senso va ricordato il concetto di co-sviluppo: l'effetto 'virtuoso' che la diaspora in Paesi a elevato sviluppo economico può avere nella creazione di nuove opportunità di lavoro e di rapporti economici con i Paesi di origine. Altrettanto importante, per la creazione di rapporti 'facilitatori' di relazioni istituzionali ed economiche più consistenti, è il ruolo che le università italiane già svolgono nella formazione di nuovi professionisti e quadri dirigenti di molti Paesi, sia a livello di dottorato di ricerca sia attraverso accordi di cooperazione e di scambio con istituzioni di formazione superiore in Africa. A questo riguardo molto si può fare con costi relativamente ridotti, accrescendo il numero delle borse di studio, migliorandone la gestione da parte di nostri enti governativi, creando canali agevolati tra i borsisti africani e gli organismi del nostro ministero dell'Interno.



Per tali ragioni, i processi di diffusione culturale relativi a più approfondite conoscenze sulle realtà africane e sui grandi spazi ancora esistenti nella costruzione delle diverse identità, anche attraverso un maggior impegno delle università e dei centri di ricerca, dovrebbero essere incoraggiati anche in ambito umanistico. Essi, infatti, costituiscono un veicolo di approccio culturale in senso ampio, puntando a quei settori che incidono nelle conoscenze della realtà del 'sistema mondo', non più richiuse su capitoli o fenomeni della sola storia europea o italiana. In questo senso può svolgere un ruolo importante l'Università degli studi L'Orientale di Napoli, che ha stipulato accordi con atenei di tutto il continente africano e nella quale vengono insegnate tra l'altro:

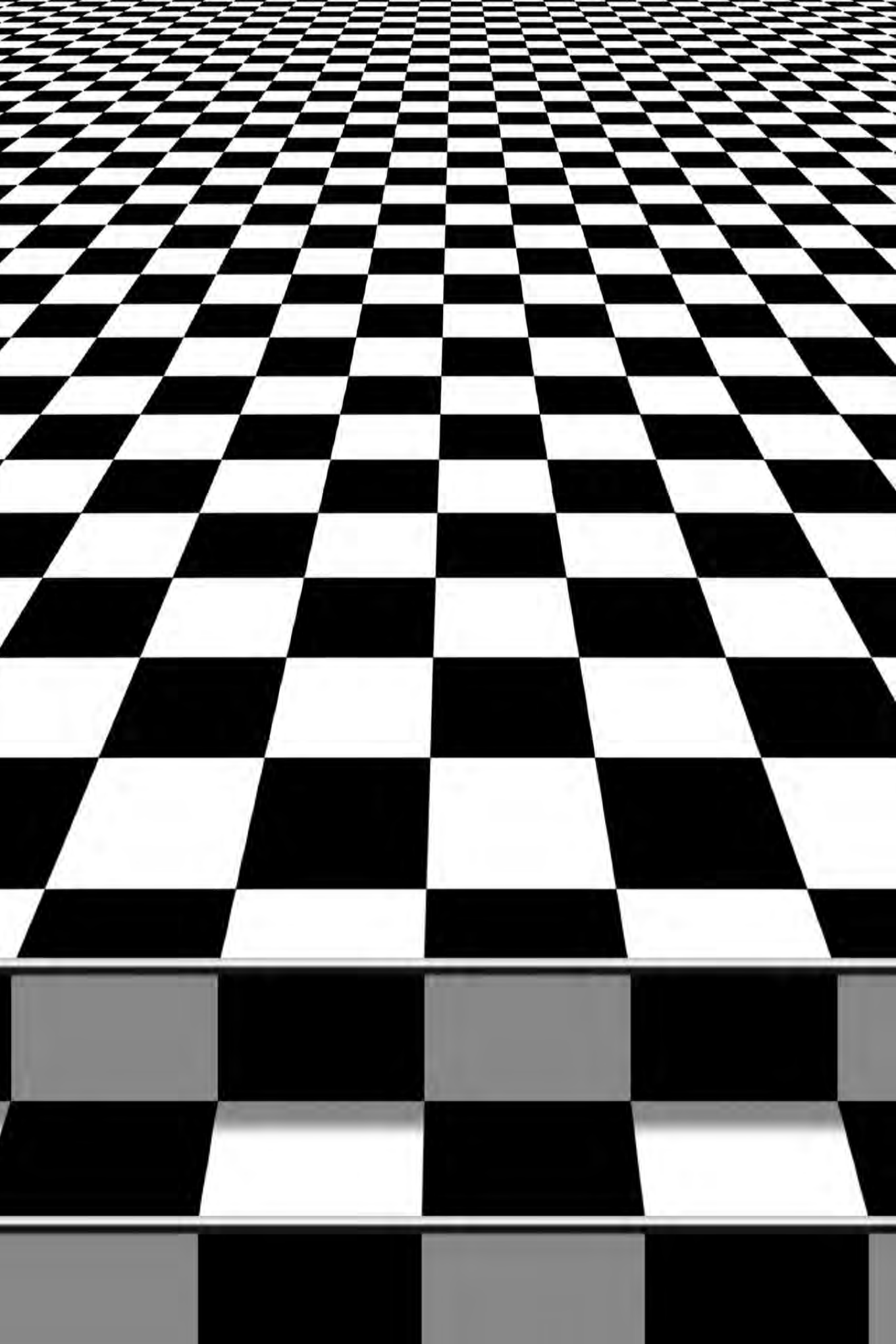
– lingua e letteratura hausa (Nigeria, Niger, Ciad e Paesi circostanti);
– lingua e letteratura swahili (Kenya, Uganda, Tanzania, Congo ex Zaire);
– lingua e letteratura amarica (Etiopia);
– lingua e letteratura somala (ex Somalia, Djibouti, Etiopia e Kenya);
– lingua e letteratura berbera (Paesi del Nordafrica, dall'Egitto alla Mauritania);
– discipline attinenti all'archeologia e ai beni culturali dell'Africa orientale (dal Sudan alla ex Somalia), strategiche nel quadro della 'politica estera attraverso l'archeologia';
– islamistica;
– discipline storiche, giuridiche ed economiche riguardanti l'Africa settentrionale e, più in generale, i Paesi musulmani;
– storia e istituzioni dell'Africa.

CONCLUSIONI

La collaborazione tra intelligence e università – consolidata dalla riforma ex l. 124/2007 che inserisce stabilmente rappresentanti delle eccellenze accademiche nei vertici della Scuola di formazione e rende possibili convenzioni con università e centri di ricerca – costituisce un virtuoso volano per la realizzazione di un fruttuoso percorso di studi sulle dinamiche presenti e future, geopolitiche e geostrategiche del continente africano.

La progettualità in questi campi passa necessariamente dalla capacità di orientarsi nelle complessità locali di ordine culturale, religioso, sociale, etnico, linguistico, di storia antica e/o coloniale nonché di storia politica recente.

In questo quadro diventa centrale per l'Italia il coordinamento nell'utilizzo sistemico delle risorse strategiche, politiche e culturali con una visione complessiva che coinvolga anche gli studi superiori.



IMPRESE E SICUREZZA NAZIONALE

Massimo Bergami

«L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali»[1]. I padri costituenti nell'articolo 41 della Carta avevano chiaramente previsto la necessità di armonizzare libertà d'iniziativa con sicurezza e altri interessi nazionali. Si tratta di una sintesi tra principi liberisti e prospettiva socialista che, se da una parte pone alcuni limiti, dall'altra nobilita l'intervento privato, attribuendogli esplicitamente finalità di utilità collettiva[2].

Prof. Massimo Bergami, docente universitario.

1. Costituzione della Repubblica Italiana 1947.
2. Galgano et al. 1982.

Le forme in cui il rapporto tra impresa e interesse collettivo è stato disciplinato dallo Stato sono numerose, a livello sia centrale sia periferico, anche in applicazione di norme comunitarie. Questo connubio di regole ispirate a impostazioni ortogonali, spesso mediato da principi riconducibili alla dottrina sociale della Chiesa, ha portato anche in Italia ad alcuni tentativi di programmazione economica, soprattutto negli anni Sessanta e Settanta, per lo più superati dalla dinamica reale dell'economia, già difficilmente prevedibile anche quando il grado di incertezza era di gran lunga inferiore a quello attuale. Superata questa fase, «le politiche» di economia industriale, per usare un termine caro a Beniamino Andreatta[3], hanno progressivamente perso intensità, mentre l'azione dei governi si è concentrata prevalentemente su interventi monetari e fiscali. In maniera intermittente, gli esecutivi hanno cercato di intervenire nell'economia reale, come nel caso delle privatizzazioni e delle liberalizzazioni, ma l'instabilità politica ha fortemente limitato una progettualità di cui il Paese avrebbe avuto bisogno. Il dibattito sull'intervento nell'economia si è acceso di tanto in tanto in occasione di operazioni di acquisizione (più o meno riusciti) da parte di operatori stranieri, in quanto la perdita d'imprese importanti è stata vista come un indebolimento del Paese e da parte di alcuni è stata posta la questione dell'interesse nazionale e dell'opportunità di difendere asset importanti per l'economia e per la sicurezza del Paese.

Dalla nascita della Repubblica, tuttavia, la tutela della sicurezza, intesa come bene pubblico, si è concentrata su aspetti riguardanti altri settori della società (difesa, ordine pubblico, criminalità, salute), mentre in ambito economico l'attenzione si è rivolta prevalentemente a sicurezza sul lavoro, sicurezza amministrativa e tutela della proprietà intellettuale. Solo recentemente, il concetto di sicurezza ha iniziato ad abbracciare altri aspetti, prendendo in esame i modelli di governance delle imprese o l'attività economica di organizzazioni criminali, fino all'approvazione del codice antimafia dell'ottobre 2017. Anche la normativa in materia ambientale, coerentemente con quanto sta avvenendo a livello internazionale, sembra aver preso una prospettiva di ampio respiro, considerando la sicurezza come concetto alto e non meramente regolatorio o sanzionatorio. La visione di un mondo sostenibile, rispecchiata nei *Sustainable Development Goals* delle Nazioni Unite[4], corrisponde a un'idea di sicurezza della società e delle persone. Resta il fatto che, in Italia, la condivisione del concetto di sicurezza sia ancora acerba, per motivi storici e culturali, anche se la storia degli ultimi cento anni avrebbe dovuto, all'opposto, suggerire di occuparsi molto di più di questo aspetto.

3. Prodi 2016.
4. United Nations 2015.

Come noto, sicurezza deriva da sicuro, dal latino *securus*, cioè tranquillo, senza preoccupazioni (comp. di *se*, che indica separazione o privazione, e *cura* «preoccupazione»[5]), un aggettivo che non descrive propriamente la condizione delle imprese contemporanee.

Nel mondo aziendale, la sicurezza non è stata diffusamente al centro della strategia e dell'organizzazione, per motivi sia dottrinali sia strutturali. Le discipline manageriali hanno privilegiato concetti come performance, efficacia, efficienza, innovazione o leadership, lasciando la sicurezza in secondo piano e affidandone la cura ai tecnici del risk management, ai garanti della sicurezza sul lavoro (un tallone di Achille dell'assetto produttivo nazionale) e, in alcuni casi, a security manager con formazione tradizionale. Allo stesso tempo, in un Paese in cui le piccole e medie imprese rappresentano oltre il 95% del totale, la cultura della sicurezza si è sviluppata con moderazione, sia per motivi economici sia per la prevalenza di profili imprenditoriali e manageriali orientati a obiettivi operativi.

Indubbiamente gli eventi degli ultimi anni hanno acceso i riflettori sulla sicurezza anche nel mondo economico, con un orientamento prevalentemente rivolto alla difesa degli interessi della singola impresa. Le variabili considerate con maggior attenzione riguardano l'incolumità delle persone che lavorano in impresa considerando rischi interni ed esterni, la sicurezza dei prodotti, la tutela del patrimonio e della proprietà intellettuale, la valutazione dei rischi sui mercati finanziari e, più recentemente, la sicurezza informatica, anche se la relativa robustezza culturale della società in questo ambito rende ardua la sfida di chi si cimenta nella difesa delle imprese.

Una visione che interpreti la sicurezza come interesse nazionale, da perseguire con un'azione organica, è ancora poco diffusa o comunque più recepita a livello concettuale che nella pratica organizzativa. A ben vedere, la legge 124/2007, figlia dei grandi cambiamenti internazionali[6] e approvata durante il secondo Governo Prodi, ha rappresentato una grande innovazione anche in questo campo, affidando al Sistema di informazione per la sicurezza della Repubblica la missione di proteggere gli interessi politici, militari, economici, scientifici e industriali dell'Italia. Non che questi ultimi fossero in qualche modo esclusi dalla normativa precedente, ma l'esplicita menzione dell'industria tra i soggetti portatori d'interessi nazionali è oggettivamente un fatto nuovo. Tornando al significato etimologico di sicurezza (senza preoccupazioni) è dunque chiaro come la sicurezza industriale dipenda anzitutto dalla disponibilità d'informazioni perché solo la conoscenza può offrire uno spazio per la valutazione dei rischi. La nuova legge, di cui ricorre quest'anno

5. Treccani 2017.
6. Bianco 2007.

il decimo anniversario, rappresenta l'intelligence come un assetto unitario, bilanciando la duplice istanza che, da una parte, presuppone la collaborazione delle singole componenti e, dall'altra, lo identifica come un tassello istituzionale del più ampio sistema Paese[7]. La nuova organizzazione ha portato a un ampliamento del raggio d'azione del Sistema di informazione per la sicurezza della Repubblica[8] che, dovendo tutelare per mandato esplicito anche gli interessi economici, scientifici e industriali del Paese, si trova a giocare un ruolo di primo piano per potenziare le condizioni strutturali di competitività dell'Italia nell'economia globale[9].

GLI INTERESSI INDUSTRIALI NELLA NUOVA PROSPETTIVA DI SICUREZZA NAZIONALE

La tutela degli interessi industriali nella nuova prospettiva di sicurezza nazionale richiede anzitutto l'individuazione degli interessi da tutelare. Il campo di variazione è molto ampio: da una concezione più riduttiva, che comprende unicamente infrastrutture critiche, servizi di pubblica utilità e cluster di know how strategico, a una visione inclusiva, che si estende fino a settori economici che, sebbene non direttamente associati al concetto di sicurezza, costituiscono asset fondamentali per la struttura economica del Paese come, ad esempio, le imprese del Made in Italy. Una mappatura dei settori o delle imprese la cui sicurezza rappresenta un interesse nazionale sarebbe un esercizio destinato a produrre un risultato incompleto e comunque opinabile. Indubbiamente esiste una scala di priorità che necessariamente porta a privilegiare le imprese che assicurano i servizi essenziali e i settori che hanno un impatto più rilevante sull'economia o che sono una fonte di vantaggio competitivo per il Paese. Tuttavia, la struttura industriale dell'economia italiana, a cui si è già fatto cenno, importa che gli interessi industriali da tutelare siano diffusi e frazionati; la conseguenza di questo sguardo ampio è necessariamente un approccio inclusivo che, al di là della debolezza derivante dalle dimensioni limitate delle imprese, trova nella frammentazione un elemento di minor vulnerabilità del sistema.

Ne consegue la necessità di considerare tutti i cluster industriali, includendo anche le imprese che singolarmente potrebbero esser considerate irrilevanti. Infatti, se le grandi imprese (nel 2016 solo 193 imprese in Italia hanno superato più di un miliardo di euro[10]) sono probabilmente in grado di affrontare il tema della sicurezza in maniera strutturata, quelle di minore dimensione richiedono di essere accompagnate in un percorso obbligato per mantenere un vantaggio competitivo nel tempo.

7. Valensise 2013, p. 155.
8. Scotto di Castelbianco 2014.
9. Pansa 2017.
10. Mediobanca 2017.

Tra le numerose tematiche collegate alla ricerca di un maggior grado di sicurezza, la cybersecurity sta assumendo un'importanza sempre maggiore per una molteplicità di ragioni: in primis, le minacce informatiche stanno diventando più frequenti e più rilevanti; in seconda battuta, la nuova direttiva europea, conosciuta come *General Data Protection Regulation* (Gdpr) – di imminente applicazione – sta per modificare radicalmente il sistema di diritti e di doveri inerenti al trattamento dei dati; infine, la capacità di gestirli in modo sicuro offre alle imprese un'opportunità di differenziazione e di maggior competitività sui mercati.

Digital Transformation, Industry 4.0, Fourth Industrial Revolution, Next Production Revolution sono termini che, con sfumature diverse, si riferiscono ai grandi cambiamenti tecnologici in atto che si apprestano a sconvolgere con forza dirompente l'organizzazione della società e dunque del mondo produttivo. In particolare, la convergenza di sistemi digitali, fisici e biologici sta configurando situazioni e scenari non immaginabili fino a poco tempo fa e che richiederanno un approccio totalmente nuovo, anche in termini di sicurezza.

Lo sviluppo di sistemi d'intelligenza artificiale, la diffusione della robotica, l'avvento dell'I*nternet of Things*, la crescita esponenziale del volume di dati generati dalle tecnologie connesse in rete fanno emergere tematiche nuove non solo in termini di protezione della privacy ma, più drammaticamente, nella gestione della sicurezza di tutti i sistemi cibernetici. In Italia la diffusione di queste tecnologie sta iniziando a cambiare i sistemi produttivi, sia nella gestione delle relazioni con i clienti, che nei processi industriali e logistici, e in quelli di sviluppo dei nuovi prodotti. Anche in questo caso, molte delle imprese di grandi e di medie dimensioni stanno già sostenendo gli investimenti necessari alla trasformazione, disponibili anche a sostenere dei costi di apprendimento, mentre le piccole e le piccolissime hanno unicamente la chance di restare agganciate alla propria filiera di riferimento. La quarta rivoluzione nel sistema industriale italiano è prevalentemente legata alla capacità d'integrazione di nuove tecnologie nei sistemi produttivi, ma nonostante ciò, come in altri contesti[11], molte imprese non sono in grado di sostenere tutti i costi della trasformazione, ivi inclusi quelli necessari alla progettazione di un nuovo livello di sicurezza *by concept and by design*. Questi scenari, al fine della completa realizzazione della volontà del Legislatore, richiedono un cambiamento del rapporto tra intelligence e industria nonché il coinvolgimento di altri attori, tra cui le università. Il perno di questa riflessione è che la messa in sicurezza di singoli nodi

11. Papadopoulou et al. 2014.

della rete sarebbe poco efficace, tenuto conto delle caratteristiche della realtà produttiva italiana. Si tratta della conseguenza di quell'innovazione che vede il Comparto intelligence come una delle componenti fondanti del sistema Paese di cui, però, fanno parte anche altri attori, anch'essi portatori di responsabilità. Se, da una parte, è necessario un impegno straordinario dello Stato per rinforzare la struttura delle imprese piccole e medie, dall'altra non ci si può affidare a un modello unicamente basato sui Servizi d'intelligence, ma è necessario un atteggiamento di corresponsabilità da parte delle imprese nella definizione e nella tutela degli interessi industriali. La morfologia industriale richiede che le 'imprese guida' coinvolgano o, comunque, trascinino tutti gli attori che compongono la filiera.

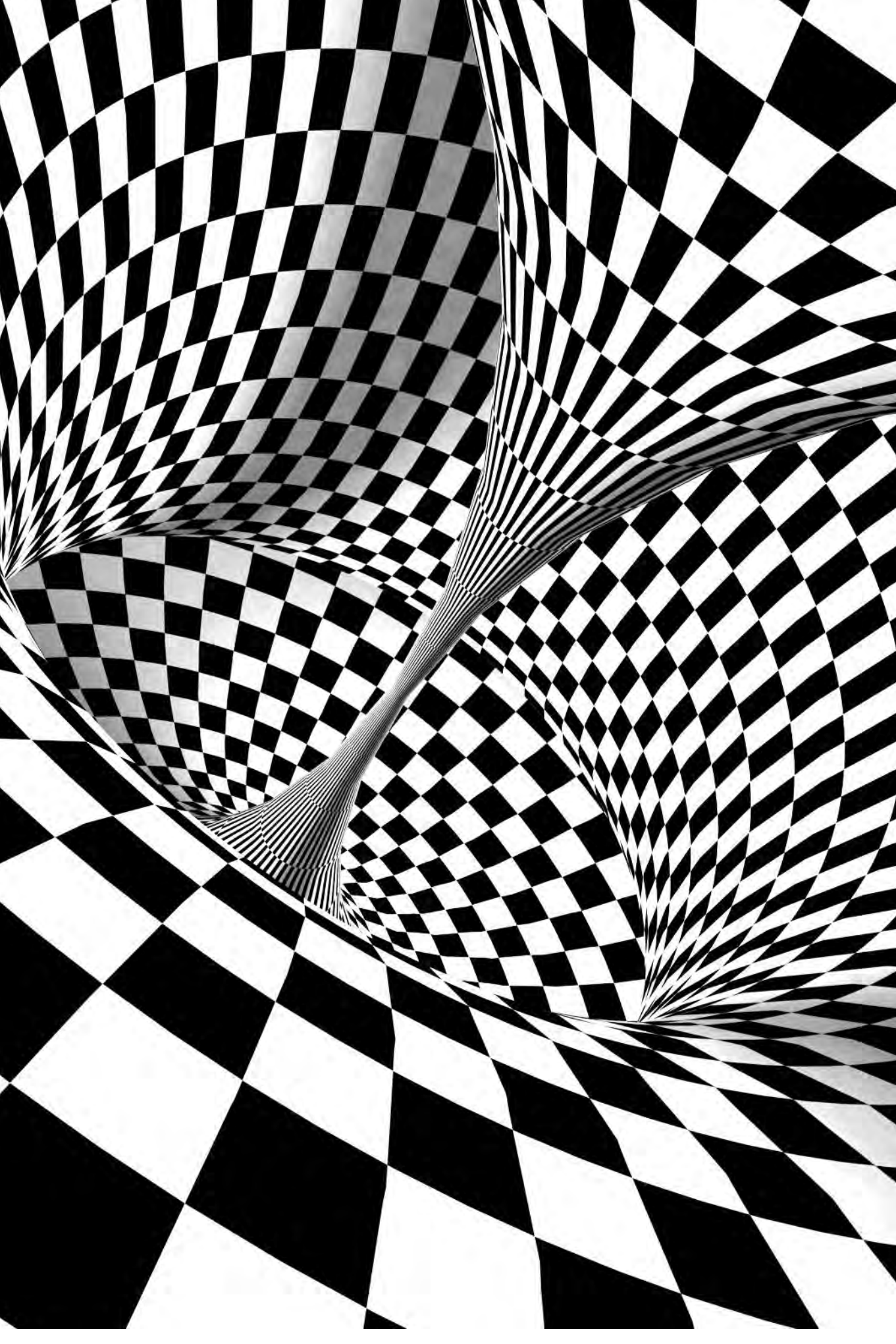
SICUREZZA TRA INTERESSE NAZIONALE E VANTAGGIO COMPETITIVO

Il governo della sicurezza in impresa è anzitutto un fatto culturale, in quanto è ormai necessario passare da una concezione che la considera come una condizione a una nuova visione in cui sicurezza è una fonte di vantaggio competitivo. Normalmente gli atteggiamenti evolvono in maniera lenta e progressiva, mentre in questo campo è necessario un repentino cambio di velocità se non si vuole rischiare una selezione darwiniana delle organizzazioni che non possiedono tale elemento nel proprio patrimonio genetico. Un'occasione si presenta ora con l'entrata in vigore della direttiva Gdpr che, da maggio 2018, prevede, a carico di tutti coloro che gestiscono dati, l'assunzione di nuovi comportamenti a tutela delle informazioni di terzi. Al di là di tutti gli aspetti normativi che introducono novità importanti, la direttiva richiede sostanzialmente un'assunzione di responsabilità da parte delle imprese e delle altre organizzazioni interessate che può esser interpretata in due modi: un adempimento normativo oppure un'opportunità per ridefinire la propria strategia considerando la sicurezza informatica come una sua componente essenziale. Questa seconda opzione corrisponde a una prospettiva di lungo periodo in cui l'impresa imposta una relazione di fiducia con clienti e fornitori (i proprietari dei dati), ripensa al concetto di sicurezza dei sistemi cyber fisici, sia che si tratti di prodotti sia che si tratti di sistemi tecnologici di produzione, trasformando la sicurezza in una fonte di vantaggio competitivo. La risposta non può unicamente essere affidata ai Chief Information Security Officer o a coloro che, nei fatti, svolgono questo ruolo nelle piccole e medie imprese, ma implica un coinvolgimento del top management, affinché la sicurezza diventi una delle componenti della strategia aziendale. Il cambiamento non può che passare per le risorse umane perché la tecnologia da sola non può trasformare le organizzazioni e, tanto meno, la società. Al di là di una piccola comunità di esperti, la consapevolezza dei rischi in questo campo è molto bassa per cui la predisposizione a rispondere alle minacce è insufficiente. Sul piano formativo è necessario intervenire a tutti i livelli, pensando a una strategia nazionale che parta anzitutto dalle imprese e dai giovani, ma interessi rapidamente tutti gli ambiti della società e tutti i gruppi anagrafici.

La scuola dovrebbe essere il primo ambito in cui viene affrontato il tema della sicurezza informatica, anzitutto come strumento di autodifesa personale ma, più in generale, come occasione per diffondere il valore fondamentale della sicurezza nazionale. Dall'abolizione del servizio di leva e dalla soppressione dell'ora di educazione civica nelle scuole (ora affidata a un coordinamento trasversale tra diverse materie), lo Stato fatica a raggiungere i giovani direttamente, mentre la sicurezza informatica sarebbe una grande occasione per avviare un dialogo a partire da un tema che toccano personalmente attraverso il touch screen dello smartphone. Un grande piano d'informazione e di formazione richiederebbe un approccio coinvolgente e motivante, coerente con il linguaggio dei giovani, basato su metodi di *edutainment*. Contemporaneamente, è urgente intervenire sulle imprese, progettando percorsi formativi che non riguardino soltanto i tecnici della sicurezza informatica, ma coinvolgano il top management e consentano di coniugare elementi di strategia aziendale con aspetti organizzativi, giuridici e, ovviamente, tecnologici.
Un piano con tale respiro richiede una squadra che, per iniziare, sia composta da scuole, università, imprese, associazioni di imprenditori e business school; come in ogni squadra, serve un regista e questo è un ruolo che la legge – per certi aspetti profetica – approvata nel 2007 assegna al Sistema di informazione per la sicurezza della Repubblica.

BIBLIOGRAFIA

E. Bianco, *Così è cambiata l'intelligence in Italia*, «Gnosis» (2007) 3.
Costituzione della Repubblica Italiana, *Gazzetta Ufficiale* del 27 dicembre 1947, n. 298 <http://www.quirinale.it/qrnw/costituzione/pdf/costituzione.pdf> [16-11-2017].
S. Dörr et al., *Credit-Supply Shocks and Firm Productivity in Italy*, «International Monetary Fund Working Papers» WP/17/67 (2017).
F. Galgano et al., *Rapporti Economici. Tomo* II *art.* 41-44 *Costituzione*, Zanichelli, Bologna-Il Foro Italiano, Roma 1982.
Istat, *Noi Italia. 100 statistiche per capire il Paese in cui viviamo*: <http://noi-italia.istat.it.> [16-11-2017].
Mediobanca, *Le principali società italiane*, Ufficio Studi, Milano 2017.
D. Nuechterlein, *National Interests and Foreign Policy. A Conceptual Framework for Analysis and Decision-Making*, «British Journal of International Studies» 2 (1976).
A. Pansa, *Il Sistema di informazione per la tutela degli interessi economici nazionali*, Università Bocconi, Milano 3 Aprile 2017: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/Pansa-lectio-magistralis-Bocconi.pdf> [16-11-2017].
D. Papadopoulou et al., *Industry 4.0 – Smart Factory. Also something for medium size Companies*?, Working paper 2014.
R. Prodi, *Andreatta Lecture*, Biblioteca dell'Archiginnasio, Bologna 2016: <https://www.youtube.com/watch?v=AAWxHjehp9g> [16-11-2017].
P. Scotto di Castelbianco, *A che serve l'intelligence italiana*, «Limes» (2014) 7.
Treccani, *Vocabolario* on line: <http://www.treccani.it/vocabolario/sicuro/> [16-11-2017].
United Nations, *Resolution* A/RES/70/1, Paragraph 54, 25 September 2015.
B. Valensise, *La security aziendale e le agenzie di informazione e sicurezza. Il ruolo della legge* 124/2007, «Gnosis» (2013) 1.
World Economic Forum, *The Global Competitiveness, Report* 2017-2018 (2017).



6

LA SICUREZZA ENERGETICA NAZIONALE

DIMENSIONI, CULTURE E STRUMENTI

Francesco Profumo – Ettore Bompard

Nel 2015 il consumo energetico interno lordo italiano è stato di 170 Mtep, del quale solo il 24,8% prodotto a livello nazionale. In termini di singole commodity, sempre nel 2015, il consumo interno lordo di petrolio è stato di 57,3 Mtep, di gas naturale di 50,7 Mtep, di rinnovabili di 34,7 Mtep, di combustibili solidi di 13,7 Mtep e quello di energia elettrica di 9,6 Mtep (importazione netta). Olio e gas giocano un ruolo predominante rappresentando, rispettivamente, il 51,3% e il 32,0% del totale[1]. L'Italia ha una quota del 10,4% nel consumo lordo europeo (EU28), che ammonta a 1.627,5 Mtep (2015). I settori industriale, civile e dei trasporti sono responsabili del 90% dei consumi finali. Il gas naturale è dominante nel settore civile, specialmente per il riscaldamento, mentre l'olio combustibile e, in particolare, i suoi derivati sono usati in larga misura dal settore dei trasporti; infine, i combustibili solidi sono minoritari negli usi finali, limitati alla sola siderurgia. A livello europeo i tre settori rappresentano il 97,4% dei con-

Prof. Francesco Profumo, presidente della Compagnia di San Paolo.
Prof. Ettore Bompard, docente universitario.

Gli autori ringraziano gli ingegneri Daniele Grosso e Giulia Crespi per il supporto fornito.

1. Mise 2015.

sumi finali; quello civile è il maggior consumatore di gas naturale (60,1%), mentre i trasporti sono responsabili del 78,2% degli usi finali di olio combustibile e i combustibili solidi ammontano solo al 17,6%[2]. La dipendenza energetica dell'Italia, definita come il rapporto tra le importazioni nette e la somma del consumo interno lordo e dei bunkeraggi marittimi, è particolarmente pronunciata, attestandosi, nel 2015, al 77,1%, valore relativamente alto rispetto ad altri Paesi europei e alla media europea (Germania 61,9%, Francia 46,0%, UK 37,4%, Spagna 73,3%, EU28 54,1%). La dipendenza italiana dall'importazione del gas naturale è stata, nel 2015, del 90,4%; di questo, il 42,7% è stato importato dalla Russia, che rappresenta il maggiore fornitore nazionale di commodity energetiche con una quota del 24,3% del totale. A livello europeo, l'olio combustibile e il gas naturale sono le due commodity caratterizzate dalla più alta dipendenza (88,8% e 69,1% rispettivamente). Nel 2015 la Russia è stata il maggior fornitore, con una quota del 17,1% dell'importazione totale (29,4% del gas e 24,7% dell'olio combustibile).

DEFINIZIONE E DIMENSIONI DELLA SICUREZZA ENERGETICA

Le varie definizioni di sicurezza energetica disponibili in letteratura pongono l'accento su dimensioni diverse nonostante quella *fisica* e quella *economica* siano ricorrenti. Dal nostro punto di vista, la sicurezza energetica è la possibilità di garantire l'energia per il soddisfacimento degli usi finali (le 'domande di servizi', quali riscaldamento, raffrescamento, illuminazione, mobilità di passeggeri e merci, produzione industriale...), nelle quantità, nei luoghi e secondo i profili di domanda (potenza) richiesti dagli utilizzatori finali, in condizioni normali e quando si verifichino una serie prevedibilmente ragionevole di eventi avversi o *minacce* declinabili in tre macrocategorie: *naturali*, *accidentali e intenzionali*. La sicurezza energetica dipende dalla disponibilità di *fonti energetiche primarie* (gas, olio combustibile, fonti rinnovabili) che possano essere rese disponibili nel Paese, attraverso *corridoi energetici*, trasformate, quando necessario, in commodity secondarie (elettricità, derivati del petrolio), trasportate e distribuite fino agli utilizzatori finali. Da questo punto di vista si possono individuare due fronti per la sicurezza elettrica nazionale (figura 1): uno esterno, dalla fonte all'*entry-point* nazionale, attraverso corridoi di vario tipo (oleodotti, gasdotti, rotte marine, linee elettriche e trasporto su rotaia / gomma) e uno interno, rappresentato dall'infrastruttura di trasporto e distribuzione (reti nazionale del gas ed elettriche, sistemi di distribuzione locale di gas ed elettricità) delle commodity energetiche.

2. Eurostat 2015.

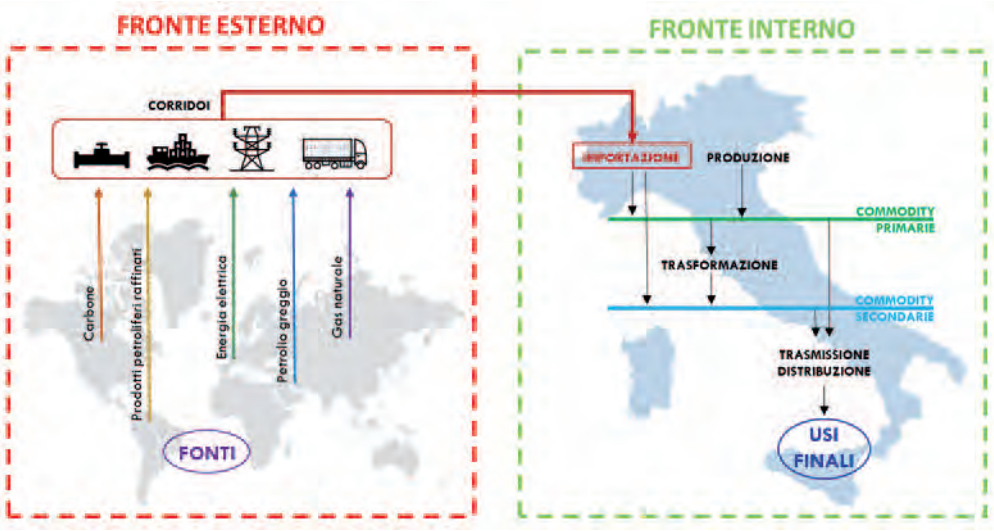
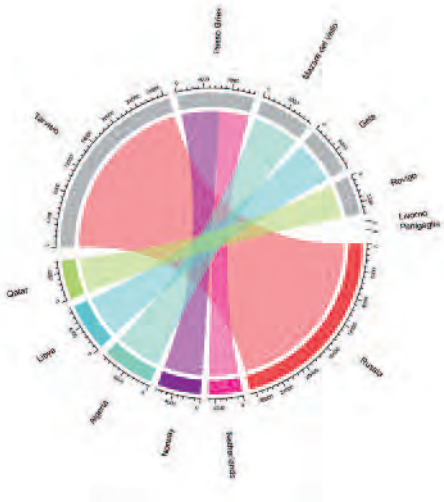
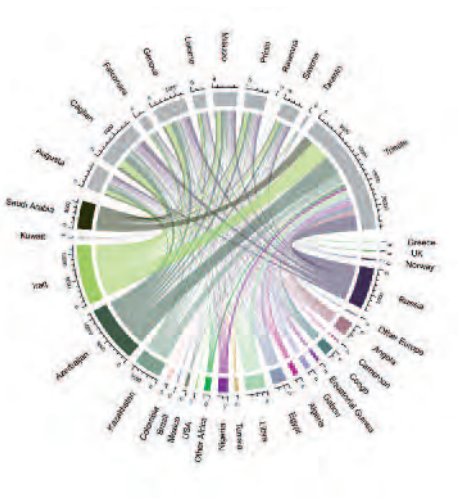


Figura 1. Fronte esterno e interno per la sicurezza nazionale.
In basso, da sinistra, **figura 2.** Importazione di gas naturale: Paesi d'origine ed entry-point nazionali; **figura 3.** Importazione di olio combustibile: Paesi d'origine ed entry-point nazionali.

Mentre la dimensione interna è comune a tutti i Paesi, quella esterna è particolarmente rilevante per quelli come il nostro, fortemente dipendenti dall'importazione. In un contesto di questo tipo, la necessità di garantire l'approvvigionamento dalle fonti e la consegna della commodity agli entry-point nazionali può risultare particolarmente critica e richiede una diversificazione sia delle fonti sia dei corridoi. Una visione sinottica della situazione italiana per gas e olio combustibile è rappresentata nelle figure 2 e 3.
Si noti la dipendenza delle importazioni di gas da un numero relativamente piccolo di Paesi, alcuni con quote predominanti, da cui il gas approda a un numero limitato di entry-point nazionali; al contrario, per l'olio combustibile siamo in presenza di una situazione più variegata.





SICUREZZA ENERGETICA E OBIETTIVI ENERGETICI

La sicurezza energetica deve essere inquadrata in una visione energetica più generale e, in particolare, nell'E*nergy Transition* – tanto auspicata e, per alcuni versi, già in atto – motivata dalla ricerca di una sostenibilità, soprattutto ambientale, dell'energia rispetto al riscaldamento globale e all'inquinamento. In quest'ottica, s'inserisce l'obiettivo di decarbonizzazione dei sistemi energetici. La sostenibilità può essere intesa come la produzione, la trasmissione-distribuzione e l'uso finale di risorse energetiche in grado di soddisfare i consumi, attuali e futuri, garantendo adeguata qualità della vita, giustizia sociale, equa allocazione del welfare ed efficienza economica. Accanto alla sostenibilità è estremamente importante anche l'accessibilità, correlata alla dimensione economica, e rappresentata dalla possibilità per gli utilizzatori di acquisire sul mercato, e ai prezzi di mercato, l'energia necessaria al soddisfacimento degli usi finali. I tre obiettivi energetici primari (sostenibilità, sicurezza e accessibilità economica) devono essere considerati congiuntamente in una visione olistica, tenendo conto delle loro interazioni, locali e globali, all'interno di uno scenario in transizione dei sistemi energetici[3]. Gli obiettivi, tra loro complementari, possono tuttavia presentare elementi sia convergenti che confliggenti, a seconda delle policy adottate e, quindi, siamo in presenza di un problema di ottimizzazione multi-obiettivo, in cui la sicurezza energetica deve essere armonizzata con le altre dimensioni, posto che azioni positive per una di esse potrebbe confliggere con le altre. Ad esempio, considerando l'incremento di penetrazione delle rinnovabili, l'adozione di microreti elettriche locali è coerente sia con l'obiettivo della sostenibilità (perché consente lo sfruttamento di risorse localmente disponibili) sia con quello della sicurezza (perché lo sfruttamento di risorse rinnovabili locali permette di ridurre la dipendenza dall'importazione di commodity fossili da Paesi potenzialmente instabili dal punto di vista geopolitico). D'altro canto, un incremento di penetrazione delle rinnovabili perseguito mediante l'implementazione di interconnessioni elettriche ad altissima tensione su scala globale, con la produzione concentrata in macroaree del mondo (quali l'Artico per l'eolico o le aree desertiche per il solare), è positiva sotto l'aspetto della sostenibilità, ma maggiormente critica sotto quello della sicurezza, poiché tali interconnessioni potrebbero essere soggette a minacce di tipo intenzionale (geopolitiche, fisiche, cyber). Inoltre, un incremento significativo delle rinnovabili cosiddette 'non programmabili' (condizionate, cioè, da fattori di natura climatica e meteorologica) potrebbe originare instabilità critiche del sistema elettrico, legate alla difficoltà di bilanciamento tra produzione e domanda, determinando così una ripercussione negativa sulla sicurezza.

3. Bompard et al. 2017 (c).

CULTURE A CONFRONTO PER LA SICUREZZA: APPROCCIO UMANISTICO E APPROCCIO SCIENTIFICO

In un Paese tradizionalmente caratterizzato da una visione dicotomica della cultura, che divide formazione e approcci tra umanistici e scientifici sulla lunga scia del confronto dell'inizio del secolo scorso tra Federigo Enriques, da una parte, e Benetto Croce e Giovanni Gentile, dall'altra, le questioni della sicurezza, in generale, e della sicurezza energetica, in particolare, sono state affrontate alla luce di questa separazione, con un marcato contributo delle discipline umanistiche. La cultura umanistica utilizza i meccanismi del pensiero filosofico per esplorare e raccontare la realtà, facendo riferimento anche a situazioni in cui mancano dati oggettivamente misurabili; le 'parole' giocano un ruolo cruciale. La cultura scientifica vuole descrivere la realtà in termini di modelli matematici per comprenderla e, entro certi limiti, interagire e controllarla; i 'numeri' sono fondamentali. I due approcci, umanistico e scientifico, sono stati tradizionalmente considerati come ambiti separati, con qualche concessione, soprattutto in Italia, alla superiorità di quello umanistico.
Nell'analisi della sicurezza energetica, l'approccio umanistico definisce e analizza il concetto di sicurezza sotto forma di logos e studia – in modo diretto o indiretto e con varie prospettive – la sicurezza e le sue dinamiche attraverso differenti branche, tra cui scienze politiche, scienze strategiche, diritto internazionale e geografia politica. Gli approcci di tali discipline tendono ad analizzare il problema della sicurezza, inclusi i suoi riflessi nell'ambito energetico, come conseguenza di eventi geopolitici e di dinamiche politiche, storiche e sociali. Questa visione ha quindi il vantaggio di catturare le diverse sfumature derivanti dall'interazione tra sistemi sociopolitici, ma manca della possibilità di quantificarle numericamente e di classificarle in ordine di priorità, così da meglio indirizzare investimenti, azioni preventive ed eventuali contromisure.
L'approccio scientifico, per contro, definisce e analizza il concetto di sicurezza sotto forma di modelli matematici, mirando a studiare il problema della sicurezza energetica come concatenazione numerica di flussi, capacità e percorsi dei corridoi energetici, indici di rischio e scenari ecc. Questa visione ha pertanto il vantaggio di quantificare il rischio energetico-economico e di identificare priorità di intervento, così da meglio definire investimenti, azioni e contromisure; tuttavia, senza il supporto di esperti geopolitici, non consente di cogliere le citate sfumature di natura politica e sociale in grado di influenzare la sicurezza stessa. In questo contesto i due approcci, umanistico e scientifico, apparentemente alternativi, possono e devono dialogare per trovare una sinergia che superi le limitazioni e integri i contributi. Essi sono, infatti, portatori di saperi differenti ma necessari gli uni agli altri per consentire una visione olistica e il più possibile onnicomprensiva della sicurezza energetica.

IL CONTRIBUTO SCIENTIFICO E I MODELLI 'SCIENCE BASED' PER LA SICUREZZA ENERGETICA

L'approccio scientifico alla sicurezza degli asset energetici si concretizza in alcuni modelli, intesi come insiemi di equazioni di varia natura e di teorie matematiche utili per modellizzare la realtà. Pur non potendone dare un quadro esaustivo, proviamo a elencarne alcuni a mero titolo di esempio. Il primo contributo riguarda i M*odelli fisici delle infrastrutture* che consentono di modellizzare, attraverso opportuni sistemi di equazioni (algebriche lineari o non lineari, differenziali...), i flussi energetici per le diverse commodity in condizioni statiche e dinamiche, tenendo conto dei limiti operativi (massima portata legata alla sezione di condotti e conduttori, massima-minima pressione o tensione ammissibile...). Sono utilizzabili per valutazioni di sicurezza del sistema in condizioni normali o 'n-k' (k elementi non disponibili) e per l'analisi del ridispacciamento dei flussi in caso di guasti o indisponibilità di parti dello stesso[4]. Un secondo contributo è dato dai M*odelli per l'analisi di rischio*, i quali permettono di valutare il rischio mediante approcci probabilistici (probabilità di accadimento per il danno, fisico e/o economico associato). Questi sono utilizzabili per effettuare analisi di *safety* (rischi di natura accidentale o tecnologia) e *security* (rischi associati ad attacchi intenzionali o a eventi di natura geopolitica)[5]. Le analisi di rischio possono essere associate utilmente ai modelli fisici delle infrastrutture. I M*odelli ibridi fisici-georeferenziati* (figura 4) consentono di accoppiare – in una visione olistica e di sintesi – la dimensione fisica delle infrastrutture analizzate, con modellizzazione operativa e di analisi dell'indisponibilità originata da diverse tipologie di eventi, con quella geomatica (cartografica digitale e satellitare), che permette invece di considerare la spazialità dell'infrastruttura e di studiare e monitorare, sotto diverse prospettive (geopolitica, climatica ecc.), l'interazione con l'ambiente in cui è inserita e i riflessi che questa può avere sulla sicurezza.

La T*eoria dei giochi* permette di modellizzare le interazioni strategiche tra diversi attori, cioè le situazioni in cui l'utilità di un singolo attore non dipende unicamente dalle proprie azioni, ma anche da quelle degli altri attori. Questa teoria può essere applicata allo studio della sicurezza energetica, sia del fronte esterno sia di quello interno, modellizzando l'interazione strategica geopolitica tra diversi Paesi oppure l'interazione tra attaccanti e difensori – stimando la probabilità, per ciascun elemento del sistema, di essere attaccato e, di conseguenza, il rischio a esso associato – nel caso di

4. Zaccarelli et al. 2014, p. 89.
5. Bompard et al. 2017 (b).

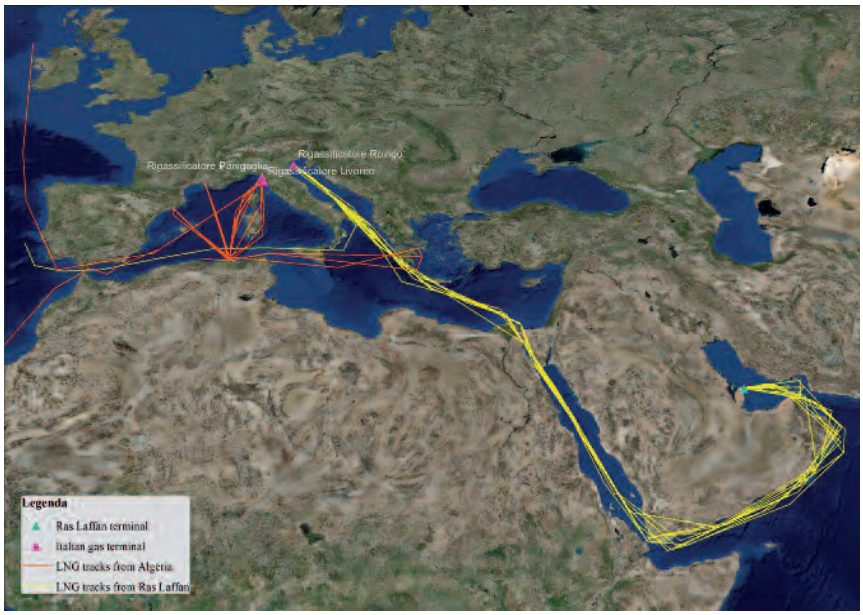
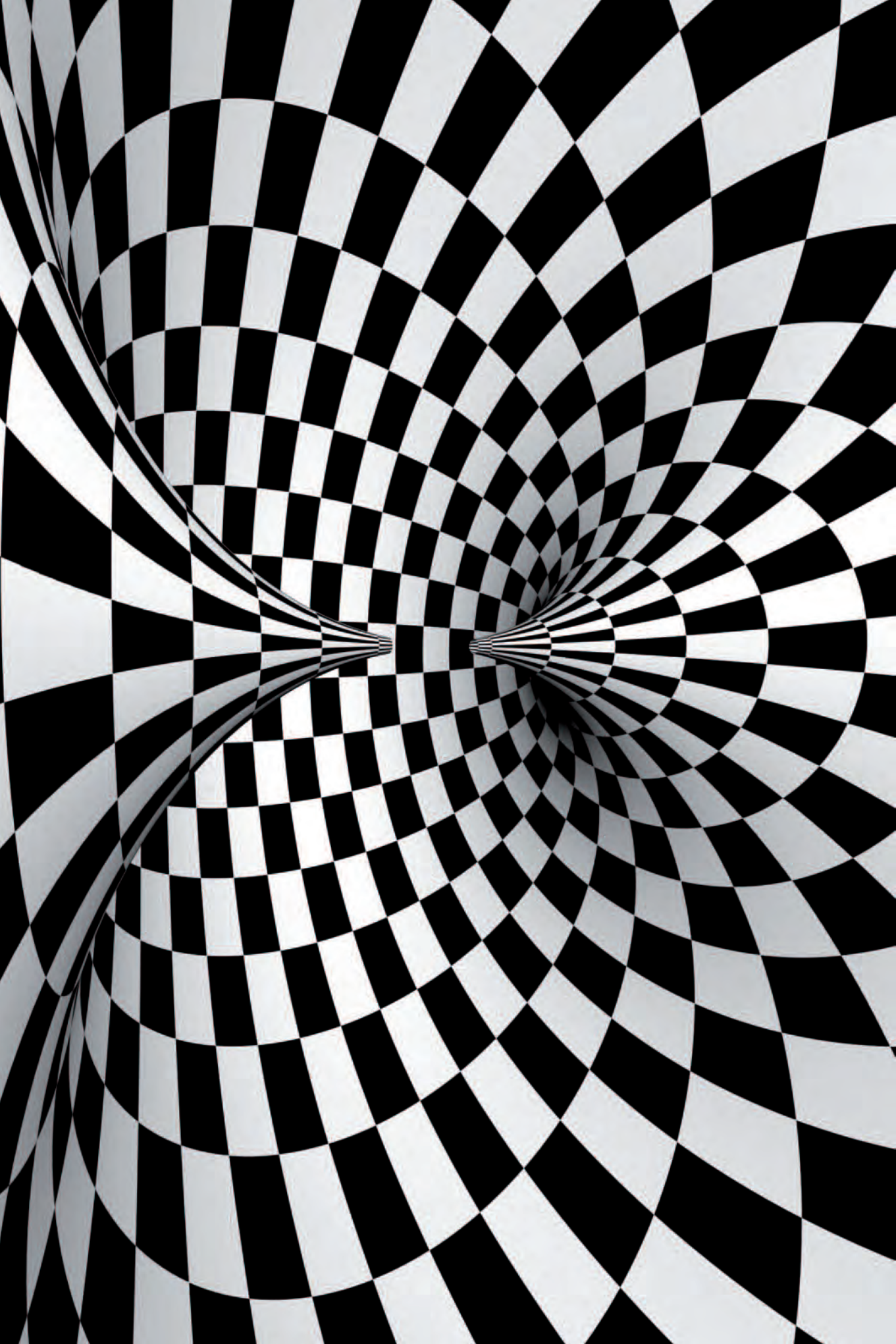


Figura 4. Esempio di modellizzazione ibrida (fisica e georeferenziata): corridoi LNG Ras Laffan (Qatar)-Algeria – Italia (Panigaglia, Rovigo e Livorno).

attacchi intenzionali[6]. I M*odelli di simulazione e di ottimizzazione* vengono tradizionalmente utilizzati nelle analisi di pianificazione dei sistemi energetici; i modelli di simulazione valutano l'evoluzione di un asset rispetto a possibili valori associati a un dato set di variabili assunto arbitrariamente come input (come la variazione della capacità installata per una certa tecnologia), gli impatti e i costi-benefici della configurazione considerata; questi modelli sono adatti a effettuare il confronto tra due o più scenari (corrispondenti a diverse politiche energetiche). I modelli di ottimizzazione, ad esempio Times[7], calcolano invece, per tutte le variabili, i valori che portano alla configurazione ottimale, cioè a quella che minimizza-massimizza una data funzione obiettivo (minimo costo totale del sistema, massima sicurezza), sotto diversi vincoli o target (emissioni di CO_2, penetrazione di una determinata tecnologia, diversificazione delle fonti). Le analisi, effettuabili con modelli del tipo descritto, devono essere relazionate agli *scenari temporali* e alle *ottiche di gestione*. Le *scale temporali* spaziano dal tempo reale, al breve e al lungo termine, dove i primi due sono definiti da un'infrastruttura energetica invariante, mentre l'ultimo è definito dalla possibilità di cambiare fonti, corridoi e infrastrutture. Le *ottiche di gestione* riguardano la gestione delle emergenze,

6. Bompard et al. 2009.
7. Kanudia et al. 2013.



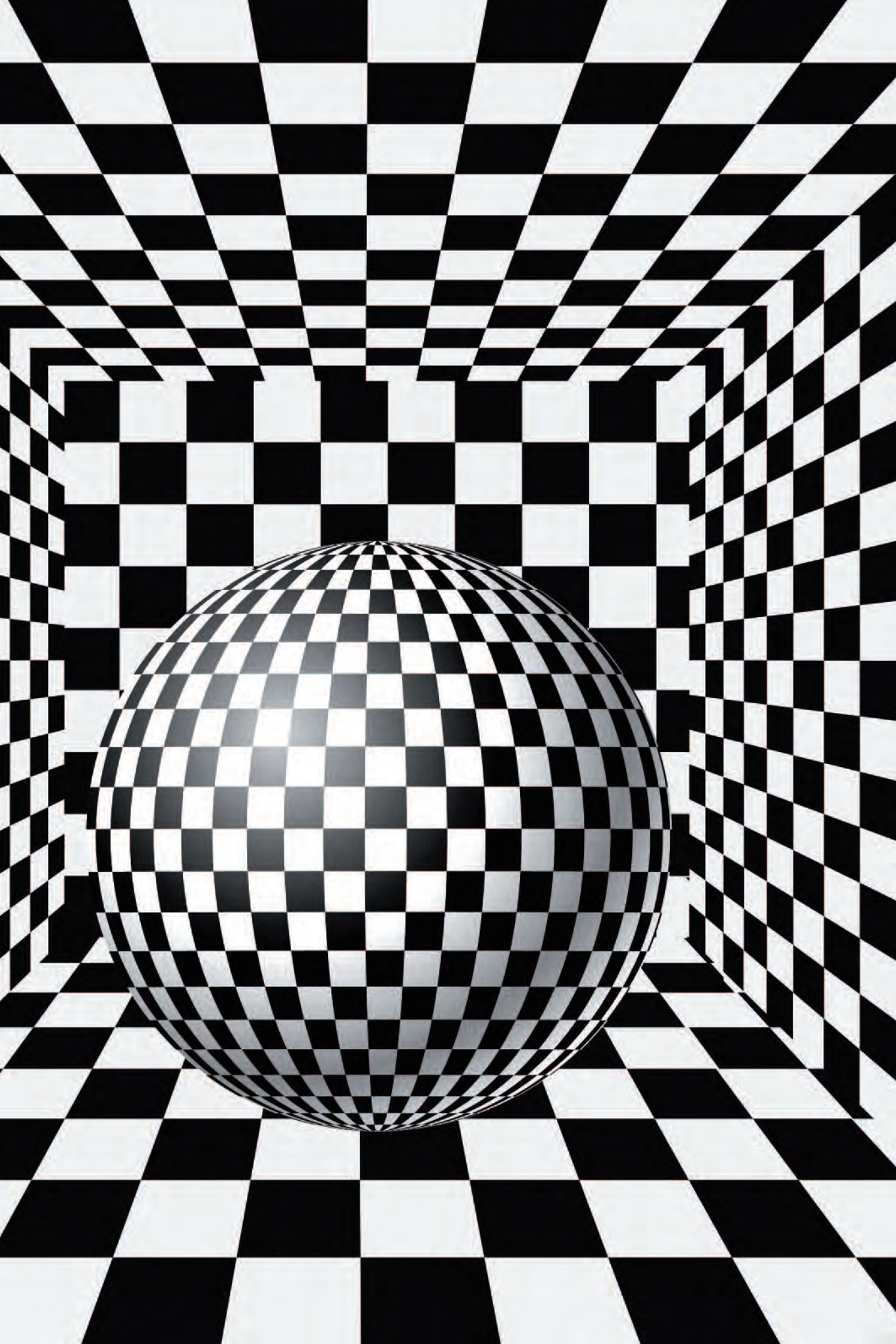
l'esercizio e la pianificazione. La gestione delle emergenze coinvolge la scala del tempo reale e implica la necessità di avere un'organizzazione resiliente in grado di garantire la propria funzionalità anche in presenza di eventi imprevisti (di origine accidentale, naturale o dolosa) che determinino l'indisponibilità improvvisa di parte di essa. L'esercizio è invece legato all'orizzonte temporale di breve termine. Nel caso dell'indisponibilità di una parte del sistema (come un corridoio per l'approvvigionamento) occorre assicurarne – ad esempio, attraverso un opportuno ridispacciamento dei flussi – il mantenimento della funzionalità nella sua presente strutturazione, cioè in assenza di interventi strutturali che ne ridisegnino l'architettura. La pianificazione, infine, è correlata al lungo termine e riguarda le scelte strategiche da effettuare (anche mediante il supporto di analisi modellistiche e comparazione di scenari) per modificarne la configurazione (ad esempio, si pensi alla costruzione di nuovi corridoi di approvvigionamento, che coinvolgono nuovi Paesi fornitori, utili per incrementare la diversificazione e/o che attraversano Paesi politicamente più stabili e sicuri).

UN LABORATORIO PER LA SICUREZZA ENERGETICA

Con l'obiettivo ambizioso di creare uno spazio in cui sviluppare strumenti di supporto *science based* per l'analisi della sicurezza energetica nazionale e la valutazione dei rischi energetici ed economici associati è nato, da una collaborazione tra il Politecnico di Torino e la presidenza del Consiglio dei ministri, il L*aboratorio per la sicurezza energetica delle fonti, dei corridoi, dei mercati e delle infrastrutture energetiche*, presso l'Energy Center di Torino. Il laboratorio ha altresì l'obiettivo di far incontrare culture diverse della sicurezza energetica, provando a sintetizzarle, e di aprire uno spazio di confronto con i maggiori attori nazionali, sia istituzionali, che accademici e industriali.

BIBLIOGRAFIA

E. Bompard et al., R*isk Assessment of Malicious Attacks Against Power Systems*, «IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans» (2009) 39, pp. 1074-1085.
E. Bompard et al. (a), S*cenari geopolitici e sicurezza energetica. Una metodologia per quantificare il rischio degli approvvigionamenti*, «Gnosis» XXIII (2017) 1, pp. 182-191.
E. Bompard et al. (b), N*ational energy security assessment in a geopolitical perspective*, «Energy» (2017) 130, pp. 144-154.
E. Bompard et al. (c), I*l ruolo dell'energia elettrica nella transizione energetica*, «Rivista Energia» (settembre 2017), pp. 34-40.
A. Kanudia et al., M*odelling* EU-GCC *energy systems and trade corridors*: L*ong term sustainable, clean and secure scenarios*, «International Journal of Energy Sector Management» (2013) 7, pp. 243-268.
Mise-Ministero dello Sviluppo Economico, B*ilancio Energetico Nazionale* 2015: <www.dgsaie. mise.gov.it/dgerm/ben.asp> [10-11-2017].
N. Zaccarelli et al., E*xtension of the* EUG*as model to* 26 M*ember States*, «JRC Report» (2014), JRC94213.



INTERNET OF THINGS

RISCHI E OPPORTUNITÀ PER LA SICUREZZA NAZIONALE

Donatella Sciuto

Con l'I*nternet of Things* (IoT) («Internet delle Cose») gli oggetti vengono dotati di 'intelligenza': sono in grado di elaborare dati, ricevere e trasmettere informazioni, anche senza interagire direttamente con gli esseri umani. Oltre alla capacità di comunicare tra loro, questi oggetti possono essere dotati di sensori per acquisire dati dall'ambiente circostante e di attuatori per eseguire alcune funzionalità in base alle informazioni ricevute. Gli oggetti sono quindi in grado di acquisire un ruolo attivo.
Obiettivo degli oggetti intelligenti è quello di semplificarci la vita, automatizzando i processi o fornendo informazioni prima sconosciute. Dai braccialetti e orologi che monitorano alcune funzioni fisiologiche (tipicamente usati dagli amanti del fitness) ai sensori che sorvegliano e alimentano animali o piante; dai sistemi di videosorveglianza (antifurti così come baby monitoring) alle auto (che ci avvisano in caso di manutenzione e intervengono in situazioni di emergenza), per non dimenticare i robot industriali.

Prof.ssa Donatella Sciuto, prorettore vicario del Politecnico di Milano.

Vista la pervasività, non sorprende che il tasso di adozione di queste tecnologie cresca esponenzialmente. I costi si riducono, l'infrastruttura di rete mobile cresce e, a breve, il numero degli oggetti collegati in rete sarà dell'ordine di decine di miliardi. Basti pensare che nel 2016 il mercato dell'IoT in Italia è cresciuto del 40% rispetto all'anno precedente.
Certamente questi sistemi offrono molte potenzialità, ma altrettanti rischi. Ogni oggetto collegato a internet è una 'porta aperta' alle nostre informazioni, che possono essere sfruttate in diversi modi se non adeguatamente protette. Nel caso del singolo utente il problema principale riguarda la tutela della privacy e il controllo delle informazioni personali (quelle in grado di 'profilarci'), ma ancora più grave è il pericolo sul fronte industriale e della sicurezza nazionale.

I principali ambiti applicativi dell'Internet of Things

La possibilità di collegare il mondo fisico alla rete internet, o ad altre reti di dati, ha profonde implicazioni per la società e per l'economia, che vanno dall'organizzazione della vita delle persone alla gestione delle infrastrutture pubbliche. Gli ambiti sono molteplici: la casa, gli edifici, le fabbriche, le strade, le città nel loro complesso. A livello economico, le maggiori opportunità provengono dalla trasformazione dei processi di gestione e produzione e dalla creazione di nuovi modelli di business[1]. Non a caso, la maggior parte dei settori industriali considera queste tecnologie una condizione favorevole allo sviluppo – dal settore bancario al manifatturiero, ai trasporti, all'energia, al commercio, alla sanità e all'agricoltura – anche se ancora non è possibile definire con esattezza l'impatto e l'estensione di questi cambiamenti. Segue un elenco, rappresentativo (non esaustivo), dei principali ambiti di applicazione[2].

– Smart City e Smart Environment: monitoraggio e gestione delle componenti di una città e di un territorio per migliorarne l'uso, la vivibilità, la sostenibilità, la sicurezza. Esempi di applicazioni nelle città possono essere la gestione dei trasporti pubblici e del traffico, la condivisione dei mezzi urbani (biciclette, moto, auto), l'illuminazione pubblica, i parcheggi, la gestione della sicurezza e delle emergenze, il monitoraggio della qualità dell'aria.
– Smart Energy: dalla rete elettrica intelligente (*smart grid*) per ottimizzare la distribuzione, gestendo anche la produzione distribuita (per esempio pannelli solari o piccole installazioni geotermiche), ai contatori intelligenti per la misura dei consumi (elettricità, gas, acqua). L'Italia ha già un altissimo tasso di diffusione di contatori intelligenti, in particolare nel sistema elettrico.

1. Rapporto McKinsey 2015.
2. Rapporto Osservatorio Internet of Things 2017.

- Smart Home: soluzioni per la gestione in automatico degli impianti domestici connessi alla rete (riscaldamento, condizionamento, illuminazione ecc.) con l'obiettivo di ridurre i consumi energetici e migliorare il comfort. Altri esempi significativi sono i sistemi di gestione della sicurezza fisica o di teleassistenza per anziani, o gli assistenti personali virtuali.
- Smart Building: gestione automatica degli impianti e dei sistemi dell'edificio per il risparmio energetico, il comfort, la sicurezza.
- eHealth: monitoraggio, in tempo reale, di parametri medici da remoto sia per diagnosi che per cura, riducendo il ricorso all'ospedalizzazione.
- Smart Car: connessione tra veicoli o tra questi e l'infrastruttura circostante per la prevenzione e rilevazione d'incidenti, per il controllo del traffico e l'ottimizzazione dei percorsi, o per la semplice manutenzione. Il passo successivo, di cui molto si parla, è il veicolo a guida autonoma.
- Smart Logistics: tracciabilità della filiera produttiva e distributiva, monitoraggio della catena del freddo, protezione dei marchi e dell'origine dei prodotti, gestione efficiente delle flotte.
- Smart Factory: evoluzione dei sistemi produttivi tramite l'utilizzo delle tecnologie digitali per abilitare nuove logiche di gestione della produzione, della manutenzione, della pianificazione e di tutto il ciclo di vita dei prodotti. L'obiettivo è migliorare la qualità dei prodotti e dei processi, incrementando la flessibilità e le possibilità di differenziazione. In Europa, tutto questo si sta affermando sotto la parola chiave 'Industria 4.0'.
- Smart Retail: monitoraggio del comportamento del cliente all'interno del negozio, con l'obiettivo di migliorare l'esperienza di acquisto e incrementare le vendite grazie a una personalizzazione del servizio, oltre al miglioramento della logistica, degli ordini e dell'esposizione.
- Smart Agriculture: monitoraggio di parametri specifici del terreno o di tipo microclimatico per migliorare la produzione e ottimizzare l'utilizzo delle risorse.

INTERNET OF THINGS E SICUREZZA

La crescente digitalizzazione, la varietà e l'ampiezza dei settori interessati portano due grandi pericoli. In primo luogo, ogni nuovo dispositivo connesso alla rete accresce la vulnerabilità agli attacchi e l'interoperabilità con altri dispositivi diffonde e moltiplica gli eventuali danni. In secondo luogo, e non meno importante, le conseguenze di un attacco informatico potrebbero coinvolgere direttamente l'ambiente e le persone.

L'IoT richiede dunque un ripensamento del concetto di sicurezza, ampliandone i campi di applicazione e attribuendo responsabilità ai diversi attori che operano in questo contesto, sia nell'ambito delle nuove piattaforme sia dei nuovi servizi.

La debolezza principale risiede nelle infrastrutture critiche[3], chiamate a garantire servizi in modo continuativo, come la produzione e distribuzione dell'energia, i sistemi sanitari e militari, quelli di produzione industriale, persino la stessa infrastruttura di rete di telecomunicazione. Tradizionalmente questi sistemi sono progettati per essere tolleranti a guasti e incidenti naturali. Oggi, è necessario garantire la loro sopravvivenza anche in caso di attacchi al sistema informatico. Se questi sistemi sono tradizionalmente progettati per essere robusti, secondo un approccio top-down, il paradigma IoT privilegia l'approccio bottom-up collegando tra loro molteplici oggetti senza che siano stati appositamente pensati per farlo. Il risultato è che mentre nel paradigma tradizionale i comportamenti sono progettati ex ante, nel paradigma IoT non sempre sono prevedibili, specialmente negli stati particolari in cui un sistema è forzato dagli aggressori.

Consideriamo, come esempio, i sistemi robotici presenti nei processi manifatturieri. Si stima che nel 2018 il numero di robot nelle fabbriche di tutto il mondo sarà di 1,3 milioni, secondo un trend in crescita. Fondamentali per supportare l'evoluzione dell'Industria 4.0, i robot automatizzano e rendono più intelligenti le fabbriche, sfruttando il collegamento in rete tra gli impianti produttivi e tra questi ultimi e i sistemi informativi aziendali. Nel momento in cui diventano sempre più intelligenti e interconnessi, cresce la loro superficie di attacco. Basti pensare che, già ora, molti robot e intere catene di produzione possono essere monitorati e mantenuti a distanza.

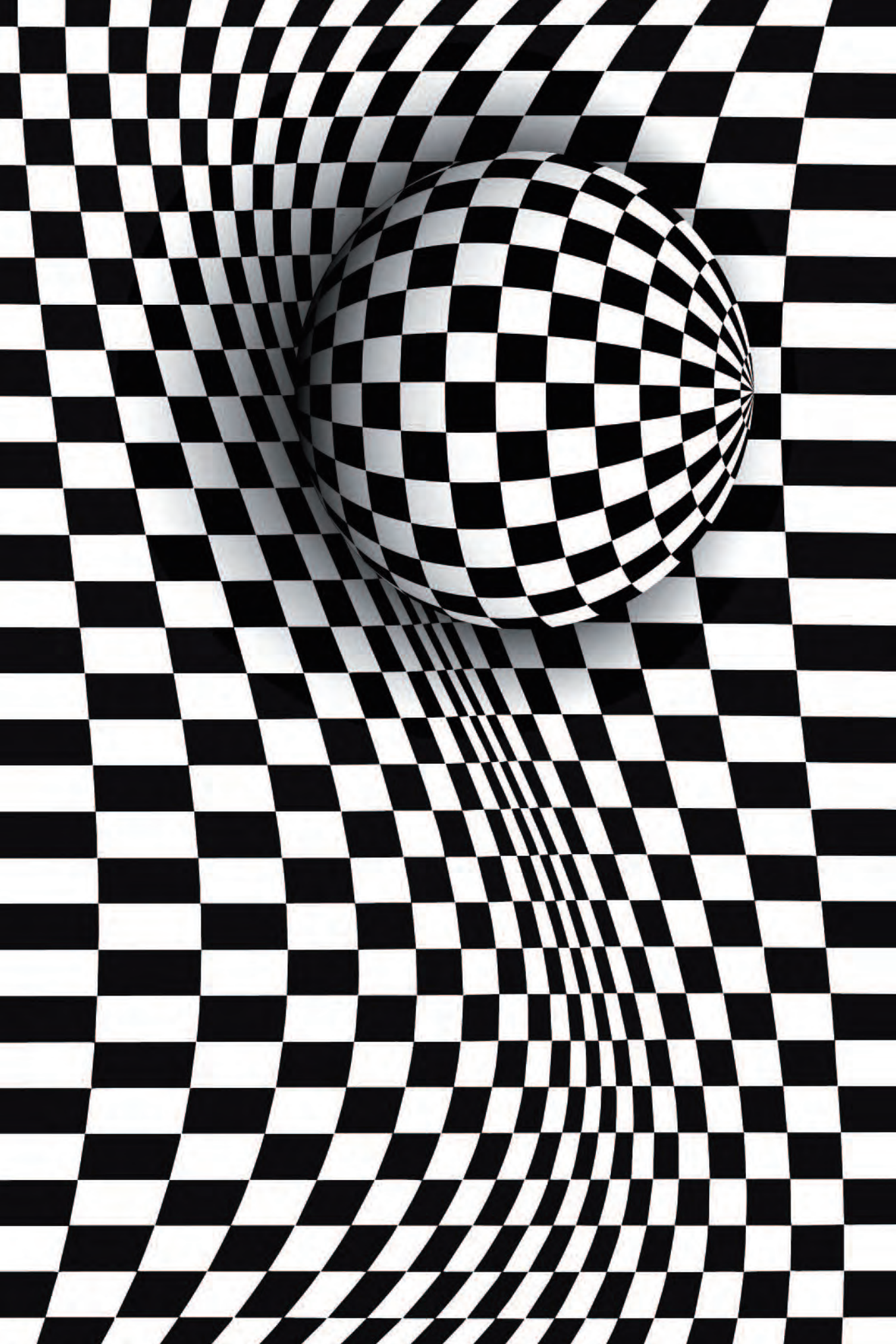
Recenti studi mostrano come molti sistemi robotici siano in realtà fragili e vulnerabili, composti da software obsoleti, basati su librerie non sempre aggiornate, con scarso o scorretto utilizzo delle moderne tecniche di protezione crittografica e di autenticazione, a volte addirittura con credenziali predefinite difficilmente modificabili[4]. Come non bastasse, i robot sono progettati per interagire sempre più a stretto contatto con gli esseri umani e questo mette a repentaglio anche l'incolumità degli operatori.

Gli scenari di attacco possono essere diversi, dal sabotaggio di prodotti all'esfiltrazione di segreti industriali. Proviamo a immaginare un aggressore che modifica e introduce microdifetti su un'unità di prodotto (magari parti di ricambio o medicinali!) e poi ricatta l'azienda.

3. Si definisce infrastruttura critica una risorsa essenziale per garantire le funzioni vitali della società, in termini di salute, sicurezza, benessere economico o sociale delle persone (EU Directive 2008/114/EC).

4. Zanero 2017.

Per garantire un appropriato livello di sicurezza dei sistemi IoT è necessario un approccio e uno sforzo olistico che richiede il sostegno e la partecipazione di tutti gli stakeholder, inclusi i fornitori di soluzioni di sicurezza e gli sviluppatori di software.
La sicurezza in ambito IoT deve essere considerata a tre macrolivelli: le piattaforme hardware e software; la rete; le applicazioni. Ognuno di questi deve essere progettato in modo da fornire le opportune garanzie in termini di riservatezza, integrità e disponibilità dei dati nonché di sicurezza fisica degli utenti e della società. Ovviamente, dal momento che la sicurezza è vista come gestione del rischio, i sistemi di protezione devono essere commisurati alla sensibilità dei dati gestiti e alla criticità del sistema.
Nel caso dei dispositivi finali essi sono composti da sensori, una minima parte di elaborazione, un componente per la trasmissione wireless delle informazioni ed eventualmente degli attuatori.
Si tratta, in genere, di sistemi che devono essere in grado di operare con basso consumo di potenza, essendo alimentati da piccole batterie. In questo caso è prima di tutto necessario certificare le componenti hardware.
La rete d'interconnessione tra i dispositivi distribuiti è poi tipicamente wireless: la protezione della trasmissione dati richiede che questi siano cifrati in modo efficiente. Ciò richiede lo sviluppo di componenti hardware specifici che ottimizzino le prestazioni, il consumo di potenza e le dimensioni.
L'autenticazione tra dispositivi IoT è un problema complesso da risolvere. Molti dei protocolli in uso richiedono che il dispositivo sia dotato di una chiave crittografica privata, diversa da quella di tutti gli altri dispositivi. Allo stesso tempo, la parte 'pubblica' di questa chiave deve essere associata al dispositivo da parte degli altri elementi della rete. L'iniezione di questo 'segreto' unico nei dispositivi risulta spesso difficile da un punto di vista d'ingegnerizzazione della produzione.
Il terzo livello da considerare è quello delle applicazioni dell'IoT, che possono essere di molti tipi e con altrettanti gradi di rischio potenziale. Un primo scenario d'attacco, molto semplice da immaginare, è quello di un D*enial of* S*ervice* che rende inaccessibile l'infrastruttura IoT all'applicazione, con la conseguente impossibilità di fornire un servizio che si basi sui dati raccolti dai dispositivi (servizio che potrebbe essere di natura critica). Un'altra possibilità è che l'aggressore riesca a sostituirsi o aggiungersi ai dispositivi IoT legittimi, restituendo dati scorretti che causerebbero azioni dannose (si pensi a informazioni errate fornite dai sensori di un impianto di produzione).



CONCLUSIONI: COME INTERVENIRE PER LA SICUREZZA NAZIONALE?

Il primo obiettivo della sicurezza nazionale è quello di evitare che possibili attacchi portino a una situazione di non operatività economica e sociale del Paese. Per questo è fondamentale che i tanti soggetti che gestiscono le infrastrutture critiche valutino correttamente i rischi della digitalizzazione, del monitoraggio e della gestione d'impianti e servizi attraverso l'IoT; che definiscano e realizzino azioni di prevenzione e difesa; che sottopongano le misure adottate a *stress test* o *penetration test* per verificarne l'efficacia. Queste azioni non elimineranno l'esistenza degli attacchi, ma renderanno possibile fronteggiarli riducendone i danni potenziali; consentiranno di utilizzare le informazioni raccolte per analizzarle e individuare i punti deboli che emergeranno e permetteranno di intervenire per migliorare le soluzioni di sicurezza. La pervasività delle tecnologie digitali rende questo compito gravoso e allo stesso tempo sfidante, aprendo nuove opportunità di intelligence.

La quantità di dati generati dai sistemi IoT e il controllo del territorio rappresentano un vantaggio nella prevenzione e nella rilevazione di segnali, anche deboli, di possibili attacchi fisici o virtuali. Tracce che, con la giusta capacità di analisi, possono essere individuate e acquisite da fonti eterogenee, utilizzando tecniche di apprendimento automatico e d'intelligenza artificiale.

Nel prossimo futuro le tecnologie digitali definiranno, in maniera sempre più incisiva, il modo in cui vivremo e lavoreremo. Gran parte di questa trasformazione dipenderà dall'«Internet delle Cose» e da applicazioni che si basano su tecniche d'intelligenza artificiale. Tecnologie vulnerabili che offrono enormi benefici alla società e altrettanti rischi. I governi europei dovranno inserire tra i primi punti in agenda la protezione dello sviluppo socioeconomico abilitato da queste tecnologie, attraverso norme che regolino i cambiamenti e che individuino un compromesso sostenibile tra libertà e sicurezza.

Le politiche di cybersecurity dipenderanno sempre di più dalla cooperazione tra imprese, istituzioni e cittadini, tra Stati membri e istituzioni dell'Unione europea.

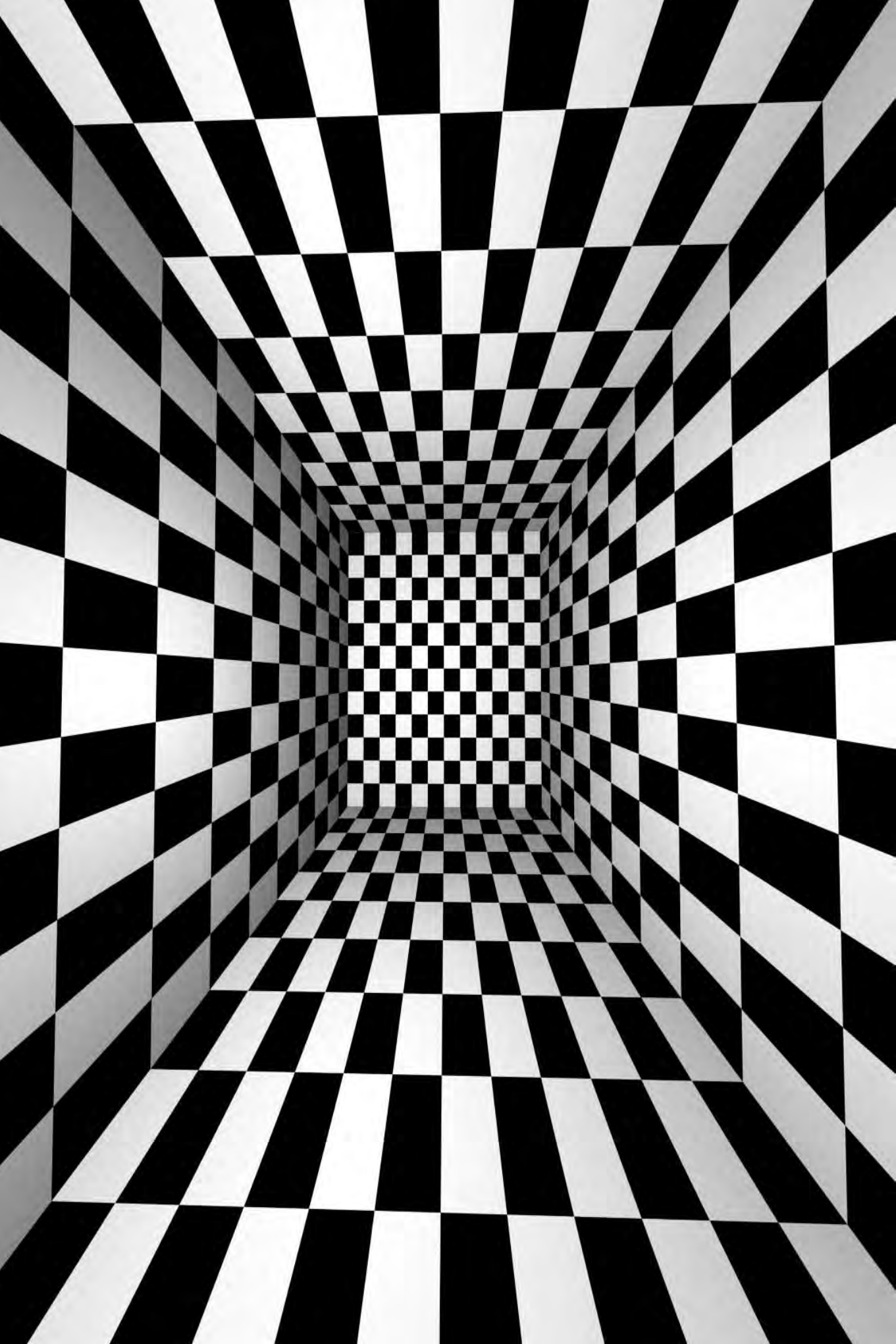
La gestione della sicurezza non è, e non sarà, meramente una questione tecnica, ma richiederà, al contrario, un'azione di sensibilizzazione, di formazione e di divulgazione a tutto tondo. L'obiettivo finale è che le organizzazioni coinvolte, pubbliche e private, considerino la sicurezza *by design* in qualunque iniziativa di trasformazione digitale. Ciò significa introdurre le proprietà di sicurezza come requisito funzionale nel processo ingegneristico di pianificazione, progettazione e realizzazione dei sistemi basati su IoT.

BIBLIOGRAFIA

RAPPORTO MCKINSEY, *Internet of Things: mapping the value beyond the hype*, McKinsey Global Institute, giugno 2015.

RAPPORTO OSSERVATORIO INTERNET OF THINGS, *Internet of Things: oltre gli oggetti, verso i servizi*, Politecnico di Milano, aprile 2017.

S. ZANERO ET AL., *An Experimental Security Analysis of an Industrial Robot Controller*, IEEE Symposium on Security and Privacy 2017.



PARTENARIATO INTELLIGENCE

RICERCA AI FINI DELLA SICUREZZA CIBERNETICA NAZIONALE

Roberto Baldoni

Il 2017 ha mostrato, attraverso le campagne dei *criptolocker wannacry* e *notpetya*, come sia importante per un Paese alzare le proprie difese cibernetiche partendo dai cittadini, fino alle grandi organizzazioni pubbliche e private. Capire che far parte del cyberspazio comporta dei rischi per sé e per gli altri è una presa di coscienza fondamentale, passo base per implementare qualsiasi misura di sicurezza allo scopo, ad esempio, di mitigare l'impatto di un attacco. Il cyberspace è quanto di più complesso e articolato che l'uomo abbia mai concepito, unione di migliaia di reti dati e di stratificazioni di software che interconnettono uomini e cose in giro per il mondo. Tuttavia, questa complessità, non avendo come fulcro la sicurezza, è generatrice di vulnerabilità nelle reti, nei programmi software e nelle loro interazioni.
Imprese, Pubblica amministrazione e cittadini devono essere pronti a monitorare il loro mondo digitale, parte del grande cyberspazio. Tenere sotto controllo i nostri dispositivi, aggiornare i software, conoscere le nostre eventuali vulnerabilità in un ciclo senza fine di gestione del rischio informatico. Questi processi vanno tuttavia indirizzati e coordinati all'interno di un quadro nazionale e non possono essere isolati tra loro.

Prof. Roberto Baldoni, docente universitario.

In questo contesto entra in gioco il nuovo Dpcm 17 febbraio 2017, c.d. Gentiloni, in materia di protezione cibernetica e sicurezza informatica, pubblicato nel mese di aprile, che costituisce un efficace riferimento strategico multidimensionale nazionale entro cui sono chiamati a operare, in modo ordinato e coordinato, pubblico e privato, militare e civile, grandi organizzazioni e cittadini, in un esercizio continuo a livello di sistema Paese. In quest'ottica il Dpcm, che colloca il Comparto intelligence alla guida della difesa nazionale cyber, dà forte impulso, tra l'altro, alla collaborazione tra settore pubblico e privato, la ricerca nazionale e le università.
L'articolo dapprima analizza come la trasformazione digitale stia cambiando progressivamente processi, asset e modelli di business di tutte le organizzazioni nazionali, segnatamente industrie, infrastrutture critiche, Pubblica amministrazione. Con essa muta anche profondamente il modello di minaccia per la sicurezza nazionale rispetto al passato, rendendola imprevedibile. Per affrontarla diventa elemento essenziale la ricerca, multidimensionale e multidisciplinare, con al centro la tecnologia e la sicurezza informatica.
Nel nostro Paese, dal 2010, è stata avviata la costruzione di un partenariato strategico tra intelligence e ricerca, che ha dato vita al Centro di ricerca di cyberintelligence e information security di Sapienza (2012), al Laboratorio nazionale di cybersecurity del Consorzio interuniversitario nazionale informatica (2014) e al Comitato nazionale per la ricerca in cybersecurity (2017).
Il partenariato ha cambiato profondamente il rapporto tra i due mondi mutando il paradigma di interazione vigente in passato ed è per questo da molti considerato una best practice internazionale.

LA TRASFORMAZIONE DIGITALE E IL MODELLO DI MINACCIA NEL CYBERSPAZIO

Lo sviluppo tecnologico, in particolare quello degli ultimi trent'anni, ha ingenerato due trend: l'incremento dell'internazionalizzazione e della privatizzazione. Private sono, infatti, la stragrande maggioranza delle reti e privati sono i computer e gli oggetti smart che formano il cyberspazio che è per definizione globale e non rispetta i limiti nazionali fisici. Tutto questo ha cambiato nettamente le prospettive della sicurezza nazionale, modificandone i confini e i modelli di minaccia. Nel mondo basato sulle barriere fisiche e sulle informazioni immagazzinate su carta, la minaccia era stata modellata ed erano chiare le azioni da mettere in atto per affrontarla sia nel pubblico che nel privato. Conservare alcune informazioni, in base al grado della loro riservatezza, in una cassaforte ben sorvegliata all'interno del perimetro fisico di un'organizzazione rendeva complessa la loro sottrazione. I malfattori dovevano agire sul posto con l'aiuto eventuale di qualche basista. Minore era la protezione del perimetro fisico più facile era la sottrazione delle informazioni e maggiore il numero di criminali in grado di attuarla.

La trasformazione digitale ha portato sempre più alla rimozione del perimetro fisico. Nei primi anni Novanta eravamo in presenza, all'interno di un'organizzazione, di isole automatizzate in genere non connesse. Ad esempio, in un'industria avevamo alcune macchine computerizzate nella parte di produzione oltre a quelle impiegate nelle procedure amministrativo-contabili. Dal 1990 al 1995, le isole sono state integrate all'interno di piattaforme software e reti locali. Questi erano gli anni in cui la parola *middleware* fu coniata come elemento di integrazione tra sistemi computerizzati autonomi e nacquero due elementi distinti in azienda: la rete di business e quella di missione. Nella seconda parte degli anni Novanta, prese piede il commercio elettronico sul web e iniziarono a svilupparsi tecnologie basate su *web services* che permettono l'interazione remota tra i servizi di sistemi informativi. Questo ha portato la rete di business aziendale ad aprirsi verso l'esterno attraverso anche l'utilizzo di terze parti per l'erogazione di alcuni servizi fino all'integrazione tra la rete di business di un'azienda e quelle dei suoi fornitori o clienti.

In questo processo, il perimetro fisico dell'azienda ha iniziato a perdere progressivamente di significato poiché le connessioni informatiche possono essere sfruttate da cybercriminali per entrare all'interno del perimetro e sottrarre informazioni sensibili. Tale trend è continuato negli anni Duemila grazie all'avvento delle cloud e dei social che portano sempre più dati all'esterno. Inoltre, in quegli anni, con l'irrompere di smartphone e tablet si è intensificata l'abitudine di portare i propri dispositivi personali al lavoro (Bring Your Own Device) utilizzati come strumenti di processamento di dati sensibili aziendali. Questi dispositivi, essendo molto più esposti a minacce, contribuiscono ad abbattere il perimetro fisico e aumentano i rischi di sottrazione dati.

La decade che stiamo vivendo è quella in cui le macchine di aziende diverse parlano tra loro per migliorare i processi produttivi (cyber-physical systems o Internet delle Cose). Quindi anche le reti di missione di fornitori e clienti vanno a integrarsi direttamente. Nel futuro le industrie o le reti d'impresa avranno bisogno, per ottimizzare le loro produzioni, di alimentare algoritmi di intelligenza artificiale sempre più voraci di dati in input che prenderanno da reti di missione e reti di business di fornitori e clienti. In tutto ciò il perimetro fisico è scomparso e tutto è stato trasferito nel cyberspace, aumentando a dismisura la superficie di attacco di ogni organizzazione.

Nel cyberspace la minaccia è quindi in continua evoluzione, cambia in funzione della capacità dell'attaccante, della tecnologia e delle vulnerabilità presenti nell'hardware, nel software e nei processi. In questo scenario il numero di cybercriminali che possono attaccare un'organizzazione è diventato enorme grazie al fatto che: le tecnologie internet annullano le distanze

fisiche; il rischio associato alla perpetrazione del reato è basso considerate le ridotte capacità di attribuzione nel cyberspace; gli strumenti per l'attacco sono sempre più semplici da reperire e utilizzare. Inoltre, tutte le tecnologie di stoccaggio dell'informazione sono basate su software e quindi inclini alla presenza di vulnerabilità spesso sconosciute all'organizzazione stessa.
La minaccia, in questo scenario, è difficile da modellare e quindi proibitiva da affrontare per una singola organizzazione in termini economici e tecnici.
Tutto ciò alimenta il fiorire di collaborazioni pubblico-pubblico, pubblico-privato e privato-privato per aumentare la capacità di risposta alla minaccia cyber condividendo costi e risultati. Tuttavia, l'imprevedibilità, la dimensione e la complessità della minaccia hanno reso necessaria una collaborazione forte con le università e la ricerca per comprendere il fenomeno e quindi reagire in modo efficace.

LA PARTNERSHIP INTELLIGENCE-RICERCA

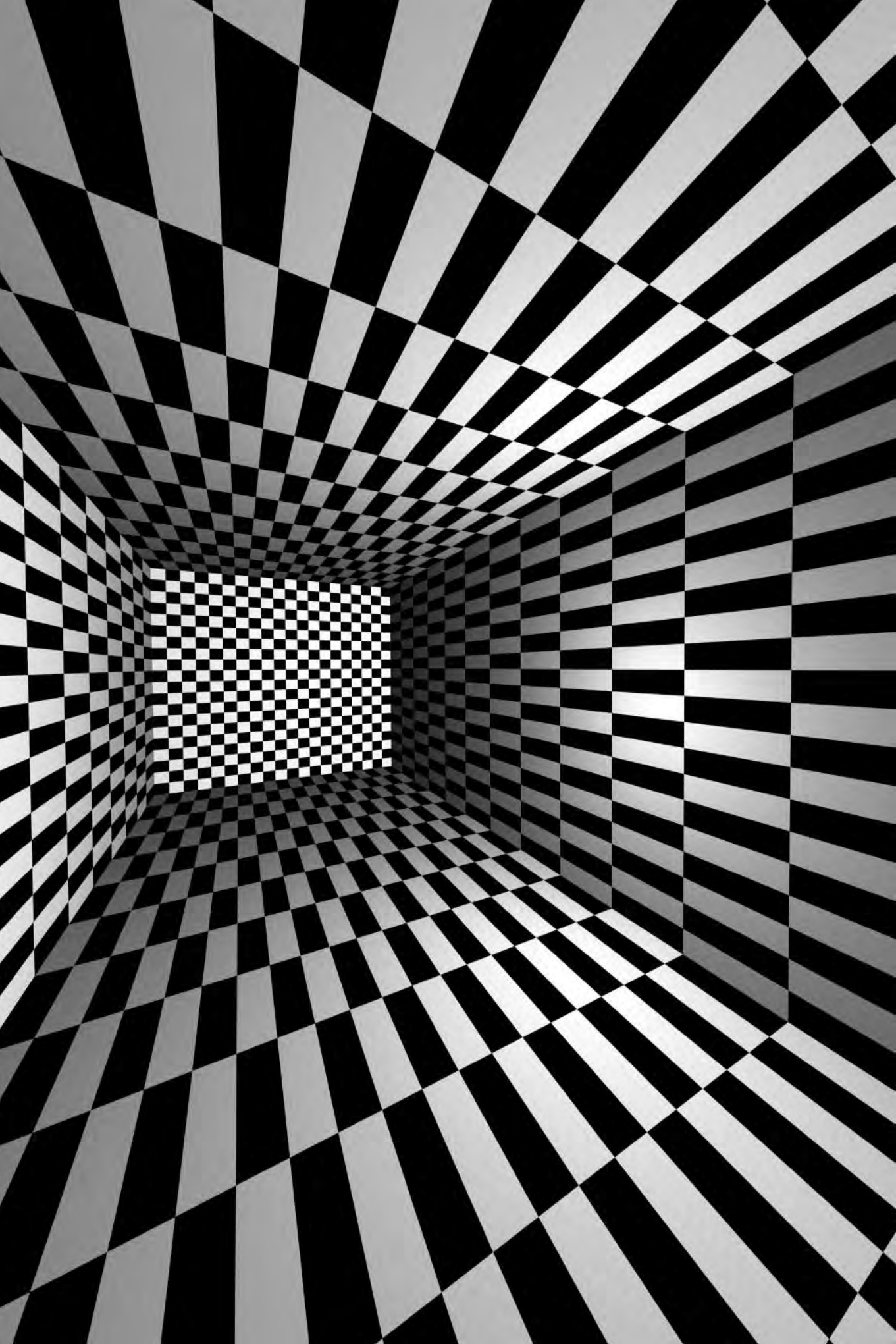
Il rapporto tra ricerca e intelligence è sempre esistito nelle culture occidentali e il nostro Paese non fa eccezione. Tuttavia in Italia le interazioni tra i due mondi erano state spesso puntiformi, mirate a un piccolo gruppo di ricercatori e alle loro specifiche competenze di nicchia, ma d'interesse per la sicurezza nazionale. La trasformazione digitale e l'ampiezza della minaccia cyber a essa associata hanno cambiato il paradigma. Infatti, rispondere a questioni chiave come, ad esempio, l'attribuzione di un attacco richiede competenze multidisciplinari che partono dalla sicurezza informatica e, successivamente, passano per diversi campi di ricerca specifici dell'informatica e delle reti di calcolatori fino a toccare l'organizzazione aziendale, la psicologia, il diritto internazionale e la geopolitica. Di conseguenza le sfide multidimensionali imposte dalla minaccia cyber devono essere affrontate attraverso masse critiche di ricercatori allineati sull'obiettivo, con un nocciolo duro nell'ambito delle tecnologie digitali e della sicurezza informatica e gruppi che si diramano poi in una moltitudine di settori di ricerca.
L'intelligence ha riconosciuto, a partire dal 2010, la ricerca e l'università come elementi fondanti per: aumentare la consapevolezza sul problema a livello nazionale; costruire la workforce indispensabile per implementare qualsiasi piano di difesa cibernetica nazionale; contribuire a progettare metodologie, strumenti e sistemi per contrastare la minaccia. Le Autorità delegate per la sicurezza della Repubblica e i Direttori degli Organismi d'intelligence che si sono succeduti in questi anni hanno sostenuto convintamente questo partenariato e sono stati, quindi, gli artefici del cambio di paradigma che ha portato a un'alleanza strutturata.

Grazie a essa, nel 2011 viene creato alla Sapienza il Centro di ricerca di cyber intelligence e information security (Cis-Sapienza), che include 50 docenti universitari nel settore economico, giuridico e tecnologico. Successivamente, nel 2014, vede la luce il Laboratorio nazionale di cybersecurity, istallato all'interno del Consorzio universitario nazionale informatica, che attualmente include 40 università pubbliche e private e cinque centri di ricerca nazionali come Enea, l'Istituto italiano di tecnologia, la Fondazione Bruno Kessler, l'Istituto affari internazionali e la Fondazione Ugo Bordoni.
Nel 2017 si realizza il connubio tra Laboratorio nazionale di cybersecurity e Cnr attraverso il Comitato nazionale per la ricerca in cybersecurity, concretando così un'unica interfaccia alla ricerca pubblica e a quella nelle università a cui afferiscono circa 500 ricercatori, ognuno con il suo gruppo. Tale soluzione supera in parte la problematica, ben nota nell'università italiana, della dispersione sul territorio delle conoscenze di settore. La rete, infatti, ha lo scopo di assistere il Governo e l'industria nazionale nello sviluppo di progetti tecnologici, pubblici e riservati, e nell'attuazione di azioni orizzontali abilitanti come la formazione o la sensibilizzazione. Tutto ciò viene realizzato impiegando un approccio di referenze di stile anglosassone per cercare di reclutare, su ogni iniziativa, le migliori competenze presenti nel Paese. Di seguito, alcuni esempi di azioni nazionali di pubblico dominio concepite e realizzate in questi ultimi tre anni:

– *il framework nazionale per la cybersecurity*[1] (2016), documento che raccoglie 98 best practices per una corretta gestione nel tempo del rischio cyber di un'organizzazione. Viene fornita una metodologia per contestualizzare e semplificare il framework rispetto all'esposizione al rischio cyber. Il framework è stato realizzato da un gruppo di lavoro guidato da Cis-Sapienza e dal Laboratorio nazionale di cybersecurity a cui hanno partecipato i principali attori della cybersecurity pubblica e le maggiori aziende strategiche nazionali;

– *i controlli essenziali di cybersecurity*[2] (2017), compendio di quindici pratiche di sicurezza che ogni azienda, in particolare le piccole e le piccolissime, deve adottare per aumentare il livello di sicurezza evitando di mettere a rischio i committenti. Il framework è stato realizzato da un gruppo di lavoro guidato da Cis-Sapienza e dal Laboratorio nazionale di cybersecurity a cui hanno partecipato alcuni attori della cybersecurity pubblica e un gruppo di aziende nazionali;

1. <www.cybersecurityframework.it/> [13-11-2017].
2. <www.cybersecurityframework.it/csr2016> [13-11-2017].



– il progetto *filierasicura*[3] (2017), studio delle modalità per aumentare la cyber sicurezza all'interno della catena di approvvigionamento di un'azienda strategica nazionale dalle minacce legate all'impiego di hardware e software specifico fino allo studio della sicurezza dei processi aziendali rispetto alla minaccia cyber. Il progetto, finanziato da Cisco US e da Leonardocompany SpA, è guidato dal Laboratorio nazionale di cybersecurity e include sette prestigiose università nazionali;

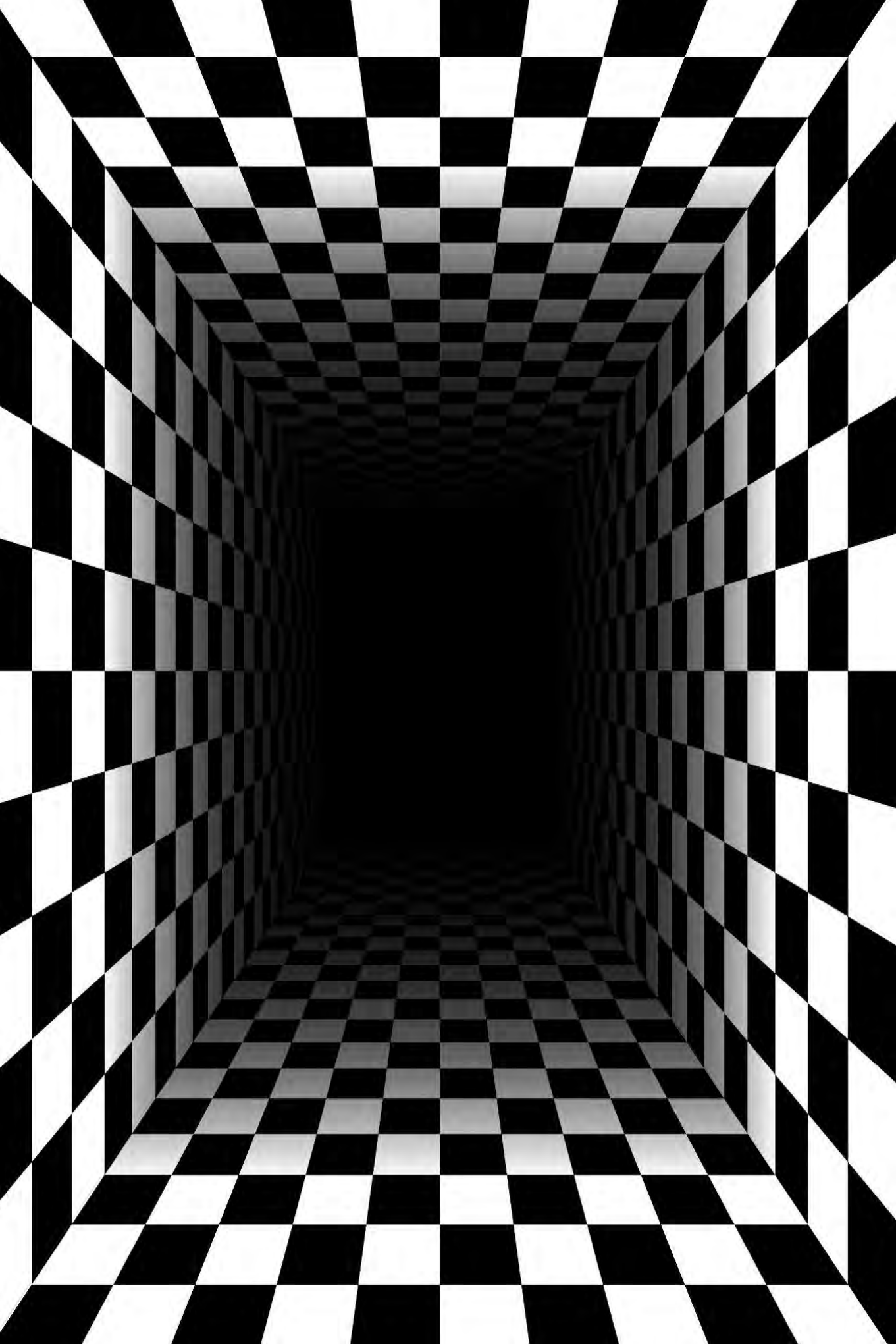
– *il programma nazionale di ricerca di talenti* Cyberchallenge.IT[4] (2016), ospitata nella prima edizione alla Sapienza, ha portato alla selezione di 20 talenti tra i 16 e i 21 anni all'interno di un gruppo di 800 ragazzi che avevano fatto domanda di partecipazione. I ragazzi prescelti sono stati sottoposti a tre mesi di corso di attacco e difesa informatica in preparazione di una Capture-the-Flag nazionale. I vincitori della Ctf nazionale hanno rappresentato, per la prima volta, l'Italia alla Ctf europea organizzata da Enisa, piazzandosi al terzo posto. Nel 2018 Cyberchallenge.IT sarà erogata da dieci università italiane;

– *il libro bianco della cybersecurity nazionale*[5] (2015), realizzato da oltre 60 ricercatori di più di 20 università e centri di ricerca nazionali, ha avuto lo scopo di focalizzare le sfide più importanti, elencando una serie di raccomandazioni per il decisore politico che sono state per la gran parte assorbite dal Dpcm Gentiloni del 2017. Nella nuova versione del libro bianco, in uscita a inizio 2018, l'accento verrà posto su progetti importanti da realizzare nel pubblico e nel privato per aumentare il livello di resilienza del Paese rispetto ad attacchi di tipo cibernetico;

– la *conferenza nazionale sulla cybersecurity* Itasec[6] (2016). Qualsiasi piano operativo venga definito a livello nazionale ha bisogno di una comunità che lo implementi. Itasec vuole riunire tutti gli appartenenti a questa comunità nel pubblico, nel privato e nella ricerca nazionale all'interno di un evento annuale guidato dall'accademia. La prima edizione di Itasec si è tenuta nel 2016 a Venezia alla presenza di oltre 500 partecipanti. La seconda si terrà a Milano nel gennaio del 2018.

La partnership intelligence-ricerca è destinata a continuare e a consolidarsi nel tempo. Come ricordato dal presidente Junker nel discorso dell'Unione di quest'anno, la cybersecurity è la seconda emergenza europea dopo il cambiamento climatico. La partnership deve fare un salto di qualità importante. Infatti, la rete ha una debolezza intrinseca legata all'assenza di una struttura centrale, un *core* strategico, organizzativo e operativo. È importante che questo e i prossimi governi intervengano supportando una transizione da rete a struttura operativa a servizio del bene pubblico e della sicurezza nazionale.

3. <www.filierasicura.it> [13-11-2017].
4. <www.cyberchallenge.it> [13-11-2017].
5. <www.consorzio-cini.it/labcs-home/libro-bianco> [13-11-2017].
6. <www.itasec.it> [13-11-2017].



EVOLUZIONE DELLA MINACCIA CIBERNETICA E DELLE RELATIVE CAPACITÀ DI REAZIONE E RISPOSTA

Michele Colajanni

La rivoluzione digitale comincia a destare preoccupazione a tutti i livelli. Finalmente. È un primo passo, auspicabile ma non risolutivo, in quanto l'inquietudine senza consapevolezza delle cause induce a scelte erronee. La rivoluzione digitale è una trasformazione epocale che non condurrà tutti verso un'Arcadia felix: alcune Nazioni, aziende e persone ne beneficeranno; altre subiranno perdite in termini economici, lavorativi e sociali. Anche la minaccia cibernetica è un unicum della storia: inafferrabile, in continua evoluzione, pervasiva. Persone, aziende e organizzazioni costituiscono un bersaglio. Qualsiasi dispositivo, i relativi dati e applicazioni rappresentano un obiettivo.

Gli avversari possono agire nell'ombra, protetti da tecniche di anonimizzazione e da distanze che costituiscono un problema solo per le Forze dell'ordine contingentate dai confini nazionali.

Prof. Michele Colajanni, docente universitario.

Furto di dati, furto di denaro e sabotaggio dei servizi informatici hanno rappresentato i rischi degli anni Novanta e Duemila. Di recente, si sono aggiunti quelli connessi al sabotaggio d'impianti e alla guerriglia informativa che, in termini economici e d'impatto sociale, rappresentano una preoccupante escalation. All'orizzonte si profilano i rischi connessi all'intelligenza artificiale che, se non ben gestita, potrebbero risultare l'*atto definitivo*.
Ciascuna di queste minacce può essere affrontata e, se non debellata, almeno temperata. Non esistono scorciatoie né azioni unilaterali e tantomeno soluzioni tecnologiche. È l'intero Paese che deve prendere consapevolezza e muoversi in modo sinergico in quanto risultare perdenti in una rivoluzione planetaria determina il declino di una Nazione.

IL FATTORE UMANO

Nonostante la narrativa vigente, i maggiori problemi cyber sono causati da comportamenti errati e carenze organizzative, non dalla tecnica. Vi sono innumerevoli vulnerabilità e ancor più minacce pronte a sfruttarle, ma la causa prevalente è l'uomo. Tre fattori meritano una riflessione.
Per troppi anni, il top management è stato assente nella gestione del processo di digitalizzazione e della sicurezza informatica derubricati a problemi tecnici. La trasformazione digitale e le relative politiche di sicurezza vanno governate ai massimi livelli, non dai tecnici, non dai consulenti, non da uffici preposti ad altri processi.
Il professionista, che gestisce sistemi e applicazioni, può commettere errori, ma ogni minimo sbaglio può essere sfruttato dall'avversario. La sfida è ben lungi dall'essere cavalleresca.
Ma il miglior alleato di ogni attaccante sono le debolezze di tutti noi utenti di servizi informatici. Scarsa osservanza delle regole, insoddisfazione, ricerca di facili guadagni e di pseudo-amicizie, esibizionismo costituiscono il terreno fertile di 'esche digitali' mediante le quali gli avversari agganciano noi e le nostre organizzazioni. Le nostre debolezze riguardano anche la leggerezza nell'uso dei servizi digitali, l'illusione che – caso unico nella storia economica – possano essere gratuiti senza alcuna contropartita. E le grandi multinazionali dell'informatica, moderni pifferai di Hamelin, sono abilissimi nel promuovere tale inconsapevolezza.
Nessuno emerge senza colpe e ha poco senso maledire gli attaccanti. I criminali informatici, i mercenari, gli attivisti, gli apparati parastatali svolgono il loro lavoro con determinazione, fantasia e competenza. Enormi margini di miglioramento sono da ricercarsi lato vittime e difensori, ove si riscontrano incompetenze digitali e carenze di specialisti.

La sicurezza delegata alle tecnologie proposte dal marketing come 'protezione totale' è illusoria e deleteria in quanto induce deresponsabilizzazione, mentre siamo tutti in prima linea. Quando e se diverrà veramente efficace, la protezione totale sarà venduta insieme a polizze cyber-Kasko. Fino ad allora, sana diffidenza e investimenti tecnologici mirati.
Se i maggiori problemi cibernetici sono dovuti a fattori umani, le capacità di reazione e risposta si devono basare sull'informazione e formazione a tutti i livelli. Le scuole e le università giocano un ruolo chiave, ma servono istruttori, ricercatori, docenti e un piano nazionale straordinario per acquisirli. Parallelamente, va contrastato il continuo flusso migratorio di esperti verso altri Paesi: defiscalizzare per migliorare le retribuzioni, adottare nuove forme di contratti e moderni percorsi di carriera sono alcuni obiettivi da perseguire.

IL FATTORE SOFTWARE

Le applicazioni costituiscono l'essenza della rivoluzione digitale. Tutto è software e ciò che non lo è lo sarà. Il software rappresenta il valore aggiunto delle infrastrutture e dei dispositivi fisici, ed è altissimo prodotto dell'ingegno informatico. O così dovrebbe essere. La realtà è differente. Per vari motivi, tra cui l'oggettiva complessità del manufatto e la concorrenza spietata, l'altissimo prodotto è spesso un semilavorato parzialmente testato e pertanto vulnerabile, 'bacato' per adottare un termine gergale quanto espressivo. Più del 90% dei problemi informatici è causato da software difettoso o da configurazioni errate.
Inoltre, vi sono da considerare i fattori di amplificazione che rendono tali vulnerabilità ancor più critiche. In primis, l'intervento degli Stati. Nel momento in cui l'economia e la società stanno transitando verso il digitale e tutti i processi industriali e organizzativi ne sono pervasi, non c'è più spazio per il romanticismo che ha connotato gli albori di internet e dell'informatica. Le Difese hanno dichiarato lo spazio cibernetico quinta dimensione e possibile terreno di confronto. Di conseguenza, tutti si stanno dotando di *cyber warrior* e di silos di armi digitali. L'intervento statale ha determinato un'impennata dei prezzi, che sta spingendo molti informatici a dedicarsi all'individuazione di nuove vulnerabilità rivendibili a caro prezzo ad aziende intermediarie con tanto di tariffari esposti in rete. Purtroppo, i silos digitali si sono dimostrati molto meno difendibili dei silos atomici con conseguenze devastanti: varie armi digitali sono state trafugate e messe alla mercé della rete. Alcuni criminali ne hanno approfittato lanciando nella primavera 2017 attacchi su larga scala che hanno causato danni per 4-5 miliardi di dollari e guadagni al confronto risibili, stimabili in qualche decina di milioni di dollari.

Tre ordini di grandezza tra danni e benefici dovrebbero sensibilizzare qualunque amministratore e manager su quale sia il principale terreno di scontro e confronto del prossimo futuro. Farsi trovare impreparati, ritardare gli interventi e investimenti nel settore della sicurezza informatica è inaccettabile nel momento in cui l'informatica ci conduce verso l'Impresa 4.0, mentre la società e le città diventano sempre più *smart*. Se affrontassimo la sicurezza dei sistemi industriali e delle infrastrutture critiche con la stessa superficialità, sottovalutazione, investimenti errati che sono stati adottati dal mondo informatico negli ultimi vent'anni, rischieremmo scenari da fantascienza apocalittica.
Fortunatamente, a differenza delle aziende di produzione software, l'industria che caratterizza il nostro Paese, favorita o forzata da regolamentazioni e standard, ha introiettato la cultura della sicurezza *by design* dei prodotti. Non esistono analoghe norme che obblighino i fornitori software a garantire la sicurezza dei propri manufatti e, quindi, il fattore economico diventa abilitante a favore della sicurezza preventiva e del controllo del processo di aggiornamento. Le grandi aziende nazionali sono fondamentali in quanto possono pretendere la sicurezza intrinseca dei prodotti informatici, così come la pretendono dai fornitori di componenti e servizi delle altre industrie. La buona qualità del software diventerà prima un differenziatore con relativo vantaggio competitivo del fornitore, poi un obbligo certificato a livello nazionale o internazionale. Almeno, questi sono gli auspici.

LA GUERRIGLIA INFORMATIVA E IL RUOLO DELL'INTELLIGENZA ARTIFICIALE

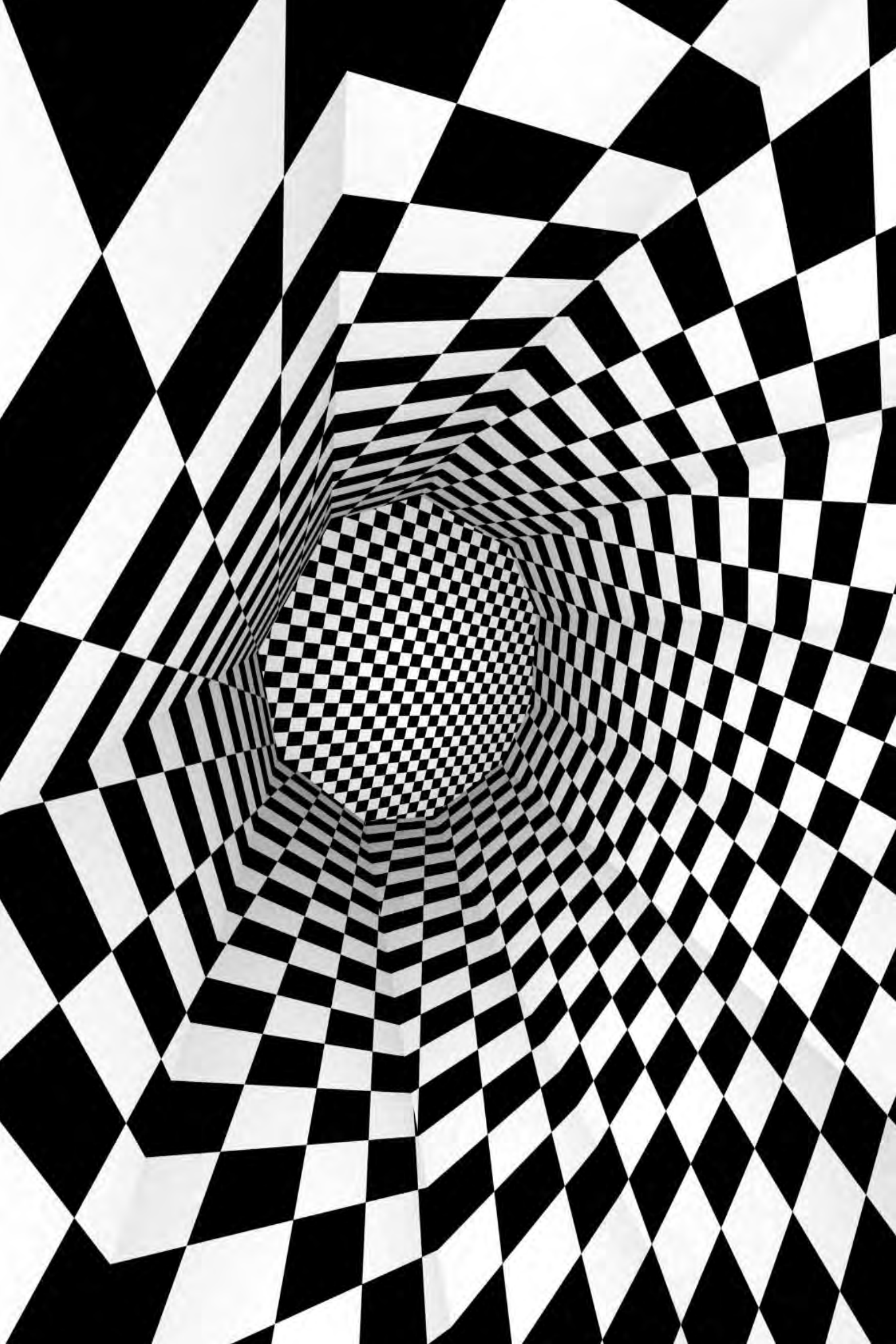
Il mondo cyber ha realizzato molto del sogno illuministico: accesso universale all'informazione, collegamento tra tutti i popoli, libertà di pensiero e di espressione. La realtà è deludente: un maggiore accesso all'informazione non ha ampliato la partecipazione dei cittadini alla vita pubblica, la totale libertà di espressione non ha migliorato la democrazia. Ora che la verità unica è morta, troppi dèi si affacciano all'orizzonte e ciascuno può esprimere il proprio pensiero sfruttando la più grande cassa di risonanza della storia. L'uomo nuovo, libero da catene e che promuove la sua verità protetto dall'anonimato di internet, si rivela sempre più spesso un essere gramo, rapace, fanatico e che nulla ha a che fare con l'oltreuomo zarathustriano. Il disagio è diffuso e si aprono margini per campagne (dis)informative soprattutto in prossimità di scadenze elettorali. Se nessuno gradisce vivere in un babelico caleidoscopio informativo di verità parziali, è anche vero che non si può tornare indietro; non si è mai tornati indietro. Gli spiriti maligni non sono rientrati nel vaso di Pandora, così abbiamo imparato a conviverci provando a limitare i danni. Le proposte orientate a censurare, correggere, imporre la verità ufficiale sono inefficaci, talvolta controproducenti, e mascherano i veri rischi del prossimo futuro.

L'uomo è sopraffatto dalle troppe verità e preferirebbe il mondo lineare a uno reticolare, ritenuto caotico perché non ha mezzi adeguati per gestirlo. Siamo a disagio con troppa informazione? Non sappiamo dove andare? Cerchiamo nuovi amici e compagnie? Ci serve un prodotto? Non sappiamo chi votare? O, viceversa, ci serve un programma elettorale? Nessun problema, l'intelligenza artificiale 'sa tutto', 'controlla tutto', 'prevede tutto', 'risponde a tutte le domande'. Più siamo a disagio, più cerchiamo una soluzione che ci garantisca la nostra *comfort zone*. Si percepisce un'aspettativa quasi messianica, favorita in tal senso dal marketing dei citati pifferai digitali. Sebbene l'intelligenza artificiale aumenterà il suo potere nella misura in cui l'uomo sarà disposto a cedere spazi di autonomia decisionale, il conflitto sulla libertà decisionale è solo un aspetto del problema.

La moderna intelligenza artificiale si fonda sull'apprendimento automatico. La macchina osserva e impara qualsiasi cosa: il comportamento, il gioco, il lavoro, il linguaggio. Si sta realizzando il più impressionante trasferimento di competenze dall'uomo alle macchine, che affievolisce la famosa dichiarazione del generale Clapper, allora direttore della National Intelligence, sulla Cina che «sta realizzando il più grande trasferimento di conoscenze della storia mediante attacchi cyber». Le conseguenze sono considerate imprevedibili dagli ottimisti, socialmente catastrofiche dagli altri.

Le armi digitali non risuonano di echi metallici, le truppe si schierano in modo silenzioso, eppure s'intravedono scontri titanici all'orizzonte. Se tutte le principali multinazionali digitali gareggiano a colpi di decine di miliardi di dollari in investimenti a favore dell'intelligenza artificiale e dei Big Data che ne costituiscono l'alimento indispensabile, se Amazon, Apple, Facebook, Google, Ibm e Microsoft, strenui rivali, creano un partenariato su 'AI to Benefit People and Society', l'impressione è che lo scenario non si limiti alla profilazione degli utenti per commercializzare prodotti.

La posta in gioco è la definizione dei ruoli e dei modi per gestire il futuro. Spiace osservare che non vi siano analoghe iniziative da parte di organismi nazionali e internazionali. Nel rapporto cittadino-Stato si è insinuato un terzo attore, vero protagonista del mondo cibernetico: le regole di quello che rappresenterà tutto il nostro mondo stanno per essere scritte da multinazionali, non da rappresentanti eletti. Tra tutte le minacce, questa è probabilmente la più insidiosa, in quanto nessun Paese che non sia dotato di analoghe corazzate digitali può farvi fronte.



CONCLUSIONI

Le minacce cibernetiche sono planetarie, ma l'Europa si muove a livello di singolo Paese. Senza speranza di competere sul piano economico-militare-cyber con Cina e Stati Uniti, sta rispondendo con le armi del diritto. Alcuni Paesi, del pari non competitivi rispetto alle due potenze mondiali, hanno preferito attrezzarsi nella 'guerra di corsa'. Altri, tra cui Regno Unito, Germania e Francia, stanno serrando le fila del sistema Paese in un modello dove collaborano Difesa, Forze dell'ordine, Intelligence, Università, grandi aziende nazionali e piccole realtà di punta. Ogni Paese sistematizza ciò che lo caratterizza: anche se non abbiamo corazzate digitali, va benissimo mettere a fattor comune snelle corvette, flessibili unità anfibie e rapide fregate.

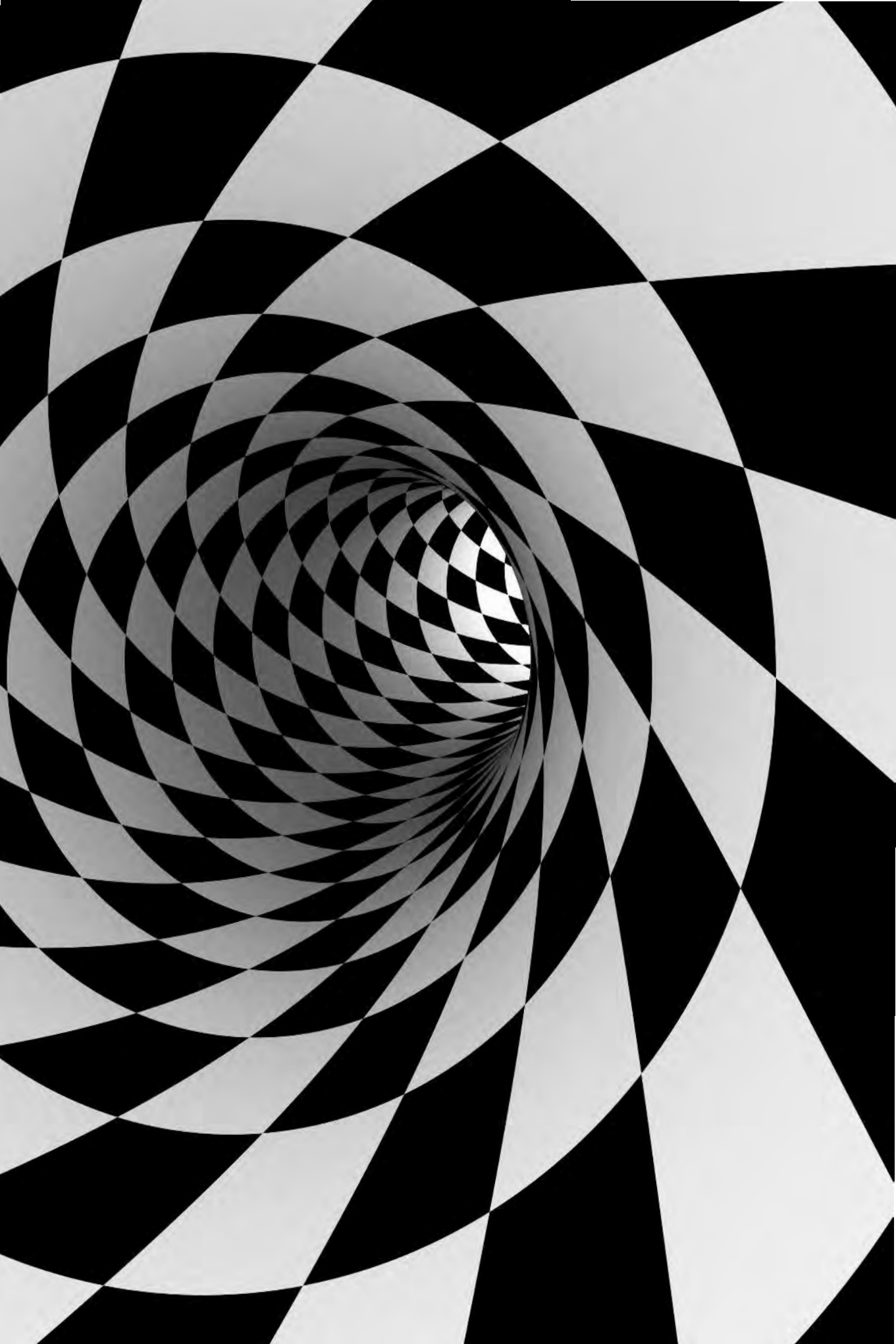
Il nostro Paese non è all'anno zero. I decreti Monti e Gentiloni che attribuiscono al Dis il ruolo di coordinamento della sfida cyber sono figli della riforma del 2007. La Difesa ha varato il Comando interforze per le operazioni cibernetiche dove la parola chiave è «interforze». Le Forze dell'ordine combattono da anni su vari fronti, procedendo anche a potenziamenti formativi nel settore. Le aziende nazionali strategiche, anche in seguito alla direttiva europea Nis, collaborano tra loro e con le entità nazionali. Le università hanno risposto sia sul piano della formazione specialistica che della ricerca. Abbiamo ampi margini di miglioramento, ma la strada intrapresa è giusta. E, soprattutto, la natura ci ha dotato delle risorse più importanti per affrontare le sfide cibernetiche che, oltre a un computer e una buona connessione, richiedono curiosità, creatività, empatia, intuizione, di cui i nostri ragazzi sono ricchi. Sono loro il valore aggiunto su cui il Paese deve investire e, per farlo, deve adeguare la filiera di valorizzazione.

Il primo intervento è nella scuola che non richiede enormi investimenti tecnologici, ma quelli necessari ad avere formatori aggiornati e stimolanti.

La consapevolezza delle opportunità e dei rischi cyber deve diventare una componente fondamentale della cultura, pervadendo quella umanistica ed essere da questa contaminata.

Si deve agire anche a livello di aziende e organizzazioni, adeguando gli stipendi alle competenze perché i talenti vanno retribuiti. Poi, servono idee per gestire giovani competenti, con molteplici alternative, che hanno sostituito il classico mantra 'titolo di studio, ufficio, stabilità, gerarchia, stipendio elevato' con 'apprendimento continuo, ambito lavorativo piacevole, flessibilità, collaborazione, retribuzione adeguata alle competenze'. Non è semplice, ma esistono aziende e organizzazioni pronte a provarci.

Alla fin fine, anche Pandora ha liberato lo spirito della *speranza* e, probabilmente, è questa l'arma più potente da trasmettere ai giovani affinché il nostro Paese risulti vincente nella sfida cibernetica.



EVOLUZIONE DELLA NORMATIVA SULLA SICUREZZA NAZIONALE A DIECI ANNI DALLA LEGGE 124/2007

Antonino Alì

Il supremo interesse della sicurezza dello Stato, ovvero l'«interesse dello Stato-comunità alla propria integrità territoriale, alla propria indipendenza e – al limite – alla stessa sua sopravvivenza»[1] è uno dei pilastri fondamentali dello Stato in quanto soggetto di diritto internazionale ed è di conseguenza uno dei capisaldi dell'ordinamento giuridico italiano. Come affermato a più riprese dalla Corte costituzionale, questo interesse è «presente e preminente su ogni altro in tutti gli ordinamenti statali, quale ne sia il regime politico» e trova espressione, nel testo costituzionale «nella formula solenne dell'art. 52, che afferma essere sacro dovere del cittadino la difesa della Patria»[2]. Nel nostro ordinamento, la competenza in materia di difesa, Forze armate e sicurezza dello Stato è esclusivamente statale, in base all'art. 117, secondo comma lett. d) della Costituzione[3].

Prof. Antonino Alì, docente universitario.

1. Cfr. Corte cost., sentenze n. 82 del 1976; n. 86 del 1977; n. 110 del 1998 e 106 del 2009.
2. Cfr., per tutte, le sentenze n. 82 del 1976 e n. 86 del 1977. Secondo Labriola 1978, p. 45 il fondamento costituzionale dell'attività d'informazione per la sicurezza è contenuto nel principio di fedeltà alla Repubblica sancito dall'art. 54 della Costituzione; sul tema cfr. Giupponi 2010, p. 57.
3. L'unico riferimento espresso alla «sicurezza nazionale» nella Costituzione compare nell'art. 126, secondo cui, con decreto motivato del presidente della Repubblica, possono essere disposti lo scioglimento del Consiglio regionale e la rimozione del presidente della Giunta che abbiano compiuto atti contrari alla Costituzione o gravi violazioni di legge e anche per ragioni di sicurezza nazionale.

La tutela della sicurezza nazionale è la missione primaria attribuita alle Agenzie d'intelligence negli Stati, pur coinvolgendo in maniera ora diretta, ora mediata lo Stato-apparato e lo Stato-comunità[4]. In questa prospettiva il nostro ordinamento ha adottato un approccio teso ad accrescere nella società civile la consapevolezza per i temi della sicurezza nazionale e per la difesa degli interessi nazionali attraverso l'apertura al mondo accademico, ai centri di ricerca e alle imprese, sinteticamente riassumibile nell'espressione «cultura della sicurezza». Ben al di là di questa specifica missione vi è l'idea che la sicurezza nazionale sia un oggetto ampiamente condiviso e non il monopolio dello Stato-organizzazione (o solo di alcuni dei suoi organi). In questo intervento, tuttavia, la tutela della sicurezza nazionale sarà declinata in funzione dell'attività specifica del Sistema di informazione per la sicurezza della Repubblica creato nel 2007.

IL CARATTERE INNOVATIVO DELLA LEGGE 124/2007

La legge 3 agosto 2007, n. 124, sul Sistema di informazione per la sicurezza della Repubblica e la nuova disciplina del segreto di Stato, nel rivedere profondamente gli apparati d'intelligence, ha tenuto conto di numerosi fattori: la necessità di semplificare e riorganizzare gli stessi, la predisposizione di garanzie funzionali per gli appartenenti ai Servizi, la riforma del segreto di Stato in senso ampio, il potenziamento degli strumenti di controllo del Comitato parlamentare[5] per la sicurezza della Repubblica (Copasir) e, inoltre, un mutato scenario geopolitico con un quadro di potenziali minacce estremamente ampio[6]. L'attività dell'intelligence è stata concepita in funzione della sicurezza della Nazione (come evidenziato dall'ampio utilizzo dell'espressione «informazioni *per* la sicurezza»). In questo senso, si è inteso sottolineare il compito degli apparati disciplinati dalla legge 124 chiarendone la missione prioritaria finalizzata alla raccolta d'informazioni e conoscenza per il decisore politico. Il decennio successivo all'adozione della legge ha costituito un banco di prova per la verifica della solidità dell'impianto normativo. Basta sfogliare le relazioni al Parlamento dell'ultimo decennio per accorgersi della varietà e dell'importanza degli eventi che si sono succeduti: la crisi dei *subprime* che si è manifestata in tutto il suo carattere destabilizzante per il sistema finanziario ed economico mondiale; la successiva crisi del debito sovrano che ha colpito direttamente l'Italia; le instabilità prodotte a seguito della Primavera araba e la destabilizzazione di numerosi Stati dell'area mediterranea; il conflitto siriano; il terrorismo internazionale di matrice jihadista, l'aumento dei flussi migratori, solo per citare alcuni degli avvenimenti più significativi.

4. Valentini 2015, p. 145.
5. Giupponi 2010, p. 54.
6. Per un quadro complessivo, cfr. Mosca et al. 2008; Giupponi 2010 e Montagnese – Neri 2016.

La disciplina previgente, contenuta nella l. 801/1977, prevedeva che la politica informativa e di sicurezza si svolgesse «nell'interesse e per la difesa dello Stato democratico e delle istituzioni poste dalla Costituzione a suo fondamento» e prevedeva in capo al Sismi e al Sisde compiti informativi e di sicurezza, per la difesa sul piano militare dell'indipendenza e dell'integrità dello Stato da *ogni pericolo, minaccia o aggressione*, nonché compiti di controspionaggio. L'oggetto principale di tutela era lo Stato apparato e i campi di azione apparivano ampi e indeterminati, in assenza di una loro declinazione in settori specifici. Questa impostazione, con buona probabilità, derivava anche da una concezione della sicurezza nazionale focalizzata prevalentemente sugli aspetti politico-militari nel contesto di un mondo sostanzialmente bipolare.

Uno dei perni su cui ruota la disciplina introdotta dalla l. 124/2007 è l'istituzione dell'Agenzia informazioni e sicurezza esterna (Aise) e dell'Agenzia informazioni e sicurezza interna (Aisi) – cui sono affidate le attività informative che si svolgono, rispettivamente, al di fuori e all'interno del territorio nazionale, *a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia*[7] – e del Dipartimento delle informazione per la sicurezza (Dis), in qualità di organo di coordinamento delle Agenzie medesime[8].

Le classiche minacce alla sicurezza dello Stato, esplicitate nella l. 801/1977, sono state ribadite nella l. 124/2007 ove si sottolinea, in aggiunta, che esse possono derivare dalle più svariate forme di aggressione criminale o terroristica. Inoltre, al di là della protezione degli interessi politici e militari, classicamente punto di forza degli ambiti di azione dei Servizi d'informazione, si è inteso sottolineare l'ampliamento del raggio d'azione della tutela della sicurezza nazionale evidenziando la necessaria protezione degli interessi economici, scientifici e industriali dell'Italia. In altri termini, è avvenuta una sorta di perimetrazione dei campi di svolgimento delle attività informative di competenza delle Agenzie che, pur non definendo il concetto di sicurezza nazionale, descrive quali siano gli ambiti in cui quest'ultima può essere minacciata. Pertanto, pur in assenza di un'esplicita nozione di sicurezza nazionale nel testo della legge, attraverso la definizione dei compiti delle Agenzie si è messo in luce un quadro di minacce potenzialmente molto ampio e, di conseguenza, la necessità di acquisire informazione e conoscenza in campi tecnici che richiedono nuove expertise (si pensi al settore economico-finanziario e a quello cibernetico)[9].

7. Il riferimento a questi interessi è anche nell'allegato al Dpcm 8 aprile 2008 («Criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato»), pubblicato nella GU del 16 aprile 2008, n. 90 dove, in via esemplificativa, si fa riferimento alle materie della «tutela di interessi economici, finanziari, industriali, scientifici, tecnologici, sanitari e ambientali» ai fini dell'apposizione del segreto di Stato.

8. Soi 2014.

9. Sul tema complesso della nozione di sicurezza nazionale, cfr. Valentini 2002 e 2015.

Ciò ha richiesto che fossero apportati una serie di aggiornamenti, tanto della normativa primaria che secondaria, per rispondere alle nuove esigenze e alle sollecitazioni anche di carattere internazionale / europeo. In questo senso, giova ricordare che il quadro internazionale (ed europeo) ha un impatto sull'attività dei Servizi, come evidenziato tanto nell'articolo 6, quanto nell'art. 7, secondo cui l'attività dell'Aise e dell'Aisi si svolge «anche in attuazione di accordi internazionali». Pur competenza intima dello Stato, gli impulsi derivano dunque anche da accordi che lo stesso decida di concludere sul piano esterno per la gestione delle minacce.

LA SICUREZZA ECONOMICA NAZIONALE

La considerazione quasi scontata che la sicurezza nazionale dipenda anche dalla situazione economica dello Stato (e dalla sua sicurezza su questo versante) e, quindi, dalla sua capacità d'investire nella protezione dei propri interessi è ormai un tema centrale degli ultimi decenni per la maggioranza degli Stati della comunità internazionale[10]. La sicurezza economica dello Stato, in termini generali, ha un impatto immediato sulle altre componenti della sicurezza nazionale specialmente in un periodo in cui emergano minacce di nuovo genere. È abbastanza chiaro che il fenomeno migratorio e quello degli attacchi informatici alle infrastrutture critiche e alla proprietà intellettuale comportano costi non indifferenti per lo Stato. Non ultima, la questione energetica, formalmente ricadente all'interno delle questioni di sicurezza economica nazionale, ma con peculiarità così specifiche da renderla un settore dalle caratteristiche proprie, in relazione alle problematiche connesse alla dipendenza del nostro Paese in questo settore.

Va osservato che la dimensione economica della sicurezza nazionale è anche una conseguenza inevitabile dell'ampio utilizzo dell'intelligence economica da parte degli Stati (e, in particolare, di quelli che sono diretti concorrenti dell'Italia sul piano internazionale) sia in funzione difensiva, ma soprattutto in funzione offensiva.

Le minacce in questo campo hanno trovato risposte, anche in termini di sistema Paese, che hanno coinvolto ampiamente sia lo Stato organizzazione sia lo Stato-comunità e determinato un aumento degli scambi tra il settore pubblico e quello privato.

10. Fin dalla prima Relazione annuale sulla politica dell'informazione per la sicurezza del 2007 vi è un chiaro riferimento alla sicurezza economica nazionale. Per Jean – Savona 2011, p. 115, la legge in questo senso segna «un punto di svolta per il futuro dell'intelligence economica in Italia prevedendo sinergie e coordinamento fra le varie amministrazioni dello Stato»; Savona 1999; Gaiser 2015.

La l. 124 si dimostra, sotto questo aspetto, ancora attuale, a dieci anni dalla sua entrata in vigore, nella misura in cui le sfide hanno condotto – come emerge dalle Relazioni al Parlamento – all'ampliamento degli ambiti specifici di intervento che richiedono figure con alta preparazione tecnica.

È di tutta evidenza l'estensione e la rilevanza delle minacce che rischiano d'indebolire l'economia dello Stato e che, in alcuni casi, sono il risultato di operazioni dirette o indirette condotte da altri Stati. Ha sollevato particolare attenzione, come viene evidenziato a più riprese nelle Relazioni al Parlamento, la progressiva emersione dell'azione dei Fondi sovrani e, non meno importante, delle imprese pubbliche o private rispondenti a strategie statali più che a quelle di un investitore privato operante in un'economia di mercato aperta. È un settore caratterizzato da alta impermeabilità informativa e non è sempre facile comprendere e valutare l'effetto sulla sicurezza nazionale. Si tratta, peraltro, di giudizi estremamente delicati in termini di opportunità / rischi che non devono limitare l'apertura dei nostri mercati con anacronistici blocchi.

È necessario, dunque, operare delle *valutazioni* («di impatto sulla sicurezza economica») che tengano conto della progressiva 'giuridicizzazione dell'economia' tanto a livello europeo che internazionale; fondamentali si rivelano, pertanto, la comprensione e l'utilizzo di tutti gli strumenti economico-giuridici per la tutela dell'interesse nazionale e, in ultima analisi, per la protezione della sicurezza dello Stato.

Si può osservare che la sicurezza nazionale, pur restando, secondo il dettato dell'art. 4, par. 2, del Trattato sull'Unione europea, un'esclusiva competenza dei Paesi membri, si muove in un quadro fortemente normato dove le risposte dello Stato rischiano di entrare in collisione con le regole dell'Unione e/o internazionali.

A questo proposito va ricordata la nota vicenda che ha portato alla progressiva modifica delle regole relative alla *golden share* e all'adozione di una legge più organica sulla tutela degli assetti strategici nazionali (legge 11 maggio 2012, n. 56 e relativi decreti di attuazione del 2014). In assenza di una disciplina europea unitaria in materia, il nostro ordinamento, così come altri, si è adoperato per rispondere alle obiezioni mosse dalla Corte di giustizia dell'UE. La legge, attribuendo al Governo poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché in quelli dell'energia, dei trasporti e delle comunicazioni, mira a tutelare lo Stato dalla minaccia derivante da un investimento o dall'acquisizione di una società nei settori indicati. In questo campo è fondamentale l'attività di supporto informativo ai fini dell'adozione di strumenti interdittivi rispetto a operazioni che minaccino la sicurezza nazionale[11].

11. Il recente Dpcm del 16 ottobre 2017, espressione dell'attività congiunta del Sistema, è il risultato tanto dell'applicazione della legge sui golden powers che della direttiva contenuta nel Dpcm del 17 febbraio 2017 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.

LA TUTELA DELLA SICUREZZA INFORMATICA NAZIONALE

A cinque anni dalla legge istitutiva del Sistema di informazione per la sicurezza il Legislatore è intervenuto con la legge 7 agosto 2012, n. 133 che, tra l'altro, ha inteso «rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali», assegnando alle due Agenzie le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali e al Dis la relativa attività di coordinamento.
Sulla base dell'art. 1 comma 3-bis della citata l. 133/2012, il presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (Cisr), ha adottato nel 2013 la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali[12], poi rivista il 17 febbraio di quest'anno[13], con il fine di definire «in un contesto unitario e integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali». Sono stati così adottati: il «Quadro strategico nazionale per la sicurezza dello spazio cibernetico, contenente l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale»; il «Piano nazionale per la protezione cibernetica e la sicurezza informatica contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale»[14]. La l. 133/2012, nel novellare l'art. 38, comma 1-bis, della l. 124/2007, ha previsto, inoltre, che alla relazione annuale al Parlamento sulla politica dell'informazione per la sicurezza venga allegato il «documento di sicurezza nazionale» concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica.

L'AGGIORNAMENTO DELLA NORMATIVA IN MATERIA DI SICUREZZA NAZIONALE NEL QUADRO EUROPEO E INTERNAZIONALE

È di tutta evidenza che il nostro Legislatore abbia inteso rispondere alle sfide dell'ultimo decennio conservando la l. 124/2007. In alcuni casi si è provveduto con corpi normativi separati, in altri casi con ritocchi alla medesima e successivi interventi con norme primarie e secondarie.

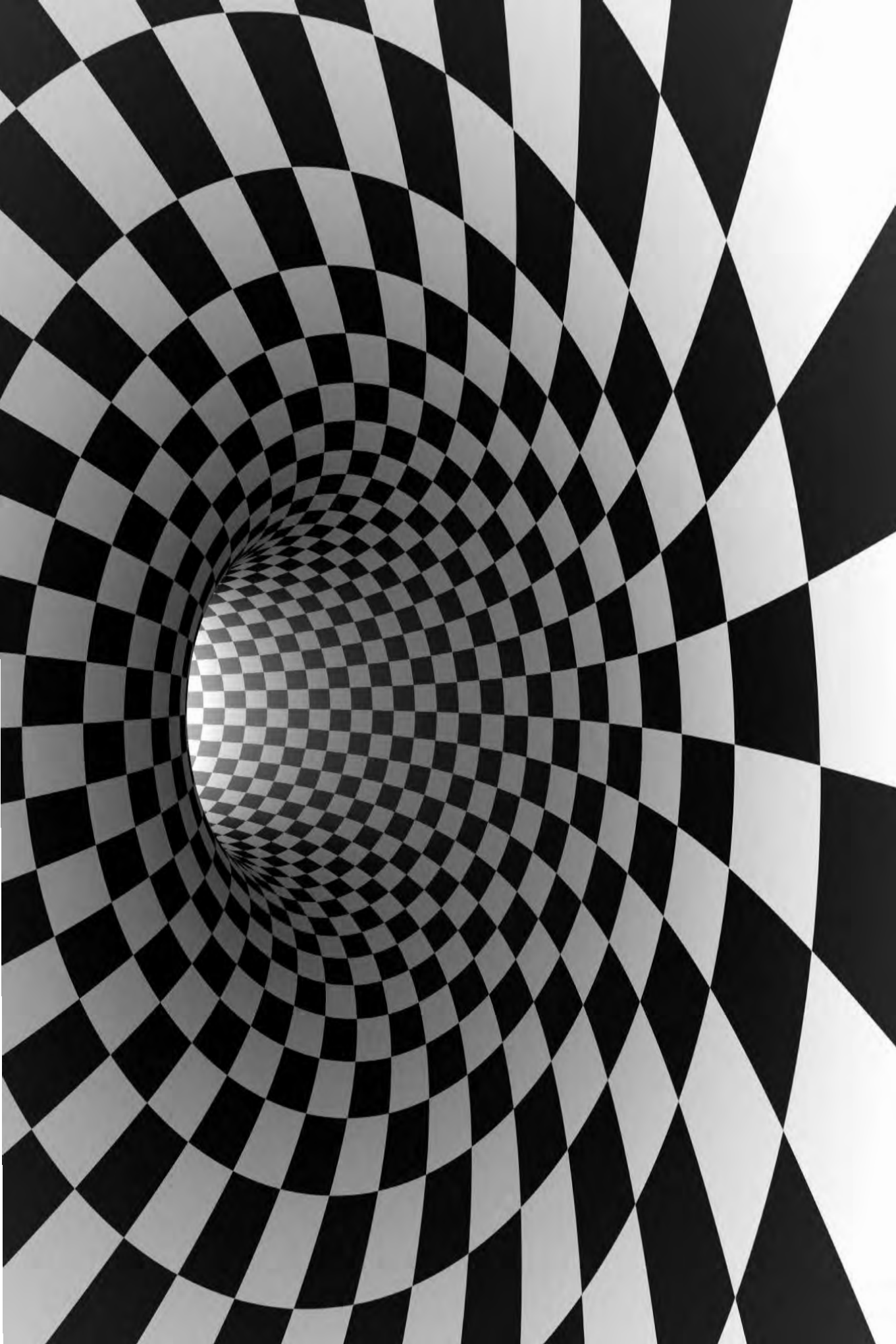
12. Dpcm del 24 gennaio 2013 (GU n. 66 del 19 marzo 2013).
13. Dpcm del 17 febbraio 2017 (GU n. 87 del 13 aprile 2017).
14. GU n. 125 del 31 maggio 2017.

In particolare, nel settore dell'economia e della cibernetica[15] si è intervenuti anche in ragione di vincoli internazionali ed europei. Come abbiamo avuto modo di sottolineare, sia pure in assenza di un atto UE armonizzatore-uniformatore, la normativa sulla c.d. *golden share* è stata sostituita dalla più compatibile disciplina dei c.d. *golden powers*. È stata inoltre recepita la direttiva UE relativa all'individuazione e alla designazione delle infrastrutture critiche europee[16]. A breve un esito significativo avrà il recepimento nell'ordinamento interno della Direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva Nis)[17].

15. Senza dimenticare il settore del terrorismo internazionale, si pensi agli interventi normativi per recepire gli obblighi contenuti nella risoluzione del Consiglio di Sicurezza delle Nazioni Unite, 2178 del 24 settembre 2014 sulla risposta della comunità internazionale al fenomeno dei foreign terrorist fighters; cfr. Alì 2015, pp. 181 ss.
16. La direttiva 2008/114/CE dell'8 dicembre 2008 in GU dell'UE L. 345 del 23 dicembre 2008 recepita con D. Lgs n. 61 dell'11 aprile 2011 in GU 102 del 4 maggio 2011.
17. In GU dell'UE, L. 194/1 del 19 luglio 2016 e in attesa di recepimento dello Stato italiano.

BIBLIOGRAFIA

A. Alì, *Il diritto dell'Unione europea e la tutela della sicurezza nazionale degli Stati membri*, in U. Gori – L. Martino (a cura di), *Intelligence e interesse nazionale*, Aracne, Roma 2015.
A. Alì, *La risposta della Comunità internazionale al fenomeno dei foreign terrorist fighters*, «La Comunità internazionale» 20015, II volume.
G. Cocco, *I servizi di informazione e di sicurezza nell'ordinamento italiano*, Cedam, Padova 1980.
A. Corneli, *I servizi di intelligence e l'interesse nazionale*, «Per Aspera ad Veritatem» (1997) 7.
L. Gaiser, *Intelligence economica*, Aracne, Roma 2015.
T.F. Giupponi, *Le dimensioni costituzionali della sicurezza*, Libreria Bonomo, Bologna 2010.
T.F. Giupponi, *La riforma del sistema di informazione per la sicurezza della Repubblica e la nuova disciplina del segreto di Stato*, in G. Illuminati (a cura di), *Nuovi profili del segreto di Stato e dell'attività di intelligence*, Giappichelli, Torino 2010, pp. 53-128.
C. Jean – P. Savona, *Intelligence economica*, Rubbettino, Soveria Mannelli 2011.
S. Labriola, *Le informazioni per la sicurezza dello Stato*, Giuffrè, Milano 1978.
A. Montagnese – C. Neri, *L'evoluzione della sicurezza nazionale italiana* (2016): <http://www.sicurezzanazionale. gov.it> [10-11-2017].
C. Mosca et al., *I servizi di informazione e il segreto di Stato*, Giuffrè, Milano 2008.
A. Poggi, *Servizi di informazione e sicurezza*, in *Dig. disc. pubbl.*, XV, Torino 1999.
P. Savona, *Presupposti, estensione, limiti e componenti dell'organizzazione dell'intelligence economica. Inaugurazione dell'a.a.* 1999-2000 *della Scuola di addestramento del Sisde*, «Per Aspera ad Veritatem» 15 (1999).
A. Soi, *L'intelligence italiana a sette anni dalla riforma*, «Forum di Quaderni Costituzionali» (2014) 3: <http://www.forumcostituzionale.it/wordpress/wp-content /uploads /2014/09 / L'intelligence-italiana-a-sette-anni-dalla-riforma-A.-Soi.pdf> [10-11-2017].
M. Valentini, *Sicurezza nazionale, sicurezza della Repubblica*, «Per Aspera ad Veritatem» (2002) 22 .
M. Valentini, *Sicurezza della Repubblica tra teoria e prassi*, «Rivista di Polizia» (gennaio-febbraio 2015).



LA TUTELA DELL'INTERESSE NAZIONALE

NEL NUOVO SISTEMA INTERNAZIONALE

Alessandro Colombo

Dal principio degli anni Novanta, per effetto dapprima del collasso dell'ordine bipolare e poi del declino apparentemente inarrestabile del 'Nuovo ordine' chiamato a sostituirlo, la tutela dell'interesse nazionale italiano ha dovuto passare attraverso un processo ininterrotto di adattamento.

Il contenuto dell'interesse nazionale

Intanto, è cambiata la natura stessa dell'interesse da tutelare. Con il venir meno di ogni minaccia credibile alla sopravvivenza fisica e all'integrità territoriale, la tutela dell'interesse nazionale ha finito per mettere in primo piano tutte quelle dimensioni, non necessariamente militari, capaci di avere «un impatto diretto sulla vita, l'incolumità e il benessere dei cittadini»[1] – dalla dimensione economica a quella ambientale fino a quella in senso lato identitaria. Una volta scardinata la rigidità del precedente mondo bipolare, l'Italia è stata chiamata ad assumere sempre maggiori

Prof. Alessandro Colombo, docente universitario.

1. European Union 2010, p. 8.

responsabilità politiche e militari, anche a costo di mettere sotto pressione la regola aurea di ogni politica estera: l'equilibrio tra impegni e risorse[2]. Mentre, infatti, i primi non hanno smesso di crescere dal 1990 a oggi, le seconde si sono scontrate con il permanere di forti vincoli di bilancio, difficilmente superabili in una fase di contenimento della spesa pubblica.
Oltre a rispondere ai mutamenti del contesto circostante, questa assunzione di impegni perpetua la costante storica a compensare l'insicurezza con il presenzialismo, fino a rischiare di rovesciare il rapporto realistico tra ruolo e rango – seguendo l'imperativo di esserci sempre e comunque, anche solo per dimostrare che 'l'Italia conta'. Come osservava Carlo Maria Santoro agli inizi degli anni Novanta, «il 'ruolo' dell'Italia... è stato spesso interpretato e quindi misurato dall'assetto politico interno, dai partiti e dal personale politico, più in termini di posto da occupare nella scala formale di potenza fra le Nazioni industrializzate europee o mondiali (rango) che non in termini di contenuti politici effettivi, ovvero nell'equazione costi-benefici per la reale salvaguardia degli interessi nazionali (ruolo)»[3].
A maggior ragione ciò avviene in una fase come l'attuale di ridefinizione della natura e dell'identità delle principali organizzazioni internazionali e, quindi, anche dei pesi e degli equilibri al loro interno. Nella grande partita per la nuova gerarchia del potere e del prestigio internazionale, l'interesse nazionale italiano tende a riorganizzarsi attorno all'obiettivo (realistico) di non 'perdere posizioni' o, almeno, di perderne il meno possibile: vuoi rispetto alla crescita di altri grandi attori (Cina, India, Brasile) destinati a guadagnare posizioni al suo posto, vuoi per il timore di marginalizzazione dal nucleo di comando delle istituzioni esistenti, Unione europea in testa.

DALLA MINACCIA AI RISCHI

Al cambiamento della natura degli interessi è corrisposto, in secondo luogo, un analogo cambiamento della natura delle minacce da cui tutelarsi. Al posto della minaccia organizzata, permanente e potenzialmente esistenziale dell'epoca bipolare, la tutela dell'interesse nazionale si è indirizzata verso un ventaglio di minacce e rischi «più eterogenei, meno visibili e meno prevedibili»[4] e, comunque, «di natura più ampia» rispetto al passato, tanto da abbracciare tutti quei processi, di lungo o breve periodo, politici o economici, internazionali o interni, suscettibili di «degradare la qualità della vita dei cittadini o di restringere in modo significativo lo spettro delle al-

2. Lippmann 1943; Gilpin 1989.
3. Santoro 1991, p. 73.
4. European Union 2003, p. 4.

ternative disponibili al governo dello Stato o a entità private non-governative (persone, gruppi, società) all'interno dello Stato»[5]: dal collasso di singoli Paesi o di intere sub-regioni ai movimenti incontrollati di grandi masse di popolazioni, dal terrorismo internazionale all'interruzione del flusso di risorse vitali, dalla proliferazione di armi di distruzione di massa al crimine transnazionale, dall'instabilità economica al cybercrime.

In questo allargamento c'è anche, almeno potenzialmente, un capovolgimento d'importanza: nella nuova condizione, il riarmo di un Paese rivierasco può costituire un fattore di pericolo meno grave del collasso delle sue Forze armate o delle sue Forze di polizia; l'emergere di una egemonia regionale può risultare meno pericolosa di un perdurante vuoto di potere; lo strumento militare, anche quando viene impiegato al di fuori del territorio nazionale, può assolvere funzioni più simili a quelle di polizia che a quelle di difesa; l'individuazione di una minaccia considerevole, ma geograficamente lontana, può richiedere meno attenzione dell'individuazione di rischi meno intensi ma geograficamente vicini.

Questa transizione dalla nozione di minaccia a quella di rischi – che l'Italia aveva già intravisto tra gli anni Settanta e Ottanta[6] – porta con sé almeno due fattori macroscopici di complicazione nella tutela dell'interesse nazionale. Il primo investe la dimensione temporale. A differenza ancora una volta della minaccia costante e riconoscibile del passato, il rischio è «un fenomeno conflittuale potenziale e latente, allo stato di semplice tensione che non ha ancora raggiunto la soglia della crisi internazionale ma che, in potenza, potrebbe trasformarsi in conflitto aperto, limitato e generale, sovente catalitico o accidentale»[7]. La sua specificità risiede, in altri termini, in una sorta di differimento temporale tra il momento in cui viene individuato e il momento (che potrebbe anche non venire mai) in cui si traduce in una minaccia definita. I suoi caratteri fondamentali sono, appunto, l'indeterminatezza e l'imprevedibilità. Mentre, dal momento dell'individuazione, la minaccia può essere misurata e confrontata con le proprie capacità, del rischio non si può mai dire se darà luogo (e in un luogo, a propria volta, spesso imprevedibile) a sfide più o meno impegnative oppure a nessuna sfida.

5. Ullmann 1993.

6. Sin dalla metà degli anni Settanta, la percezione di una crescente minaccia o rischio da Sud interessò tutti i principali cerchi della *foreign policy community* italiana. Il primo documento a fare cenno a rischi da Sud diversi da quelli sovietici fu il *Libro Bianco* della Marina del novembre 1973. Mentre, da allora, minacce «da Sud» o «a Sud» trovarono posto in tutti i principali documenti ufficiali della Difesa, benché in larga parte ricomprese nella logica del confronto Est-Ovest, il graduale riorientamento dell'attenzione non produsse che un limitato rischieramento del dispositivo militare (da Nord-Est verso Sud). La percezione dei rischi o delle minacce da Sud si estese sia alla comunità scientifica – con la pubblicazione di un numero crescente di studi e ricerche sull'area del Mediterraneo, spesso in relazione con il ministero della Difesa – sia al mondo diplomatico e politico. Su questo processo, cfr. Santoro 1996; Ilari 1996; Coralluzzo 2000.

7. Santoro 1996, p. 19.

A propria volta, questa indeterminatezza condiziona anche natura ed efficacia della risposta, e spiega l'apparente contraddizione fra la maggiore entità della minaccia rispetto ai rischi, e la più alta capacità di prevenire e gestire la prima rispetto ai secondi. Intanto, in opposizione alla semplicità della struttura bipolare del secondo Novecento e alla sua inclinazione a «restringere il campo delle opzioni... ai termini semplificati di un gioco a somma zero tra due giocatori», i rischi si presentano come plurali tanto nelle loro fonti quanto nei loro possibili destinatari. In secondo luogo, essi sono eterogenei e richiedono, pertanto, risposte ogni volta diverse – con la conseguenza che ciò che si dimostra una risorsa efficace contro certi rischi può dimostrarsi irrilevante o addirittura controproducente contro altri.
Infine, sono multidirezionali, ma in un senso completamente diverso rispetto all'onnipresenza della minaccia globale del passato. Mentre quest'ultima, pur potendo manifestarsi in diverse direzioni, conservava almeno il medesimo centro d'irradiazione e, in caso di risposta (diplomatica o, in ultima istanza, militare), il medesimo destinatario, i rischi si presentano di per sé come «locali», «regionali» o «sub-regionali», tanto da non potere essere più adeguatamente affrontati se non prima che investano direttamente il territorio nazionale.

LA NUOVA GEOPOLITICA DELL'INTERESSE NAZIONALE

A ciò si collega il terzo capitolo dell'adattamento: il mutamento radicale – nel senso letterale della parola – della collocazione e dell'orientamento spaziale dell'interesse nazionale italiano. Il motore di questo mutamento è una delle trasformazioni più profonde (sebbene, spesso, non adeguatamente riconosciute) dell'attuale contesto internazionale: il rovesciamento, in senso proprio epocale, dei rapporti tra dinamiche globali e regionali[8]. Per tutto l'ultimo secolo e, a maggior ragione, per tutto l'arco di vita dell'assetto internazionale bipolare, le prime avevano stabilmente prevalso sulle seconde. Non perché, anche allora, i vari contesti regionali non possedessero caratteristiche proprie e diverse da quelle degli altri, ma perché questa varietà era compensata e, nel momento critico, annullata dall'altissimo grado di penetrazione del sistema globale su quelli regionali, riassunta e portata all'estremo dall'interdipendenza militare, diplomatica e ideologica della Guerra fredda.

8. Su questo processo di riorganizzazione dello spazio, cfr. Buzan – Waever 2003; Colombo 2010; Lake – Morgan (eds.) 1997; Katzenstein 2005.

Nel contesto internazionale attuale, questo imponente meccanismo di subordinazione delle organizzazioni regionali a quella globale sembra essersi almeno provvisoriamente inceppato. Il riassorbimento della grande frattura comune tra liberalismo e socialismo ha lasciato spazio a una congerie di capitali simbolici e di mobilitazione variabili da una regione all'altra, efficaci all'interno della propria cultura di riferimento ma inutilizzabili o incomprensibili al di fuori di essa – come hanno confermato, negli ultimi anni, le rappresentazioni spesso affrettate che i media e gli stessi think tank occidentali hanno offerto delle vicende delle altre regioni.

La crisi dell'architettura multilaterale della convivenza internazionale ha incoraggiato la proliferazione di organizzazioni regionali altrettanto eterogenee, proprio mentre il collasso della formula di semplificazione del passato faceva risalire in superficie le enormi differenze, anche istituzionali, che si sono sempre celate dietro l'adozione superficiale della forma-Stato e dell'endiadi Stato-nazione. Soprattutto, con l'allentarsi delle interdipendenze diplomatiche e strategiche su scala globale, i diversi sistemi regionali hanno ripreso a divergere tra loro in termini di protagonisti, allineamenti e conflitti.

Questa trasformazione geopolitica ha un effetto imponente sull'interesse nazionale italiano. Intanto, la scomposizione regionale del sistema internazionale 'risucchia' sempre di più l'Italia nei contesti geografici di appartenenza, proprio mentre questi (i Balcani negli anni Novanta e la sponda Sud del Mediterraneo oggi) si rivelano tra gli spazi più precari dell'ambito internazionale. Questa liminarità rispetto al nuovo «arco dell'instabilità» postbipolare è un'altra delle grandi novità dell'ultimo trentennio. Mentre, nel contesto della Guerra fredda, l'Italia si trovava sul confine più periferico dell'Alleanza e, comunque, lontano dal teatro principale del confronto Est/Ovest, con il collasso del bipolarismo essa è stata sbalzata sul confine più esposto, sebbene non più nel senso della minaccia all'integrità territoriale ma in quello più sfuggente dei rischi politici ed economici legati alla variabilità del sistema. Con l'aggravante che, nel frattempo, la percezione italiana dei «rischi da Sud» si è ulteriormente ampliata per l'effetto dell'allargamento non soltanto della nozione di «rischio» ma della nozione stessa di «Sud». Se infatti, già nella fase declinante della Guerra fredda, questo poteva essere raffigurato come un «sistema» centrato – dal punto di vista dell'Italia – sul Mediterraneo, ma prolungato attraverso l'entroterra arabo del Maghreb verso il Sahel, attraverso il Canale di Suez e la penisola arabica verso il Corno d'Africa, e attraverso le interdipendenze politiche ed economiche del Medio Oriente verso il Golfo Persico[9], dopo il crollo della geografia bipolare, ha subìto una nuova, brusca espansione, confusamente riflessa in

9. Santoro 1996, p. 24.

espressioni quali «Mediterraneo Allargato» o «Grande Medio Oriente», ma concretamente alimentato dalla caduta dei limiti che separavano, nel contesto della Guerra fredda, la sponda Sud del Mediterraneo dalle regioni circostanti. Come se non bastasse, questo deterioramento del contesto geopolitico di riferimento avviene proprio mentre tendono a divergere gli interessi e le sensibilità dell'Italia rispetto a quelle dei nostri partner europei e atlantici[10].
Fino al 1989, grazie all'onnipresente minaccia sovietica, i confini di tutti gli alleati potevano essere considerati come il prolungamento dello stesso confine, la loro eterogeneità geografica contava meno del fatto che ovunque si giocasse la stessa partita, la loro diversità di interessi era trattenuta dall'identità dell'interesse più importante: contenere e, se possibile, sconfiggere l'Unione Sovietica. Nell'attuale ordine internazionale, al contrario, ciascun confine è tornato a essere orientato verso la propria area d'appartenenza per respingere e, specularmente, attrarre sempre nuovi e diversi rischi. La comunanza prospettica in virtù della quale gli alleati, sebbene affacciati su regioni diversissime tra loro, vi vedevano o pensavano di vedervi lo stesso paesaggio, ha ceduto il passo a una situazione nella quale non è più detto che tutti gli alleati abbiano le stesse priorità e percepiscano le stesse minacce e, quindi, non è più detto (anzi è altamente improbabile) che tutti abbiamo la stessa disponibilità ad affrontarli – come l'Italia ha già avuto modo di sperimentare nella lunga e irrisolta querelle con i propri partner sulla questione migratoria.

LA CRISI DELLA DIMENSIONE MULTILATERALE

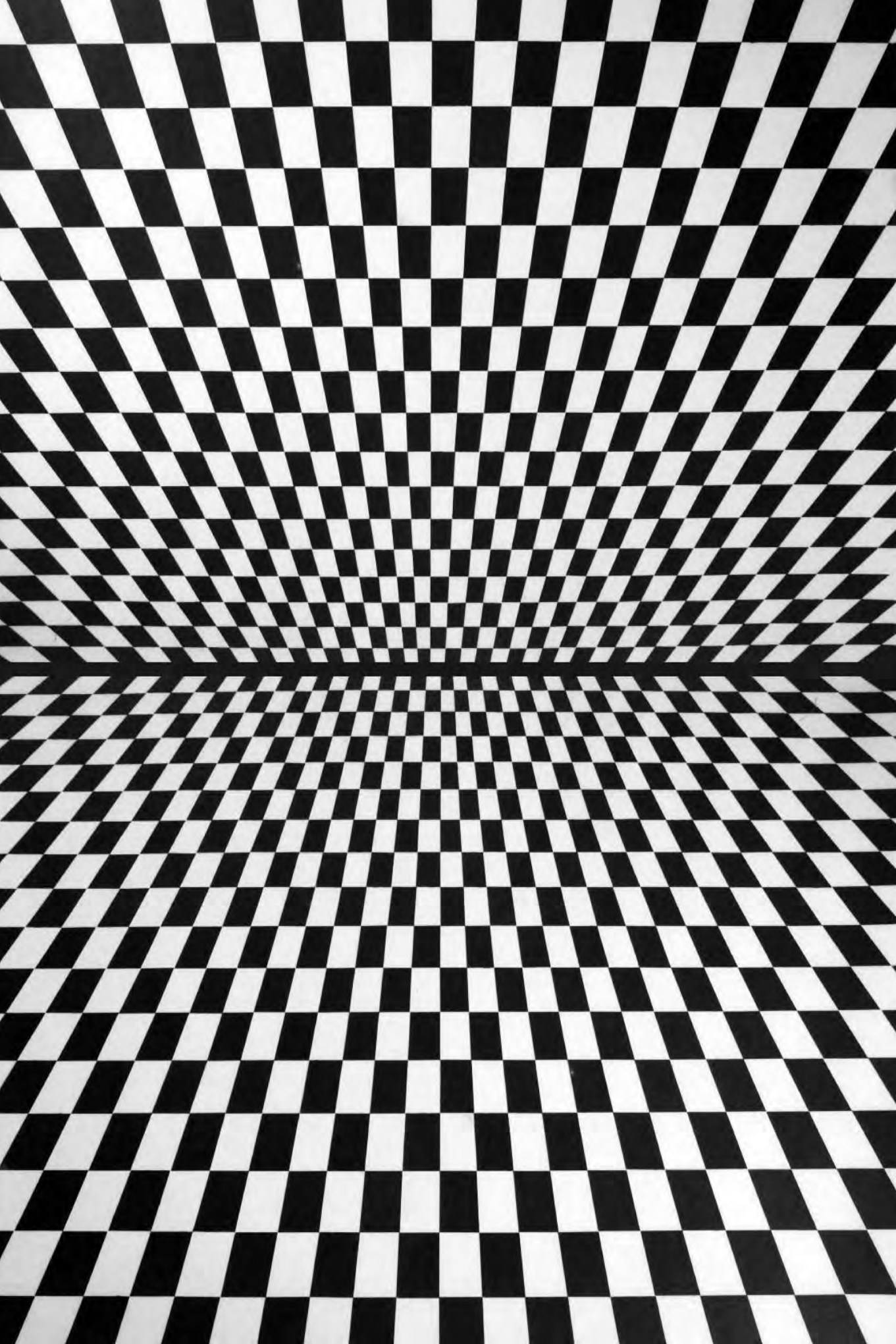
E qui arriviamo all'ultimo punto. Tutti i mutamenti che abbiamo visto fino adesso sarebbero già sufficienti a rendere complesso e, in una certa misura, problematico il processo di adattamento della tutela dell'interesse nazionale italiano al nuovo quadro internazionale. Ma a esacerbare i problemi contribuisce un mutamento più recente, che investe l'assetto tradizionalmente multilaterale della politica estera italiana degli ultimi settant'anni.
Dopo la Seconda guerra mondiale e per tutta la seconda metà del Novecento, la politica estera italiana ha beneficiato di una combinazione peculiare di bilateralismo e multilateralismo, dominata dall'appartenenza ai grandi contesti multilaterali (Comunità Europea, Alleanza Atlantica, Nazioni Unite, G7 ecc.) e corretta, se mai, dal ruolo solo residuale (e, comunque, subordinato) di rapporti bilaterali sviluppati prevalentemente nelle aree periferiche dell'assetto internazionale bipolare.

10. Colombo 2001, pp. 240-248.

Nel contesto internazionale attuale, al contrario, questa soluzione appare in misura crescente incerta, per effetto della perdita di coesione dell'Unione europea, prima di tutto, ma anche per i segnali sempre più insistenti di disimpegno da parte degli Stati Uniti. In questa nuova condizione, la tutela dell'interesse nazionale non richiederà più soltanto lo sviluppo di una più intensa attività bilaterale, per salvaguardare i propri interessi economici e di sicurezza e puntellare il proprio status. Più problematicamente, l'Italia dovrà prepararsi all'eventualità di dover affrontare da sola, o con un numero limitato di partner, crisi regionali alle quali la maggior parte dei tradizionali alleati non sarà interessata, in un tessuto meno prevedibile e più fluido di allineamenti e cooperazioni diplomatiche e militari.

BIBLIOGRAFIA

B. Buzan – O. Waever, *Regions and Powers. The Structure of International Security*, Cambridge UP, Cambridge 2003.
A. Colombo, *La lunga alleanza. La Nato tra consolidamento, supremazia e crisi*, Franco Angeli, Milano 2001.
A. Colombo, *La disunità del mondo. Dopo il secolo globale*, Feltrinelli, Milano 2010.
W. Coralluzzo, *La politica estera dell'Italia repubblicana* (1946-1992). *Modello di analisi e studio di casi*, Franco Angeli, Milano 2000.
European Union, EU *Security Strategy*, Bruxelles 2003.
European Union, EU *Internal Security Strategy*, Bruxelles 2010.
R. Gilpin, *Guerra e mutamento nella politica internazionale*, il Mulino, Bologna 1989.
V. Ilari, *La percezione del «rischio/minaccia da sud» in Italia*, in Santoro 1996.
P. Katzenstein, A *World of Regions. Asia and Europe in the American Imperium*, Cornell UP, Ithaca 2005.
D.A. Lake – P.M. Morgan (eds.), *Regional Orders: Building Security in a New World*, Pennsylvania State UP, University Park 1997.
W. Lippmann, US *Foreign Policy: Shield of the Republic*, Little Brown, Boston 1943.
C.M. Santoro, *La politica estera di una media potenza. L'Italia dall'Unità ad oggi*, il Mulino, Bologna 1991.
C.M. Santoro (a cura di), *Rischio da sud. Geopolitica delle crisi nel bacino mediterraneo*, Franco Angeli, Milano 1996.
R.H. Ullmann, *Redefinig Security*, «International Security» VIII (1993) 1.



LA TRASFORMAZIONE DELLE METODOLOGIE DI PREVISIONE STRATEGICA E DI COSTRUZIONE DI SCENARI

Luciano Bozzo

Quando nel 2007 il Parlamento italiano approvò la l. 124/2007 di riforma dell'intelligence le relazioni internazionali erano nel pieno della «turbolenza»[1] tuttora in atto e che, anzi, per molti versi da allora si è intensificata. Scatenata dalla fine repentina e inattesa della Guerra fredda, accentuata dagli attacchi dell'11 settembre e dalle loro conseguenze politiche e militari, in primo luogo in Medio Oriente, la condizione caotica delle relazioni internazionali fu poi confermata nel 2006-2008 dall'esplosione della crisi finanziaria. 'Condizione caotica' non sta qui per casuale, come nell'uso corrente, bensì implica, in senso matematico, l'imprevedibilità degli stati esatti del sistema considerato: «caos deterministico» o determinismo nascosto[2]. Gli attacchi terroristici – al pari delle presunte evidenze presentate tra la fine del 2002 e il febbraio 2003 al fine di dimostrare il possesso di armi di distruzione di massa da parte di Saddam Hussein – furono considerati in seguito altrettanti

Prof. Luciano Bozzo, docente universitario.

1. Sul concetto di turbolenza, mutuato dalla dinamica dei fluidi, cfr. Rosenau 1990, pp. 7-12.
2. Dalla teoria del caos o della complessità deriva un nuovo paradigma delle relazioni internazionali; cfr. Keating 2013; Kissane 2010, pp. 17-27; Ma 2007, pp. 57-78.

clamorosi errori del più importante sistema nazionale di raccolta e analisi di informazioni. Così negli Stati Uniti si riaccese il dibattito teorico e politico sui «fallimenti dell'intelligence»[3], che già negli anni Ottanta del secolo scorso aveva avuto a oggetto il loro possibile peggior esito: un attacco di sorpresa sul territorio americano[4]. Il rinnovato dibattito accompagnò e favorì diverse iniziative di riforma delle strutture per la raccolta e l'analisi dell'informazione create durante la Guerra fredda e rivelatesi inadatte ad affrontare le sfide generate dalla nuova e complessa realtà dello scenario globale.

La configurazione caotica assunta dalla fase post-bipolare e la necessità, in ragione di ciò, di ripensare l'intelligence nelle sue tre maggiori declinazioni – produzione di conoscenza a sostegno dei processi decisionali, organizzazione istituzionale e dimensione operativa dell'organizzazione – trovarono conferma nel 2011, grazie a un nuovo, macroscopico imprevisto: lo scoppio delle Primavere arabe. Collassato oltre vent'anni prima il sistema della Guerra fredda, semplificato e semplificante per l'analista, le minacce erano oramai divenute multiple, per provenienza e natura, spesso ambigue o «ibride», a volte poco visibili e, soprattutto nel dominio cibernetico, difficilmente identificabili. Che genere di sfida pone questa realtà nuova all'analisi strategica e previsionale d'intelligence?

Le relazioni internazionali contemporanee sono caratterizzate da processi paradossalmente contigui di globalizzazione / integrazione, da un lato, e frammentazione dall'altro; cui si aggiungono rivoluzione tecnologica, crisi d'identità e di autorità, l'emergere di nuove potenze, di attori non statuali e l'*individual empowerment*. La politica internazionale è volatile, incerta, complessa, ambigua[5] e la trasformazione in atto risulta talmente rapida e profonda da configurarsi più come «metamorfosi»[6], che quale mutamento tradizionalmente inteso. Aumenta così l'imprevedibilità di accadimenti che pure determinano salti evolutivi del sistema. Sono i «cigni neri»[7], eventi altamente improbabili e d'estremo impatto che, giunti imprevisti, vengono normalizzati in autoriferimento, ex post, dai loro interpreti (predicibilità retrospettiva): lo scoppio della Prima guerra mondiale, la rivoluzione iraniana, l'avvento di internet, l'11 settembre. «Unknown unknowns», espressione resa nota dall'ex segretario alla Difesa Donald Rumsfeld, «game changers» o «wild cards» sono altrettanti sinonimi dei cigni neri, che ne enfatizzano la rarità. All'analista, consapevole che l'inaudito e l'inatteso accadono, resta come unica paradossale certezza l'incertezza; che, relativa a eventi straordinari,

3. Bracken et al. 2008; Dahl 2013; Jervis 2010; Neri – Pasquazzi 2015, pp. 283 ss.
4. Tra altri, cfr. Handel 1984, pp. 229-281; Idem 1985, pp. 239-269; Levite 1987.
5. Giancotti – Shaharabani 2008, p. 15.
6. Beck 2017, p. 8.
7. Taleb 2007.

cioè senza precedenti, al contrario del rischio non è quantificabile tramite assegnazione di una probabilità di accadimento agli eventi considerati, ovvero sulla base della loro frequenza calcolata. A fronte di minacce simili l'esito dell'analisi strategica e previsionale deve farsi flessibile, creativo, pensando reazioni rapide e multiple a sfide impreviste. L'unica risposta credibile agli «sconosciuti non-noti» è sviluppare sufficiente «resilienza» rispetto alle possibili conseguenze di quelli di segno negativo, sfruttando invece quelli di segno opposto. A questo fine è necessaria la crescita di una cultura istituzionale che riconosca centralità ai temi dell'interesse e della sicurezza nazionale, nelle sue nuove e diverse declinazioni, perciò al ruolo e alle esigenze specifiche della funzione d'intelligence. Considerata in quest'ottica, la riforma del 2007 rappresenta un indubbio e rilevante salto di qualità.

Per decenni il sistema politico italiano aveva riprodotto in maniera pressoché speculare quello internazionale bipolare. Non fu dunque tanto per influenza del dibattito sui fallimenti dell'intelligence, quanto grazie al superamento del confronto tra i due blocchi, dentro e fuori il Paese, che vennero a crearsi le condizioni politiche finalmente favorevoli alla riforma degli apparati d'intelligence attesa dagli anni Ottanta. Il necessario processo legislativo si trovò infatti libero dai vincoli e timori contrapposti che ne avevano ostacolato il positivo sviluppo ancora nel decennio seguente la fine della Guerra fredda.

Al capo I della legge del 3 agosto 2007 n. 124, che delinea la struttura del Sistema di informazione per la sicurezza della Repubblica, l'art. 4, comma 3, lett. c, recita che il Dipartimento delle informazioni per la sicurezza (Dis): «raccoglie le informazioni, le analisi e i rapporti provenienti dai Servizi di informazione per la sicurezza [...] elabora *analisi strategiche* o relative a particolari situazioni; formula valutazioni e *previsioni*, sulla scorta dei contributi analitici settoriali dell'Aise e dell'Aisi»; aggiungendo infine, sub d: «elabora *analisi globali*» [*enfasi nostre*]. Nel nuovo sistema d'intelligence «a tridente» il Legislatore attribuiva dunque al Dis non solo funzioni tradizionali di coordinamento, collezione ultima e analisi delle informazioni, bensì compiti più ambiziosi e innovativi: l'elaborazione di analisi strategiche, previsionali e globali.

L'attenzione al futuro, componente essenziale delle interazioni conflittuali di vario genere e livello, violente e non, è insita nella natura stessa dell'analisi strategica e la distingue da quelle definite di primo impatto e breve periodo. Il collegamento codificato dalla legge di riforma tra analisi strategica e attività previsionale è perciò centrato. Al fine di «porre a disposizione di chi deve decidere e agire [...] le conoscenze necessarie all'esercizio delle massime responsabilità politiche»[8] alla prima è chiesto, infatti, di superare l'urgenza dell'immediato, che è inevitabilmente all'attenzione continua del decisore po-

8. Antiseri – Soi 2013, p. 96.

litico, per proiettarsi verso il futuro. Nelle relazioni internazionali contemporanee la «predizione» è impossibile, ammesso lo fosse in sistemi passati assai più semplici e stabili. Accettare un grado maggiore o minore d'incertezza è perciò inevitabile. È però possibile guardare agli esiti dell'evoluzione di situazioni, fenomeni o minacce specifiche (*horizon scanning*), identificando *drivers* e trend del mutamento, segnali deboli, minacce, rischi e opportunità[9]. Questo al fine di sviluppare scenari, ovvero futuri alternativi, tentando di stabilire cosa è possibile, plausibile o probabile; per poi valutare se, e quanto, i mezzi di varia natura disponibili all'attore di riferimento siano adeguati rispetto a quei possibili scenari e individuare le vulnerabilità che eventualmente minerebbero la capacità di resistenza dell'attore stesso[10]. In sintesi, oggi «le previsioni [...] diventano probabilistiche [...] infatti i fenomeni sono governati da leggi di evoluzione non lineari, condizionate – oltretutto – dalla forte dipendenza dalle condizioni iniziali»[11]. L'analisi strategica e la costruzione di scenari concorrono all'elaborazione delle «analisi globali» cui fa riferimento la legge del 2007, che attengono a contesti ampi e fenomeni particolarmente complessi e, perciò, richiedono competenze di ricerca specifiche e sofisticate. L'approccio non può che essere sistematico e insieme intuitivo, multidimensionale e multidisciplinare[12], poiché l'oggetto di studio è costituito appunto da sistemi complessi adattivi, caratterizzati da reti di relazioni non-lineari e circuiti di retroazione. L'ottica sistemica e la teoria cibernetica, nei suoi più recenti sviluppi, paiono gli strumenti che meglio consentono di trattare gli attori e l'insieme delle loro molteplici relazioni e interdipendenze, in una prospettiva di ampia portata e lungo periodo.

Il disposto dell'articolo 4 della legge di riforma individua dunque, con chiarezza, strumenti e modi atti a soddisfare il «fabbisogno informativo» del decisore politico: conoscenze strategiche-previsionali che non siano frutto dell'organizzazione in qualche modo strutturata d'informazioni e pensiero, bensì di procedure sistematiche che, trattando l'informazione nel rispetto di principi e regole predefiniti, consentano di produrre risultati con valore stimato. Ciò significa, ad esempio, che il «brain storming» non è una metodologia d'analisi in senso proprio; mentre lo sono il modello *Swot*, quello *Multi-Attribute Utility*, l'*Analysis of Competing Hypothesis*, l'*Analytic Hierarchy Process* e l'*Analytic Network Process*, varianti del *Multi-Criteria Decision Making*, la *Social Network Analysis* e le analisi basate sulla statistica bayesiana. Negli studi d'intelligence tradizionali, refrattari al concetto stesso di teoria, ritenuta

9. Walton 2017, p. 41.
10. Ghez – Treverton 2017, pp. 1-18.
11. Gori in Caligiuri 2016.
12. Antiseri – Soi 2013, p. 103.

qualcosa di astratto se non astruso, trovavano largo spazio il metodo intuitivo e la logica situazionale. L'analista accumulava una gran quantità di informazioni, spesso nell'arco di una vita intera, su un dato tema, area geografica o problema e all'occorrenza, sfruttando la conoscenza approfondita dell'oggetto di studio, produceva in base alle sue riflessioni e intuizioni il risultato richiesto. La logica era situazionale: focalizzare il caso singolo, individuando e studiando il maggior numero possibile di variabili che ne definiscono la specificità; col rischio però che l'analisi fosse inficiata da un insieme di pregiudizi di varia natura – cognitivi, organizzativi, sistemici[13] – del resto necessari per trattare la complessità del reale tramite strategie di semplificazione.
La rivoluzione tecnologica, con l'affermazione inattesa e impressionante di internet dopo il 1995, ha peggiorato lo stato delle cose, dando il via a un nuovo modo di produzione della conoscenza, globale e totale, che a sua volta «ha ridefinito le metodologie e i processi di fruizione dell'informazione»[14]. Il facile e rapido accesso a un'enorme e sempre crescente massa di dati, anche grazie al contributo del web 2.0 e di Internet of Things, enfatizza l'Open Source Intelligence[15] e tuttavia inevitabilmente aumenta il 'sovraccarico' che schiaccia l'analista, già punto critico del vecchio ciclo di intelligence, il quale non è in grado di leggere, vedere, ascoltare tutto quanto può risultare rilevante rispetto all'oggetto di studio. Per far fronte al problema, probabilmente, non sarà sufficiente lo sviluppo di nuovi metodi e tecniche atti a raccogliere e trattare questo materiale nei B*ig Data*: il dominio degli algoritmi. Oltre a far conto sulla potenza delle nuove macchine per l'analisi, gli H*igh* P*erformance* C*omputers* e gli oramai prossimi computer quantici, occorrerà coniugare la capacità di calcolo con cultura e analisi strutturata, metodo scientifico e creatività, intuizione, intelligenza ed esperienza sul campo. Ma è realistico, per una struttura d'intelligence nazionale come quella italiana, affrontare con speranza di successo le sfide poste da un sistema di relazioni internazionali altamente complesso, dall'evoluzione rapida, repentina e all'apparenza del tutto imprevedibile?
Come rispondere alla rivoluzione dei Big Data e alle altre, di natura tecnologica, che seguono: sviluppi di robotica, optogenetica, nanotecnologie, integrazione tra uomo e macchina, sistema neurale e rete, introduzione dell'intelligenza artificiale e via discorrendo? In che maniera affrontare la metamorfosi in atto del sistema globale, in cui aumenta e accelera la competizione tra gli attori per il conseguimento di vantaggi decisivi nel campo economico e delle tecnologie di punta?

13. Cfr. Heuer 1999.
14. Teti 2012, p. 21.
15. Teti 2015, pp. 49-53.

Sulla carta la risposta a queste domande è semplice: incrementate risorse umane e finanziarie, aumento del numero degli analisti, maggiore capacità di raccolta delle informazioni, più attenta cura delle condizioni e dell'ambiente di lavoro, analisti meglio preparati, perciò nuovi criteri di selezione e formazione del personale nonché, naturalmente, più sofisticate e idonee metodologie d'analisi. Se il conseguimento dei primi tra questi obbiettivi sembra assai poco realistico è sugli ultimi che invece pare possibile concentrare attenzione e risorse scarse. In primis occorre sviluppare teorie e metodologie in grado di trattare la complessità, riducendola, senza che ciò si traduca in una perdita d'informazione tale da inficiare la conoscenza prodotta ed efficacemente spendibile per soddisfare le esigenze dei responsabili decisionali. Per raggiungere l'obiettivo è tuttavia necessario creare e diffondere la cultura dell'intelligence e aumentare il bacino della comunità nazionale che se ne occupa a vario titolo, tramite l'istituzione di un'università ad hoc, sulla scorta di quanto fatto negli Stati Uniti con la N*ational* I*ntelligence* U*niversity*, applicando il sistema delle «revolving doors» con la comunità accademica e della ricerca e favorendo la creazione di Corsi di studio universitari del genere, ad esempio, di quello attivo presso la James Madison University, in Virginia[16].

Certo, l'aumento esponenziale della potenza di calcolo, applicato all'enorme quantità di dati oggi disponibile, consente di collegare, anche secondo relazioni non lineari, variabili le più diverse.

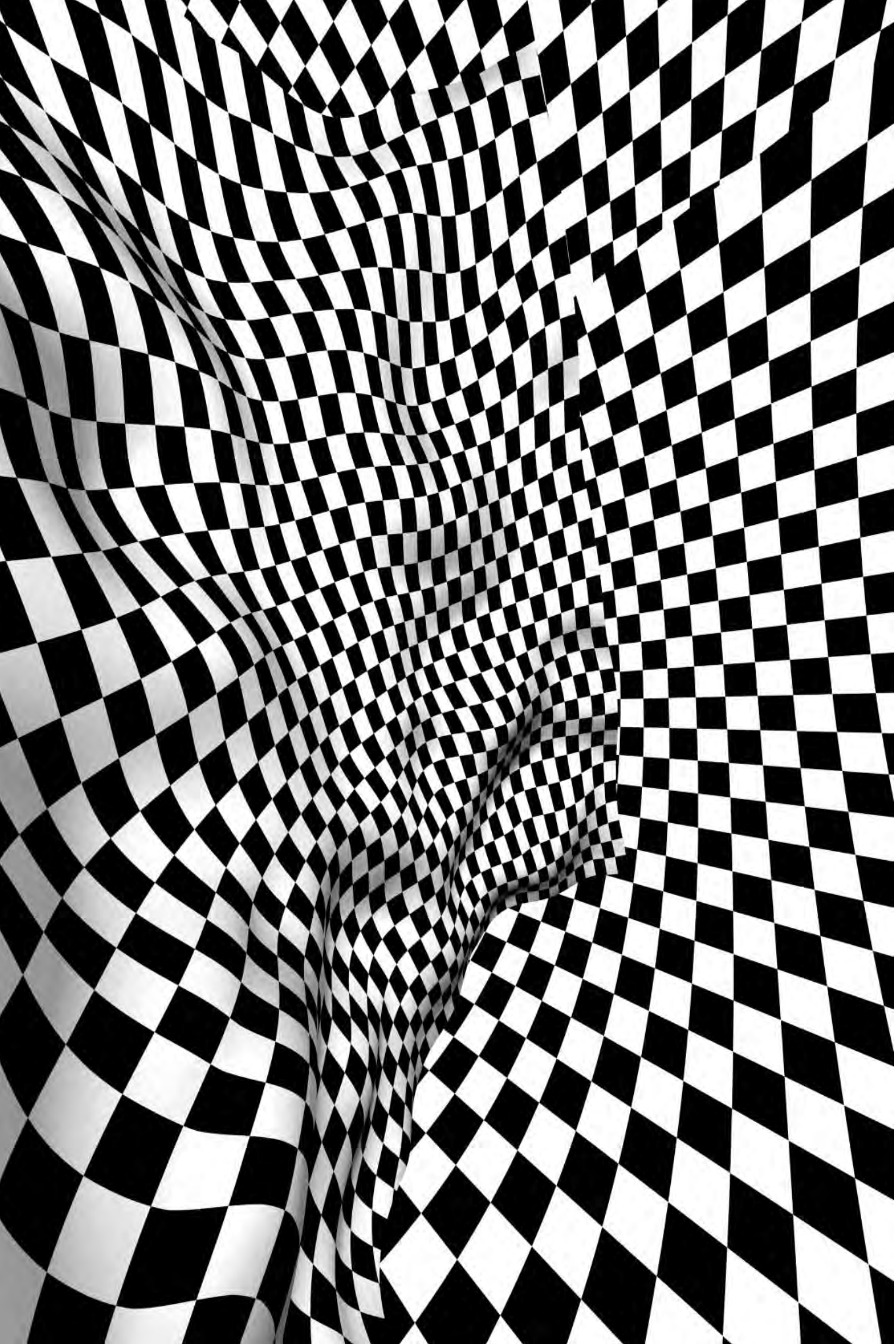
Il rapporto di causalità lascia così il passo alla correlazione. Non si tratta più «di scoprire il *perché* di un evento osservato [...] ma di predire *che cosa* avverrà incrociando migliaia di dati e di qualsiasi tipo (immagini, video, testi, audio)» [*enfasi nell'originale*][17]. L'analisi d'intelligence e, in particolare, la componente previsionale, è allora destinata a tradursi o ridursi all'elaborazione di algoritmi efficaci rispetto agli scopi prefissati? In realtà, proprio la mole dei dati destrutturati fa sì che per ottenere l'informazione sia necessario porre la domanda giusta: «l'informazione non esiste fintantoché non viene formulata la domanda [...] la risposta è *creata* dalla domanda [*enfasi nell'originale*], la quale ora viene ad assumere il ruolo più importante nella ricerca»[18].

Quest'affermazione suggestiva, che richiama la fisica dei quanti, è il cigno nero dell'analista: la sfida e l'opportunità che gli è offerta.

16. Sul programma della Jmu, cfr. Walton 2017.
17. Guida 2016, p. 299.
18. Marzocca in Guida 2016, p. 305.

BIBLIOGRAFIA

D. Antiseri – A. Soi, *Intelligence e metodo scientifico*, Rubbettino, Soveria Mannelli 2013.
U. Beck, *The Metamorphosis of the World*, John Wiley & Sons, Hoboken 2016 (trad. it. *La metamorfosi del mondo*, Laterza, Bari-Roma 2017).
P. Bracken et al., *Managing Strategic Surprise*, Cambridge University Press, Cambridge 2008.
M. Caligiuri (a cura di), *Intelligence e scienze umane*, Rubbettino, Soveria Mannelli 2016.
E.J. Dahl, *Intelligence and Surprise Attack*, Georgetown University Press, Washington DC 2013.
G. Ghez – G.F. Treverton, *Making Strategic Analysis Matter*, in Juneau 2017, pp. 1-18.
F. Giancotti – Y. Shaharabani, *Leadership agile nella complessità*, Guerini e Associati, Milano 2008.
U. Gori, in Caligiuri (a cura di) 2016, pp. 65-72.
E. Guida, *Intelligence*, Ledizioni, Milano 2016.
M.I. Handel, *Intelligence and the Problem of Strategic Surprise*, «The Journal of Strategic Studies» VII (1984) 3.
M.I. Handel, *Strategic Surprise*, in A.C. Maurer et al. (eds.), *Intelligence: Policy and Process*, Westview, Boulder 1985.
R.J. Heuer Jr., *Psychology of Intelligence Analysis*, Central Intelligence Agency – Center for the Study of Intelligence, McLean 1999.
R. Jervis, *Why Intelligence Fails*, Cornell University Press, Ithaca 2010.
T. Juneau (ed.), *Strategic Analysis in Support of International Policy Making*, Rowman & Littlefield, Lanham 2017.
J. Keating, *Can Chaos Theory Teach Us Anything about International Relations?*, «Foreign Policy» (23 maggio 2013): <http://foreignpolicy.com/2013/05/23/can-chaos-theory-teach-us-anything-about-international-relations/> [10-11-2017].
D. Kissane, *Mapping International Chaos*, «Contemporary Issues» III (2010) 1.
A. Levite, *Intelligence and Strategic Surprise*, Columbia University Press, New York 1987.
S.Y. Ma, *Political Science at the Edge of Chaos?*, «International Political Science Review» XXVIII (2007) 1.
F. Marzocca, *Big Data*, <http://www.fabiomarzocca.com/blog/2014/10 /04/big-data-porre-le-giuste-domande> [10-11-2017].
C. Neri – S. Pasquazzi, *Intelligence Failures. Teorie, casi empirici e fattori correttivi*, in U. Gori – L. Martino (a cura di), *Intelligence e interesse nazionale*, Aracne, Ariccia 2015, pp. 277-318.
J.N. Rosenau, *Turbulence in World Politics*, Princeton University Press, Princeton 1990.
N.N. Taleb, *The Black Swan*, Random House, New York 2007 (trad. it. *Il cigno nero*, il Saggiatore, Milano 2014).
A. Teti, *Il potere delle informazioni. Comunicazione globale, cyberspazio, intelligence della conoscenza*, Il Sole 24 ore, Milano 2012.
A. Teti, *Open Source Intelligence & Cyberspace*, Rubbettino, Soveria Mannelli 2015.
T. Walton, *How Intelligence Analysis Education Tries to Improve Strategic Analysis*, in Juneau 2017, pp. 37-56.



IL RITORNO DELLA GEOGRAFIA

NELLA PROSPETTIVA DELLA SICUREZZA NAZIONALE

Lida Viganoni

Parlare di ritorno della Geografia potrebbe indurre a pensare a una sua scomparsa. Ma la Geografia non è mai scomparsa, al contrario. Il riferimento al 'ritorno' si applica soprattutto alla rilevanza che nell'epoca contemporanea va assumendo il territorio e la sua conoscenza e, con essi, quella della sua più pregnante rappresentazione che è la carta geografica. E, nella chiave del tema della sicurezza nazionale e di quello più generale della politica estera del nostro Paese, questo 'ritorno' è particolarmente rilevante per la Geografia politica, ambito entro il quale il tema s'inscrive in maniera più evidente. Ed è un 'ritorno' che dà il senso del superamento della lunga stagione di crisi vissuta dalla Geografia politica e del cambiamento del suo stesso significato nel corso del tempo.

In effetti, dalla chiusura del Secondo conflitto mondiale sulla Geografia politica cade il silenzio. Incombe sulla disciplina lo spettro di un passato poco edificante: quello di un sapere strategico che, dopo la sua nascita nel 1897 a opera del geografo tedesco Friedrich Ratzel in occasione della pubblicazione del libro *Politische Geographie*, si era posto al servizio delle politiche espansioniste delle grandi potenze del tempo. La stagione della Geografia politica classica, destinata a protrarsi fino al 1945, marca la disciplina con una forte inclinazione verso il determinismo geografico, che attribuisce alle caratteristiche fisiche e al posizionamento di uno Stato la capacità di condizionare il suo sviluppo e la sua espansione. Una lunga storia[1] che ha visto la disciplina fortemente

Prof.ssa Lida Viganoni, rettore emerito dell'Università L'Orientale di Napoli.

1. Sull'evoluzione della Geografia politica, tra i tanti manuali, si segnalano Agnew 2003 e Lizza 2001.

influenzata dal clima culturale tra fine Ottocento e prima parte del Novecento, sponda all'affermazione della supremazia euro-occidentale, alla politica espansionistica sfociata nelle grandi guerre di conquista, nella contrapposizione tra divisione continentale tedesca e quella delle potenze marittime (inglese e statunitense)[2]. È per tutte queste ragioni, come ricorda John Agnew, che «i geografi politici appartenenti alle potenze che vinsero la guerra, come per esempio Isaiah Bowman, rinnegarono la geopolitica...», fatto che «li fece regredire a tecnici specializzati in questioni di confini territoriali anziché promuoverli a partecipanti critici degli eventi fondamentali del loro tempo».
E così la Geografia politica cadde «nell'oscurità politica e nell'irrilevanza intellettuale»[3].
Negli anni Sessanta del Novecento, sulla scia della critica mossa da alcuni geografi anglosassoni alla ormai cosiddetta 'geografia classica' cui si imputa di coltivare un tipo di analisi che guarda al particolare, irrompe l'analisi spaziale. Il territorio lascia il posto allo spazio, i luoghi scompaiono per il dominio che assumono le teorie e i modelli matematici, in quella che è stata definita la rivoluzione quantitativa della geografia[4]. Questa geografia rinuncia del tutto all'interpretazione della realtà territoriale; individua piuttosto regole utili da applicare alla stessa per il raggiungimento di determinati obiettivi. Siamo nel campo della geografia quantitativa, che spazza via rapidamente il territorio, nelle sue componenti ambientali e umane che, nel loro reciproco incontro, erano state peraltro la base della nascita, in Francia, della corrente del possibilismo geografico[5] e della geografia regionale[6]. E, in questo contesto, anche la Geografia politica che aveva perso peso perché non era riuscita ad affrontare la perdita della propria base fisico-deterministica[7], riprende un certo vigore[8], con analisi più strettamente riconducibili al marxismo[9], che trasmettono una visione dello spazio entro il quale i processi politici ed economici si integrano.
Dagli anni Settanta i non pochi problemi che da tempo vanno innescandosi nei diversi contesti territoriali mondiali vengono prepotentemente alla ribalta. Inquinamento ambientale, esaurimento delle risorse non rinnovabili, problemi generati dalla concentrazione industriale e dalla crescita urbana, emergenze economiche, sociali e politiche che finiscono per creare situazioni conflittuali con spiccate radici territoriali: dalla guerra del Vietnam alla decolonizzazione e ai temi del sottosviluppo, dalle rivolte razziali alla protesta degli studenti e ai conflitti urbani[10]. Il territorio torna alla ribalta e con esso il sapere

2. Mackinder 1904, pp. 421-437; Spykman 1944, pp. 387-391. In Italia, in quest'epoca, la Geografia politica ha i suoi più autorevoli esponenti in Giorgio Roletto ed Ernesto Massi, che nel 1939 avevano dato vita alla rivista «Geopolitica».
3. Agnew 2003, p. 107.
4. Bunge 1962; Gould 1969.
5. Febvre 1922.
6. Vidal de la Blache 1903.
7. Agnew 2003, p. 123.
8. Cox – Reynolds 1974.
9. Harvey 2010.
10. Coppola 1986.

geografico e la centralità riconosciuta alla ricerca sul terreno, campo privilegiato della geografia, in stretta connessione con il corpo sociale. Perché, come scrive Pierre George, «il documento geografico in sé è il terreno»[11]. Non manca un risvolto anche molto ideologico, che sfocia in una critica alla vecchia geografia, anche politica, troppo legata alla guerra tra Stati e alla scarsa attenzione per le componenti sociali emarginate[12].

Dalla fine degli anni Settanta in poi i cambiamenti dell'assetto mondiale accelerano progressivamente. Entrano in gioco la globalizzazione e la terziarizzazione dell'economia, il ruolo dominante delle comunicazioni, l'affermarsi progressivo del paradigma della sostenibilità, la riconfigurazione degli assetti urbani. Cambiamenti che hanno risvolti non irrilevanti, che mettono in crisi il paradigma dello strutturalismo e l'oggettività della conoscenza, a vantaggio del ruolo del soggetto nella dinamica della conoscenza.

Così, negli anni Ottanta, il nuovo clima culturale della postmodernità (*cultural turn*) coinvolge anche la geografia, a partire dall'attenzione per i paesaggi culturali ed economici, per il ruolo della politica e i discorsi femministi e postcoloniali, fino alla questione ambientale intesa come problema culturale. In questa svolta, non mancheranno voci autorevoli, come quella di David Harvey[13]. Di certo, la svolta culturale frammenta gli interessi del sapere geografico in tanti filoni difficilmente sintetizzabili che comunque vedono il ritorno di due parole chiave, ambiente e locale, e il dominio di una scala di riferimento sempre più micro, il quartiere, il gruppo di minoranza e così via. In ogni caso, bisogna sottolineare che questo approccio consente di assicurare una rinnovata centralità allo studio della relazione tra la società e lo spazio e, soprattutto in ambito anglosassone, questo assicura una grande importanza al sapere geografico. Né va dimenticato che la fine della Guerra fredda ha decretato la «fine della geografia»[14]: la caduta del muro di Berlino e la fine del bipolarismo hanno prefigurato l'avvento di un mondo senza frontiere, interconnesso, senza territorio. È un evento che «ha eroso la sovranità dello Stato, offuscato il confine tra 'interno' ed 'esterno' relativo allo Stato e prodotto una società globale comune che non fronteggia i pericoli che emanano da un singolo Stato o da una singola fonte ma semmai quelli di un'opposizione al capitalismo moderno degli anni post Guerra fredda (nelle forme di religioni ataviche e di movimenti culturali)»[15].

Si fa strada il mondo dei «flussi»[16] che sostituisce il mondo dei territori che nell'epoca della Guerra fredda, pur con molte contraddizioni, aveva garantito l'ordine mondiale.

Una visione, quest'ultima, che pur se con modalità differenti si ripropone oggi in un percorso che sostituisce la struttura territoriale con una relazionale, caratterizzata dalla 'connettività', decostruendo così l'idea che la geografia «sia un destino»[17].

11. George 1974.
12. George et al. 1964; Lacoste 1976.
13. Harvey 2010.
14. O'brien 1990, pp. 2-5.
15. Agnew 2003, p. 158.
16. Gottmann 1952.
17. Khanna 2016.

Da questo quadro generale non può non desumersi che la geografia c'è sempre stata e che se oggi si parla di 'ritorno' è perché le problematiche con le quali ci confrontiamo sono assai più complesse e per essere decodificate richiedono un approccio che dalle astrazioni del passato passi alla concretezza della realtà. In questa chiave di lettura, il 'ritorno' della geografia indica soprattutto una rinnovata attenzione al sapere territoriale inteso anche nella sua articolazione in scale geografiche e nel recupero di alcune categorie fondamentali che per un certo lasso di tempo erano state abbandonate.

Un tratto distintivo della geografia e del suo ritorno è il rilievo che torna a darsi alla conoscenza territoriale, in quanto la geografia è stata e resta scienza territoriale, pienamente inscritta nell'ambito delle scienze sociali perché è il territorio stesso prodotto del sociale. Per quanto oggetto di non poche critiche, è Robert Kaplan[18] a riportare il territorio al centro dell'attenzione, ad affermare che esso non è stato annullato dalle tecnologie della comunicazione, che abitiamo nei luoghi fisici, la cui natura politica dipende ancora dalla loro posizione geografica, che ci serve a capire dove siamo e cosa può accadere.

Ritorna la geografia per sfatare il mito del mondo ormai immateriale, per recuperare un sapere da sempre strategico, perché la sua utilità è anche strettamente pratica. Molti aspetti della nostra vita ne hanno bisogno. L'amministrazione, la politica, la diplomazia, lo sviluppo economico, la comprensione tra popoli, la gestione dell'ambiente naturale, la pianificazione del territorio hanno bisogno di buone conoscenze geografiche. E proprio la mancanza di conoscenza geografica e una sua sottovalutazione hanno spesso determinato molti errori in questi campi. Nell'analisi di una porzione di spazio, riuscire a cogliere le forme e i contenuti e «il nesso tra i processi attivati da questi contenuti e le loro forme materiali non è un esercizio culturale fine a sé stesso. È, al contrario, un'operazione di grande rilievo strategico: significa potersi muovere, poter tamponare i punti deboli di un territorio, poterne identificare i nodi essenziali, poter valutare i potenziali umani… significa sapersi orientare nel senso più lato, con consapevolezza»[19]. Il sapere territoriale è, dunque, un'esigenza per chi deve esercitare il controllo, ma lo è anche, nella società contemporanea, per le popolazioni che vivono sui territori e che da tempo guardano criticamente alle decisioni che lo concernono.

Nel corso del tempo la disciplina è andata articolandosi in molte branche differenziate: la Geografia politica, economica, urbana, culturale, sociale, dello sviluppo ecc. Anche gli approcci teorici e le metodologie si sono, come si è visto, diversificati. Quel che però oggi accomuna le tante anime della geografia è senza dubbio il valore del territorio. E questa conoscenza specifica rappresenta un grande serbatoio di saperi per la sicurezza nazionale: quali che siano i problemi su cui la politica della sicurezza nazionale porta l'attenzione, la conoscenza geografica territoriale fornisce un contributo imprescindibile, fortemente potenziato anche dalla capacità della disciplina a muoversi attraverso le analisi transcalari, sempre tra loro interconnesse, dalla scala globale a quella locale. La globalizzazione ha rafforzato il nesso tra conoscenza territoriale e sicurezza. Nel mondo aperto e intercon-

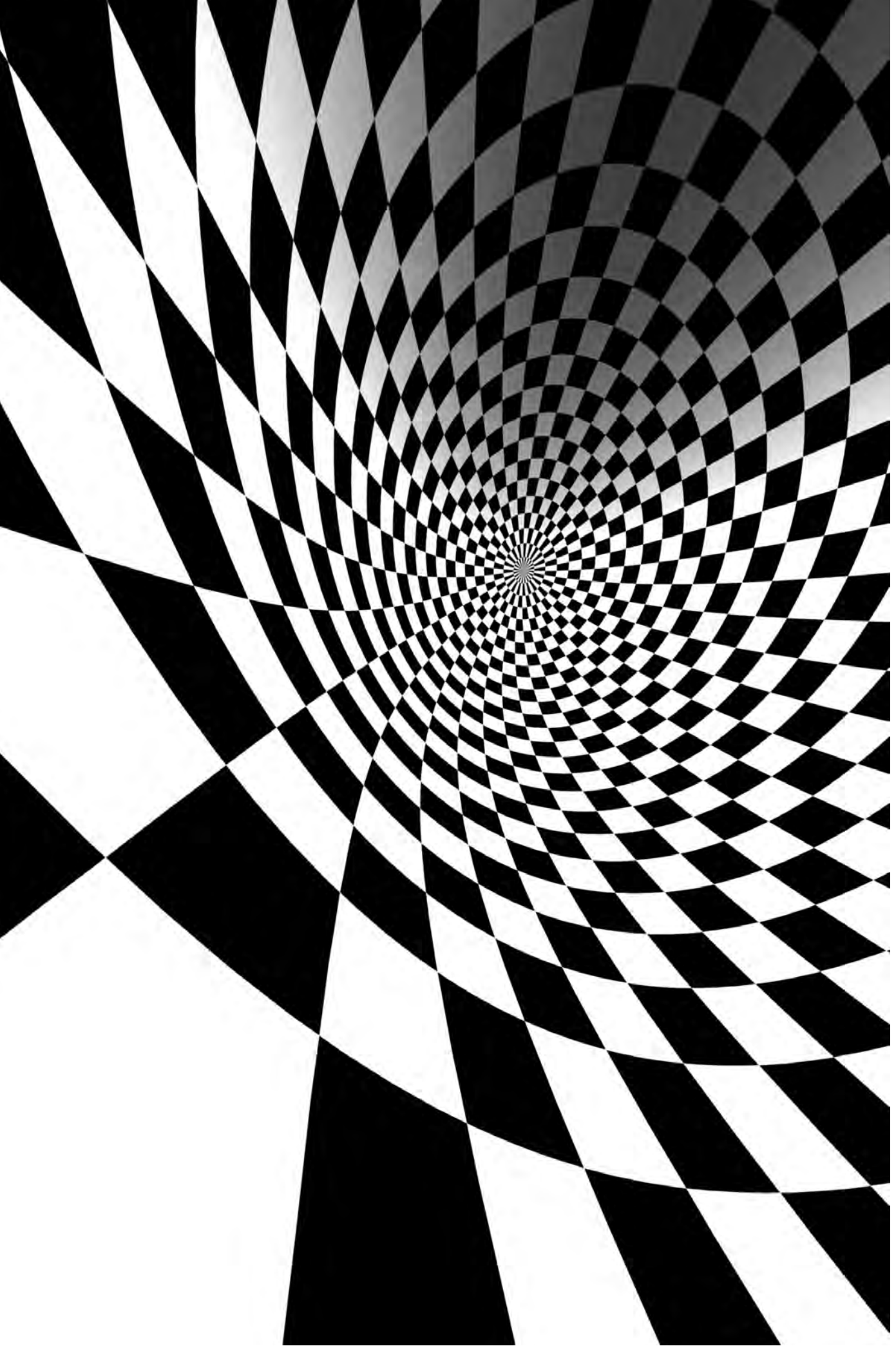
18. Kaplan 2012.
19. Coppola 1986, pp. 21-22.

nesso ciò che avviene all'esterno incide fortemente sugli assetti ed equilibri interni. Temi e questioni, anche d'interesse pubblico e di grande rilievo per la sicurezza nazionale, sono oggi più numerosi rispetto al passato (terrorismo globale, fenomeni di scomposizione territoriale, flussi migratori, indipendentismi, confini che si moltiplicano, conflitti ambientali, etnici ecc.). Si tratta di problematiche che si dipanano su più scale territoriali, perché i processi operano trasversalmente su più livelli e si condizionano reciprocamente. Tra la scala globale, nazionale, regionale e locale esistono connessioni e interdipendenze che possono essere comprese solo operando un salto di scala. Un'operazione, questa, che deve fare spesso riferimento a un approccio diacronico, alla ricerca delle cause che hanno influenzato e possono spiegare il presente; perché molti dei problemi nei quali oggi ci dibattiamo sono riconducibili a periodi precedenti che continuano a esercitare la loro influenza fino a oggi. E con riferimento all'analisi transcalare non può non considerarsi un'altra categoria prettamente geografica, quella cioè della posizione che, per il nostro Paese, rappresenta per molti aspetti un cardine di riferimento prioritario nella chiave della sicurezza nazionale e della politica estera.

Lo dimostrano le vicende passate e quelle più recenti; il Paese è ormai diventato la principale porta di accesso verso l'Europa. Una posizione che deve far maturare la consapevolezza delle responsabilità e delle prospettive che ne derivano.

BIBLIOGRAFIA

J. Agnew, F*are Geografia politica*, Franco Angeli, Milano 2003.
I. Bowman, T*he New World. Problems in political Geography*, New York 1922.
W. Bunge, T*heoretical Geography*, Royal University of Lund, Dept. of Geography, Gleerup 1962.
P. Coppola, U*na introduzione alla geografia umana*, Liguori, Napoli 1986.
K.R. Cox – D.R. Reynolds (eds.), L*ocational Approaches to Power and Conflict*, Haksted Press, New York 1974.
L. Febvre, L*a Terre et l'évolutione humaine*, Renaissance du Livre, Paris 1922.
P. George et al., L*a Geographie active*, Presses Universitaires de France, Paris 1964.
P. George, I *metodi della geografia*, il Saggiatore, Milano 1974.
G. Gottmann, L*a politique des états et leur géographie*, Armand Colin, Paris 1952.
P. Gould, T*he new geography*, «Harper's Magazine» 1969.
D. Harvey, L*a crisi della modernità*, il Saggiatore, Milano 2010.
R.D. Kaplan, T*he Revenge of Geography*, Random House, New York 2012.
P. Khanna, C*onnectography. Le mappe del futuro ordine mondiale*, Fazi Editore, Roma 2016.
Y. Lacoste, L*a géographie, ça sert, d'abord, à faire la guerre*, Maspero, Paris 1976 (ed. it. a cura di P. Coppola, C*risi della geografia, geografia della crisi*, Franco Angeli, Milano 1989).
G. Lizza, G*eopolitica*, Utet Libreria, Torino 2001.
H.J. Mackinder, T*he geographical Pivot of History*, «Geographical Journal» 23 (1904).
R. O'Brien, T*he End of Geography? The Impact of Technology and Capital Flows*, «The AMEX Bank Review» XVII (1990) 5.
F. Ratzel, P*olitische Geographie*, R. Oldenbourg, Monaco 1897.
G. Roletto – E. Massi, L*ineamenti di geografia politica: i confini*, Istituto di Geografia dell'Università di Trieste 1931.
A. Sanguin, F*ine della geografia o rivincita della geografia*?, «Bollettino della Societa Geografica Italiana» XIII (2014) 7.
N.J. Spykman, E*mpowering political struggle: spaces and scales of resistance*, «Political Geography» (1944) 13.
G. Ó Tuathail, C*ritical Geopolitics*, University of Minnesota Press, Minneapolis 1986.
P. Vidal de la Blache, T*ableau de la géographie de la France*, Hachette, Paris 1903.



RISCHIO CIBERNETICO E SICUREZZA NAZIONALE NEL SISTEMA FINANZIARIO

Marina Brogi

Il rischio cibernetico e della sicurezza nazionale nel sistema finanziario è un tema al crocevia di ambiti molto diversi: scientifico, giuridico, economico, aziendale, con implicazioni che si estendono oltre i confini di un singolo Paese. Nella prospettiva dell'economista si presta ad almeno tre diversi livelli di analisi. A un primo livello, in un'ottica macro, occorre rilevare che la sicurezza si può considerare un bene pubblico e ciò comporta che gli investimenti fatti dai singoli attori privati per la sicurezza siano inferiori rispetto a quelli che sarebbero necessari. L'incentivo al free riding, tipico dei beni pubblici, risulta particolarmente pericoloso quando i soggetti siano collegati a sistema, proprio come avviene nel sistema finanziario. Ritenendo che l'investimento di altri sia sufficiente anche per la propria tutela, il free rider rimane vulnerabile cosicché, se viene attaccato con successo, può costituire un canale di entrata e di contagio anche verso chi gli investimenti li ha effettuati. Sono quindi necessari interventi pubblici che possano dispiegarsi in modo diverso: da rimedi regolamentari volti a favorire un coordinamento fra attori privati a investimenti in aree non adeguatamente presidiate da privati, da sussidi o incentivi a privati per orientarne le attività, alla richiesta di informazione relativa ad attacchi subiti, necessaria per l'assessment del rischio e propedeutica a mappature dei sinistri che rappresentano il presupposto per forme di assicurazione e così via. L'ottica macroeconomica ci restituisce una

Prof.ssa Marina Brogi, docente universitario.

prima chiave di lettura, una visione alta in cui sono le caratteristiche di bene pubblico globale della sicurezza informatica a spingere verso un sempre maggiore coordinamento nazionale e internazionale, sotto la guida pubblica. In effetti, numerose sono le iniziative a livello internazionale anche solo di sensibilizzazione e studio dell'impatto della tecnologia e del rischio cyber. Circoscrivendo, per motivi di spazio, alle più recenti, si ricorda a ottobre 2017 la pubblicazione, in occasione del G7 dei ministri delle Finanze e dei governatori delle Banche Centrali, di E*lementi fondamentali per la valutazione efficace della sicurezza cyber per il settore finanziario*, rivolti sia agli intermediari finanziari sia alle autorità di vigilanza, che segue il documento relativo agli E*lementi fondamentali della sicurezza cyber per il settore finanziario* dell'ottobre 2016. Si tratta di uno sforzo continuativo e sono state già identificate nuove aree di approfondimento. Le proposte per condurre simulazioni di crisi cyber cross border saranno tra i prossimi temi trattati dal G7 Cyber Expert Group.

Nella R*accomandazione sulla sicurezza digitale* dell'Ocse pubblicata a ottobre 2015 sono stati delineati otto principi guida volti a sensibilizzare i governi e i vertici aziendali sulla delicatezza e sulle criticità del rischio digitale. Due sono i temi che appaiono di particolare rilevanza: la necessità di considerare il rischio digitale come propriamente economico e l'esigenza di approcciarsi all'identificazione e alla gestione di quest'ultimo in maniera olistica.

Sempre l'Ocse, nel Report sulle prospettive dell'Economia Digitale di ottobre 2017[1], fa emergere due diverse chiavi di lettura: la prima è una prospettiva positiva, che interpreta il settore dei servizi della tecnologia dell'informazione come un 'fattore trainante' dell'economia e come un'*opportunità* di cui i governi sono consapevoli. D'altra parte, permangono le *sfide* – e le conseguenti preoccupazioni – che accompagnano tale processo di trasformazione digitale delle informazioni, che, in quest'ottica, non può che essere condotto con competenze sia specialistiche che generali nella gestione dei servizi e della protezione dei dati.

Simili criticità si desumono dall'ultimo *Global Risk Report* del World Economic Forum (Wef), che riporta una sempre crescente diffusione pervasiva dei rischi tecnologici, tra cui particolare attenzione è rivolta a quello di attacchi cyber. Quest'ultimo figura nella tassonomia dei rischi globali dal 2012 ed è entrato nella Top 5 della probabilità di accadimento degli stessi, definiti come eventi incerti che al loro verificarsi possono causare impatti negativi per più Paesi e settori per i successivi dieci anni. Proprio le implicazioni sistemiche e la stretta interconnessione sono le criticità peculiari del cyber risk che, secondo il Report del Wef, destinano quest'ultimo alla collocazione tra le prime dieci minacce globali di ogni settore, presentando una crescita continua in termini d'impatto stimato e probabilità di accadimento.

Ciononostante, la crescita della tecnologia cyber è annoverata dallo stesso Global Risk Report, tra i cinque fattori determinanti per lo sviluppo globale.

1. *Oecd Digital Economy Outlook* 2017.

Nel discorso sullo stato dell'Unione, il presidente della Commissione europea Jean-Claude Juncker ha citato la cybersecurity come uno dei temi fondamentali per il futuro dell'Europa, anticipando la proposta di un pacchetto di nuove misure volte a innalzare le capacità di protezione dello spazio cibernetico comune contenute nella Comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo R*esilienza, deterrenza e difesa: verso una cibersicurezza forte per l'*UE.

Il documento fa stato su come l'Europa intenda potenziare le proprie capacità di contrasto rispetto ai piani stabiliti nel precedente dossier di cyberstrategy del 2013 (A*n open, safe and secure C*y*berspace*). In tale ambito si ricordano, inoltre, la Direttiva Europea (Network and Information Systems – c.d. Nis) e il nuovo Regolamento europeo per la protezione dei dati personali (Gdpr[2]) entrato in vigore il 24 maggio 2016 e applicabile dal 25 maggio 2018. A ciò si aggiunge la nascita di un Centro di ricerca per la sicurezza cibernetica, con il compito di sostenere lo sviluppo della ricerca e, al tempo stesso, distribuire certificati che siano riconosciuti in tutta Europa.

A un secondo livello, volendo focalizzare l'attenzione sulla sicurezza informatica e sul rischio cibernetico nel sistema finanziario, occorre ricordare che quest'ultimo – composto da intermediari e mercati – rappresenta un'infrastruttura fondamentale di qualsiasi economia moderna. Le informazioni sono alla base dello scambio finanziario, ossia le risorse dalle unità in surplus alle unità in deficit sono sempre più trasferite ed elaborate per mezzo d'infrastrutture tecnologiche in un processo evolutivo inarrestabile. Si citano solo un paio di esempi, uno riferito ai mercati finanziari e l'altro alle banche. I mercati di borsa, un tempo alle grida, sono ora piattaforme tecnologiche in cui vengono inseriti ordini di acquisto e di vendita. Nel caso delle banche, rischio informatico e cyber non riguardano solo i sistemi, ma si estendono ai canali, ossia al rapporto stesso con la clientela. È un processo incontrovertibile che pone la banca davanti a un rischio a bassa probabilità di accadimento, ma con effetti potenzialmente devastanti. Non si può dimenticare che per le banche la fiducia è alla base della sopravvivenza; un attacco in grado di minare la fiducia dei depositanti al punto da tradursi in una corsa agli sportelli diviene per esse letale[3].

2. Il Regolamento generale sulla protezione dei dati è l'innovazione più significativa degli ultimi anni in materia, non solo a livello Unione europea ma globale. Qualsiasi organizzazione che gestisca le informazioni personali dei residenti nell'UE, a partire dal 25 maggio 2018 dovrà adattarsi alla nuova normativa in materia di trattamento dei dati personali, sicurezza delle informazioni, processi di conformità e relazioni contrattuali. Le organizzazioni hanno meno di 18 mesi per farlo: ignorarlo o commettere errori nella sua applicazione può avere conseguenze costose perché alcune violazioni sono punibili con sanzioni pecuniarie fino al 4% del fatturato totale annuo dell'azienda o a un massimo di 20 milioni di euro e danneggiarne così la reputazione.

3. «La vulnerabilità più evidente di un sistema capitalistico si raggiunge nel malfunzionamento del mercato del credito. Con la platea dei risparmiatori incerta a proposito della solvibilità di date banche, anche per la non precisione e la non tempestività delle comunicazioni»; Bianchi 2016, p. 106.

Alcune caratteristiche intrinseche del settore finanziario – la centralità delle informazioni, le asimmetrie informative, il collegamento a sistema, l'importanza della fiducia – lo rendono particolarmente vulnerabile, il tallone d'Achille dei Paesi occidentali[4] il bersaglio ideale per chi desidera minacciarne il primato economico. Un bersaglio non solo per chi vuole sottrarre fondi dai clienti o dalle banche (come già avvenuto ancora di recente, rispettivamente, per i clienti di Tesco bank e, a seguito dell'attacco a Swift, nella Banca Centrale del Bangladesh) ma anche per chi desidera speculare, operando in anticipo rispetto all'immissione sul mercato d'informazioni false. Si ricorda, solo a titolo di esempio, l'impatto di un comunicato stampa falso sulla società quotata Vinci che ha determinato una discesa del 19% nel prezzo dell'azione, corrispondente a una riduzione nella capitalizzazione della società di oltre 10 miliardi di euro in pochi minuti. In un comunicato stampa che sembrava provenire da un addetto stampa della società alle 16:06 (ora di Parigi), si affermava che, a seguito di un audit interno, si rendeva necessario riformulare il bilancio 2015 e la semestrale 2016, riportando una perdita netta per i due periodi. Si annunciava anche che Vinci aveva licenziato il Cfo Christian Labeyrie, dandone informazione anche all'Autorità di vigilanza francese, l'Autorità dei Mercati finanziari. Ventiquattro minuti più tardi, Vinci dichiarava di essere vittima di una truffa, che coinvolgeva un falso comunicato stampa inviato da un immaginario membro del team di comunicazione del gruppo, che aveva come obiettivo quello di minarne l'attività.
Se l'estensore del comunicato stampa falso avesse venduto prima di emettere il comunicato e riacquistato dopo la reazione del mercato alla notizia falsa avrebbe di certo guadagnato cifre importanti. La velocità di discesa del prezzo è in parte dovuta a sistemi di stop-loss automatizzati con ordini di vendita che scattano se il prezzo scende oltre un certo livello e che contribuiscono ad alimentare il ribasso. La formazione dei prezzi sui mercati azionari dipende dalle nuove informazioni che, modificando le attese relative all'andamento futuro delle società, comportano un riallineamento dei prezzi.
Operare sulla base d'informazioni non ancora diffuse al mercato consente di guadagnare ed è per questo motivo che l'insider trading è un reato. Negli studi economici si presume una possibile attività d'insider trading quando il prezzo dell'azione si muova in maniera anomala rispetto al mercato, anticipando l'effetto della notizia non ancora divulgata, prima dell'annuncio dell'operazione straordinaria o di quell'evento in grado di spostare i prezzi. Nel caso di attacchi cyber si rilevano riduzioni di prezzo anomale prima che la notizia sia stata divulgata al mercato. È interessante notare che la notizia (eventualmente anche falsa) di un cyber attacco nei confronti di una società quotata può essa stessa essere sfruttata per conseguire un profitto operando sui titoli della società medesima. Ciò da parte del soggetto che ha inferto l'attacco (che quindi può trovarsi a guadagnare anche senza che l'attacco sia stato efficace, semplicemente anticipando i movimenti dei prezzi del titolo sul mercato) oppure anche da altri che ne vengano a co-

4. «Chi vuole fiaccare i paesi sviluppati dell'Occidente deve però agire per ridurne il grado di benessere, deve cercare il tallone d'Achille nel dominio della superiorità economica, sulla quale si fonda anche la prevalenza tecnologico-militare, per la capacità di finanziare la ricerca in materia»; Bianchi 2016, p. 105.

noscenza prima del mercato. Ad esempio, a seguito della recente offensiva a Equifax – con il furto di dati riservati di 148 milioni di consumatori americani – la Sec e il Dipartimento di Giustizia americano hanno deciso di aprire un'indagine per verificare se la vendita di titoli per un controvalore totale di 1,8 milioni di dollari da parte di alcuni top manager della società, subito prima della notizia dell'attacco, rappresentasse un caso di insider trading. Poter disporre in anticipo di notizie rilevanti sulle società quotate significa poter guadagnare facilmente. Presumibilmente è per questo motivo che nel 2011 è stato attaccato il Directors Desk del Nasdaq Omx (un'applicazione attraverso la quale i consiglieri di amministrazione delle società quotate si scambiano documenti confidenziali) e, più recentemente, il sistema Edgar della Sec (il supporto su cui le società quotate caricano i documenti riservati per l'autorità). Anche in quest'ultimo caso si teme che le informazioni siano state usate per operare in anticipo rispetto al mercato e lucrare illeciti profitti. Quanto più il sistema finanziario dipenderà da piattaforme di scambio digitali tanto più la sicurezza informatica dello stesso diviene elemento fondante per l'affidabilità dell'intera economia del paese.

La diffusione della tecnologia nell'assetto finanziario è un problema ma può, al tempo stesso, essere una soluzione, poiché se, da una parte, aumenta i rischi cyber, dall'altra, si sviluppano dal suo interno anche gli anticorpi di contrasto, come ad esempio Blockchain e Distributed Ledger Technology[5].

Terzo e ultimo livello di analisi, pensando alla singola azienda, al singolo intermediario finanziario, alla singola società di gestione del mercato. Il rischio cyber sta diventando una preoccupazione chiave per le istituzioni finanziarie con riguardo sia alla business continuity sia all'integrità dei dati. I *flash crash* hanno sottolineato la necessità di avere appropriati meccanismi di arresto del trading sui mercati.

Molto si può e si deve fare anche a livello di singola azienda. In particolare, la cybersecurity è un tema al quale i consigli di amministrazione e i comitati rischi devono dedicare un'attenzione crescente man mano che la tecnologia modifica le combinazioni economico-produttive e distributive delle loro società. Per le banche i tempi sono già maturi, la tecnologia ha modificato in modo definitivo sia i processi di back office sia quelli di front office e di rapporto con la clientela. Con essi ha altresì intensificato l'incidenza dei rischi informatici e cyber. La banca è accessibile 24 ore su 24 e il cliente assistito dalla sola tecnologia è in grado di svolgere autonomamente moltissime operazioni. Rischio informatico e cyber non riguardano solo i sistemi di supporto alle attività ma si estendono quindi ai canali, ossia all'essenza del rapporto con la clientela, le cui estensioni più recenti in altri Paesi includono il *roboadvisory* ossia l'erogazione di consulenza personalizzata automatizzata. Un ineluttabile e crescente utilizzo della tecnologia nell'interfacciarsi con i clienti di oggi è imprescindibile nel farlo con quelli di domani, ossia quegli adolescenti non più *teen ager* ma *screen ager*.

5. Per un'analisi delle potenzialità della Distributed Ledger Technology nei mercati dei valori mobiliari si rimanda a Esma 2017.

Il sempre più ampio ricorso alla tecnologia pone la banca davanti a un rischio difficile da misurare, a più bassa probabilità di accadimento rispetto ad altri, tipici dell'istituto di credito, ma con effetti potenzialmente molto gravi[6]. Un rischio molto infrequente valutato su scenari ipotetici / idiosincratici e non su dati di impatto reali in quanto è ancora in divenire la raccolta ordinata delle informazioni circa gli attacchi e gli impatti economici che hanno determinato. Un rischio che impone investimenti significativi giustificabili solo se si adotta un'ottica strategica di orizzonte non breve e che, quindi, richiede la condivisione del consiglio di amministrazione e l'individuazione e pianificazione d'interventi prioritari. Spesso, nel concreto, i sistemi informativi si sviluppano rispecchiando le singole esigenze man mano che si manifestano e non seguendo un disegno unitario. Occorre invece ricostruire la catena tecnologica e identificare le eventuali vulnerabilità, quei raccordi fra diversi applicativi che possono essere più facilmente attaccati, come pure, nel caso di fusioni e acquisizioni, l'attento smantellamento dei sistemi non più in uso. Nel definire l'ordine di priorità degli interventi, si possono considerare due direttrici guida:

a) a supporto della catena del valore: ossia l'aumento della consapevolezza del personale con riguardo alle condotte da adottare per elevare la sicurezza informatica, la mappatura e la messa in sicurezza delle procedure di rapporto con la clientela, la procedura conti correnti, l'home banking e così via;
b) a supporto della compliance alla normativa (ad esempio, l'adeguata verifica, l'antiriciclaggio e così via).

Per competere, la banca deve migliorare l'accessibilità per il cliente. Tale maggiore facilità di accesso, talvolta, si accompagna a una più ampia possibilità di attacco. L'individuazione delle priorità d'intervento a presidio dei rischi si deve, quindi, accompagnare alla consapevolezza che è molto difficile essere totalmente protetti. Ad esempio, le vulnerabilità in un'app per cellulare sono molteplici: l'hardware, il software, il flusso informativo del network e la custodia dei dati nel tempo. Occorre predisporre ex ante sia un piano di continuità e disaster recovery, che consenta alla banca di continuare a operare nonostante l'attacco, sia un piano di comunicazione e crisis management, per informare e rassicurare clienti e mercati. A conclusione, qualche spunto guardando avanti nella prospettiva dell'economista. Il contrasto al rischio cibernetico richiede un approccio olistico e competenze complementari. Un percorso comune basato sulla collaborazione tra esperti provenienti da ambiti diversi che utilizzano terminologie non univoche. È fondamentale un coordinamento internazionale tra Paesi e un approccio collaborativo tra pubblico e privato per contrastare la criminalità informatica. Le soluzioni devono essere in parte gestite dalle singole aziende, ma devono rispecchiare anche una logica di sistema. La prevenzione, con l'intercettazione di segnali deboli, ad esempio sul dark web, rappresenta un terreno elettivo per le autorità di sicurezza nazionale. Inoltre, l'esperienza dimostra la centralità della persona nei sinistri informatici, talvolta per disattenzione nella

6. Nella *Risk Dash Board*, pubblicata dall'EBA ogni trimestre, quello Cyber viene indicato come un dei maggiori rischi per la stabilità del sistema bancario europeo e a luglio 2017 si sottolinea: «Amid elevated cyber risk, improvements of IT systems are crucial to support the implementation of banks' digitalisation strategies».

gestione dei dati personali e talaltra per pratiche poste in essere da dipendenti infedeli. Il primo tipo di problematica si contrasta anche con la promozione e la diffusione della cultura della sicurezza in ambito informatico che rientra tra le attività attribuite dalla l. 124/2007 al Dipartimento delle informazioni per la sicurezza[7].

La mitigazione, con il ricorso a polizze assicurative, implica la possibilità di trasferire al mercato una parte del rischio residuo. Questo presidio è in crescita rapida negli ultimi anni e richiede mappature complete, contraddistinte da probabilità di accadimento e impatto degli eventi negativi. Il coordinamento promosso su base regolamentare deve passare attraverso la raccolta delle informazioni circa gli attacchi e gli impatti economici che hanno determinato. Quanto più si avranno informazioni tanto più sarà possibile mitigare il rischio, trasferendolo sotto forma economica alle compagnie di assicurazione.

Occorre inoltre rilevare che esistono settori ricchi d'informazioni, come ad esempio i social network, in cui eventuali manipolazioni di dati, da parte di criminali informatici, non sono soggetti alle stesse restrizioni regolamentari dell'organizzazione finanziaria tradizionale. Intermediari e mercati finanziari sono collegati e, di conseguenza, vengono sintetizzati dall'espressione sistema finanziario. Gli elementi collegati tra loro, proprio come le catene, sono forti quanto l'anello più debole. Per questo rappresentano un'infrastruttura critica da presidiare con particolare attenzione.

7. Art. 4, comma 3, lettera m.

BIBLIOGRAFIA

T. Bianchi, *Attacco all'Occidente*, Egea, Milano 2016.

M. Brogi, *Cybersecurity, la strategia che parte dal vertice*, «Il Sole 24 Ore» (14 febbraio 2016).

Clusit, *Rapporto 2016 sulla Sicurezza Ict in Italia* (2016).

Clusit, *Rapporto 2017 sulla Sicurezza Ict in Italia* (2017).

Commissione Europea, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'*UE, Comunicazione congiunta al Parlamento europeo e al Consiglio, 13 settembre 2017.

European Banking Authority (EBA), Risk Dashboard data as of Q2 2017 (2017).

European Securities and Markets Authority, *Distributed Ledger Technology. Key implementation challenges*, Report on Trends, Risks and Vulnerabilities 2 (2017).

European Securities and Markets Authority, *The Distributed Ledger Technology applied to securities markets*, Report, 7 febbraio 2017.

Gazzetta Ufficiale, *Legge 28 dicembre* 2015, *n.* 208, *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato* (*legge di stabilità* 2016), Serie Generale del 30 dicembre 2015, n. 302. Supplemento Ordinario n. 70/2015.

G7, *Fundamental elements of cybersecurity for the financial sector*, ottobre 2016.

G7, *Fundamental elements for effective assessment of cybersecurity in the financial sector*, ottobre 2017.

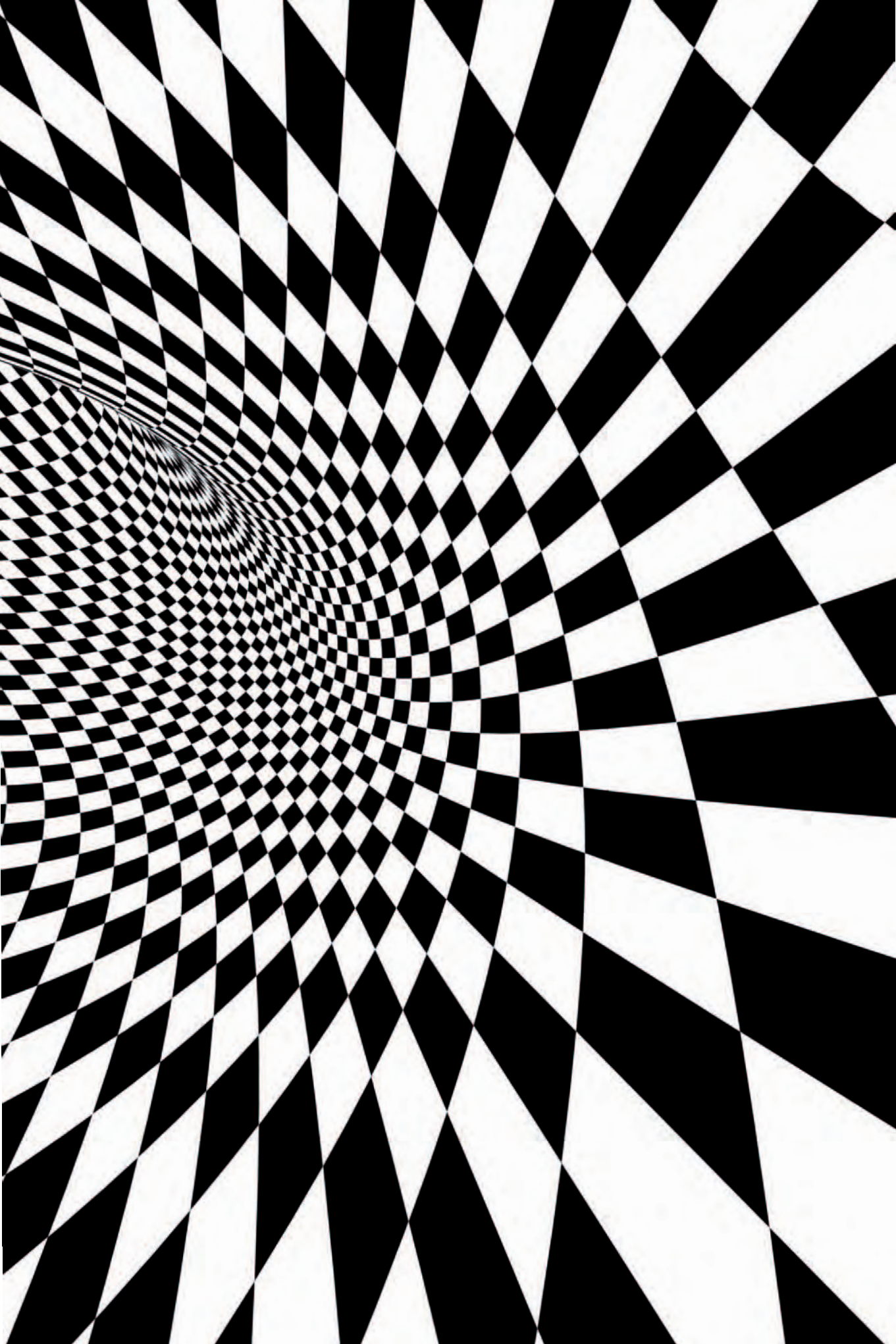
Organizzazione per la Cooperazione e lo Sviluppo Economico, *Digital security risk management for economic and social prosperity*, 1 ottobre 2015.

Organizzazione per la Cooperazione e lo Sviluppo Economico, *Recommendation of Oecd Council on health data governance booklet*, 17 gennaio 2017.

Organizzazione per la Cooperazione e lo Sviluppo Economico, *Oecd Digital Economy Outlook* 2017 / *Prospettive dell'economia digitale* 2017, 17 ottobre 2017.

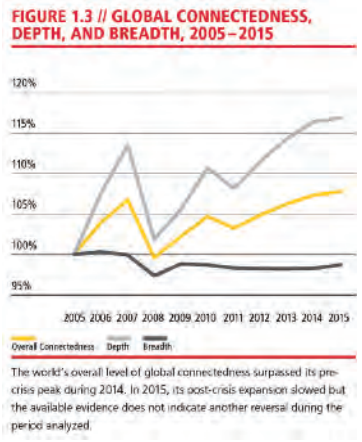
Unione Europea, *Piano di sicurezza informatica dell'*UE *per tutelare l'internet aperta, la libertà e le opportunità nella rete*, 7 febbraio 2013.

World Economic Forum, *Global Risk Report* 2017.



L'INTERNAZIONALIZZAZIONE DEI MERCATI E LA TUTELA DELL'INTERESSE ECONOMICO FINANZIARIO NAZIONALE

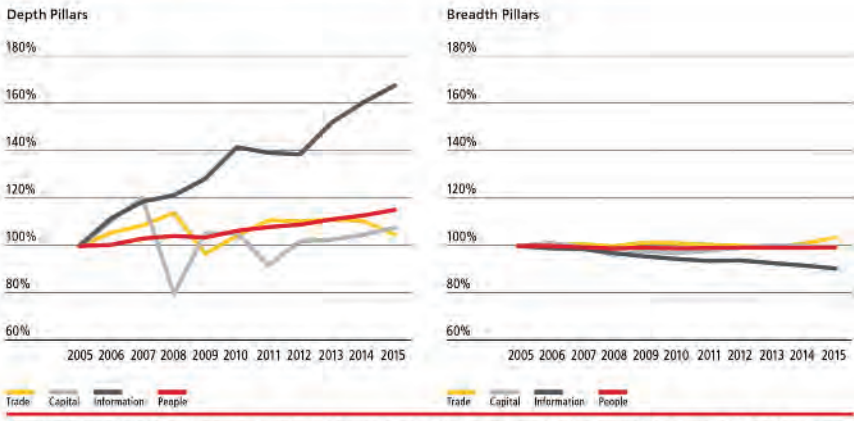
Gustavo Piga



Ancora non siamo in grado di sapere se il decennio che ci lasciamo alle spalle, che gli storici tra cento anni definiranno quello della 'grande recessione occidentale', avrà anche avviato un inizio di ripresa della 'localizzazione' ovvero sia di ritirata di quella globalizzazione che fino a pochi anni orsono ritenevamo inarrestabile. Certamente si assiste a un rallentamento della crescita della globalizzazione, come mostra il *Dhl Global Connectedness Index* 2016 *Report*: solo ora appaiono infatti restaurati i livelli pre-crisi del 2007 (nella figura sopra, linea *overall* centrale), e senza particolare dinamismo, come se la crisi avesse generato degli anticorpi specifici alla stessa.

Prof. Gustavo Piga, docente universitario.

FIGURE 1.5 //
PILLAR LEVEL GLOBAL CONNECTEDNESS TRENDS, 2005–2015



The information pillar has been the largest contributor to increases on the depth dimension of global connectedness since 2013, but those gains were offset in large part in 2015 by a sharp drop on the trade pillar. Year-to-year changes on the breadth dimension tend to be smaller. An uptick on trade pillar breadth in 2015 offset the continuation of a declining trend on information pillar breadth..

Tuttavia, dall'analisi dell'andamento della c.d. 'profondità della globalizzazione' (figura sopra, linea *depth*, in alto, che misura quanta parte di una determinata attività che potrebbe svolgersi sia all'interno che tra Paesi è internazionale piuttosto che domestica) otteniamo una maggiore chiarezza sulla composizione del fenomeno: gran parte del recupero la globalizzazione lo ha raggiunto grazie allo sviluppo dell'informatizzazione dell'economia; un ruolo decisamente minore lo ha giocato la mobilità dei capitali, a fronte di un arretramento deciso del ruolo del commercio internazionale, che non dovrebbe poi sorprendere più di tanto dato che è da lì che politicamente sono nate le maggiori resistenze a un ulteriore allargamento della globalizzazione vista, più che come fenomeno capace di permettere la crescita delle opportunità, come una minaccia ai tenori di vita e alla stabilità occupazionale delle fasce più deboli e meno protette.

La parola «protezione» ci ricorda la natura della risposta strategica più immediata a disposizione di un Paese a fronte di queste minacce portate dalla globalizzazione in un contesto di crisi o di stagnazione economica: il «protezionismo» inteso, da un lato, come restringimento unilaterale degli ambiti di penetrazione del commercio internazionale nell'economia locale da parte d'imprese estere e, dall'altro, come ritiro dai grandi accordi globali o irrigidimento negoziale negli stessi, specie quelli che richiedono sacrifici immediati – comuni – alle imprese nazionali a fronte di vantaggi incerti e di lungo periodo. Sono risposte di policy – quelle citate – che, se emergono con sempre maggior vigore nelle scelte politiche di uno degli attori più rilevanti sulla scena mondiale (gli Stati Uniti), non sono di esclusivo interesse di questi se

si considera, ad esempio, la crescita sostanziale, in termini di consenso elettorale, di movimenti (spesso imprecisamente raggruppati sotto l'egida del termine «populisti») che nelle loro piattaforme programmatiche riescono a coagulare interessi diversificati ma uniti da, appunto, un'opposizione alla globalizzazione.

È forse utile ricordare come questa strategia protezionistica abbia un costo notevole, sia nell'immediato che nel lungo periodo. Nel breve termine, l'illusione che il protezionismo commerciale possa generare benefici, basata sull'erronea congettura di un'assenza di reazione analoga da parte dei partner esteri, si scontra tipicamente con la dura realtà dei fatti e porta rapidamente a esiti di guerra economica che danneggiano tutte le Nazioni coinvolte.

Nel lungo termine, i benefici che si sarebbero potuti ottenere con negoziati globali rischiano di essere perduti, come le recenti tensioni sugli accordi climatici per comportamenti unilaterali ben mettono in evidenza. Se la sicurezza di un Paese dipende strettamente dal benessere materiale che vi prevale, non vi è dubbio che queste preoccupazioni sull'eventuale adozione di strategie protezionistiche travalicano l'ambito strettamente economico e pongono problematiche politiche che vanno al di là delle mere dinamiche interne sollevate poco sopra. In effetti, il rischio ulteriore è di lasciare il pallino del comando della governance globale a nuovi attori, cioè a Nazioni tradizionalmente contrarie sinora alla globalizzazione ma che, nel vuoto di presenza occidentale sullo scacchiere mondiale, rischiano di fare di essa lo strumento per divenire, loro, attori principali del governo internazionale[1].

La risposta non è dunque quella di chiudersi, ma di aprirsi, di affrontare la sfida economica, arrivando tuttavia al tavolo politico globale con la capacità di saper da un lato *proteggere* i propri interessi e dall'altro prevenire le minacce che permanentemente esistono al di fuori dei nostri confini. Come sostenuto dall'ex presidente del Consiglio Mario Monti in un discorso proprio sui temi della sicurezza: «Giusto appare conseguentemente lo sforzo di concentrarsi su due direttrici di fondo attorno alle quali orientare la ricerca informativa in questo ambito: da una parte la prevenzione delle minacce alla sicurezza e agli interessi economici *nazionali*, sia in Italia che all'estero; dall'altra il supporto alle decisioni del Governo volte a sostenere il sistema Paese nella competizione internazionale»[2].

1. Basta fare riferimento al discorso del presidente cinese Xi Jinping al Forum di Davos: <https://america.cgtn.com/2017/01/17/full-text-of-xi-jinping-keynote-at-the-world-economic-forum> [07-11-2017], alla strategia cinese della B*elt and* R*oad* e ai recenti accordi con la Russia, che sembra possano essere estesi addirittura ad accordi su un sistema comune di pagamenti.

2. <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/03/Inaugurazione-aa2013-Monti.pdf> [07-11-2017].

Due brevi chiarimenti sulle parole *proteggere* e *nazionali*. Primo, quello relativo al riferimento, non casuale, da parte del presidente Monti agli interessi *nazionali*. Non è forse contraddittorio, per un Paese membro dell'Unione europea, non fare dell'interesse, appunto, 'europeo' il proprio obiettivo? Non credo, anche al di là dell'evidenza, che un'Unione europea 'irreversibile' non sia più da dare per scontata come prima della crisi e che si debba dunque mantenere con pragmatismo un approccio perlomeno flessibile al riguardo, in ottica di sana gestione del rischio. Se, da un lato, vi sono infatti svariate piattaforme europee aperte, cui l'Italia partecipa certamente con attivismo per perseguire l'obiettivo comune – e l'esempio cade subito su quella forse più rilevante di tutte, di una Difesa e sicurezza comune europea[3] – dall'altro, concentrarsi su un interesse strettamente nazionale può essere funzionale a un rafforzamento della costruzione europea. Così come le debolezze nazionali vengono spesso percepite come una palla al piede per il futuro del Continente, analogamente un'Italia forte (ma non opportunista) è funzionale a un'Europa forte.

Secondo, sulla parola *proteggere*. Termine che ha sempre sofferto di 'cattiva stampa' per la sua similitudine a quell'altra, la cui utilità strategica abbiamo cercato qui sopra di smontare, ovvero «protezionismo». Se, infatti, d'interesse nazionale vogliamo parlare, sarà qui utile concentrarsi, senza timori, sulla rilevanza di una strategia di protezione appropriatamente definita: mentre è evidente che il protezionismo mette in crisi la globalizzazione, è anche vero che la globalizzazione mette in crisi alcune controparti sociali deboli e che se vogliamo far sopravvivere la prima dobbiamo esser capaci di proteggere le seconde. Non dunque una protezione 'a pioggia', ma mirata, che porti a una nuova globalizzazione, 2.0, forse meno impetuosa e prorompente, ma più stabile e duratura, capace di evitare sommovimenti politici che a loro volta mettano a rischio il potenziale di crescita e sviluppo connesso all'evoluzione delle tecnologie che mette a disposizione della collettività, comprese le fasce più deboli, vaste opportunità[4].

Mettendo insieme per l'Italia la parola «interesse nazionale» con «protezione» non dovrebbero esservi dubbi nell'identificare la controparte più meritevole di politiche di sostegno e prevenzione dei rischi: la piccola e media impresa. Tallone di Achille dell'economia italiana, su cui poggia il cammino di sviluppo del Paese ma che se non protetto e piuttosto attaccato può mettere in ginocchio, le Pmi si prestano ben più delle grandi a ricevere politiche

3. Cfr. Pecchi et al. 2017.

4. L'esempio classico nei Paesi più poveri e agricoli è l'uso del cellulare con i conseguenti abbattimenti dei costi e la riduzione dei rischi connessi alla variabilità meteorologica. Cfr, ad esempio, <https://www.researchgate.net/publication/244484894_The_Use_of_Mobile_Phone_Among_Farmers_for_Agriculture_Development> [07-11-2017].

attive di supporto. Che sia così lo mostrano le esperienze di altri Paesi, a cui accenneremo di seguito, ma lo vorrebbe anche il buon senso: per fare un'analogia quanto mai appropriata, una mamma sente il bisogno di proteggere il suo bambino nei primi anni di vita, quando è più fragile, non certo dopo una certa età, quando è tempo di lasciarlo andare da solo nel mondo. Non a caso le politiche di altri Paesi, cui faremo riferimento spesso, prevedono che tale protezione sia estesa soltanto nelle prime fasi di vita dell'azienda e non divengano un vizioso 'protezionismo' cronico.

L'esempio più calzante, non sorprendentemente, deriva da quel contesto in cui più facile è riuscire a far crescere le piccole imprese: la domanda pubblica. Negli Stati Uniti, nel 1953 venne approvato lo Small Business Act, ancora oggi vigente e anzi allargatosi nel tempo per coprire nuovi settori, con il quale viene stabilita la nascita di un'Agenzia (la Small Business Administration) mirata esclusivamente a proteggere la piccola impresa statunitense in nome… della concorrenza. Val la pena soffermarsi sull'incipit di quella legge, capace di farci percepire la posta in gioco con ammirevole chiarezza:

> The essence of the American economic system of private enterprise is free competition… The preservation and expansion of such competition is basic not only to the economic well-being but *to the security of this* Nation. S*uch security and well-being cannot be realized unless the actual and potential capacity of small business is encouraged and developed*. It is the declared policy of the Congress that the Government should aid, counsel, assist, and protect, insofar as is possible, the interests of small-business concerns in order to preserve free competitive enterprise, to insure that a fair proportion of the total purchases and contracts or subcontracts for property and services for the Government (including but not limited to contracts or subcontracts for maintenance, repair, and construction) be placed with small business enterprises...

Spicca il riferimento, significativo per il contesto di questo volume in cui celebriamo la legge di riforma 124/2007, all'inseparabilità tra la sicurezza di una Nazione e l'incoraggiamento e lo sviluppo della capacità attuale e potenziale delle Pmi: i secondi come condizione addirittura necessaria per la prima! Come raggiungere dunque tale sviluppo? Le linee successive dell'incipit lo chiariscono, di nuovo magistralmente: con l'aiuto, la consulenza, l'assistenza e la *protezione* (mio corsivo) degli interessi delle Pmi. In particolare, negli appalti pubblici, riservando una quota (del 23%) esclusivamente alle piccole imprese nei primi anni di attività, così da permettere loro di apprendere a vendere, pianificare, organizzarsi in un mercato protetto e lentamente ma inesorabilmente farsi trovare pronte a sostenere l'impatto della concorrenza in mercati privati, inizialmente locali e infine internazionali.

Due precisazioni meritano di essere fatte al riguardo. Prima, queste politiche di protezione negli appalti pubblici sono previste ovunque nel mondo e non solo negli Stati Uniti: in Cina, Giappone, India, Brasile, Corea del Sud, Messico… ma non in Europa dove, in nome della parità di trattamento, obblighiamo le piccole a confrontarsi (e inevitabilmente a perdere) in gara con le grandi imprese. Seconda, è evidente che svariati sono i campi in cui questa protezione dovrebbe essere applicata, con sforzi mirati da parte di politiche industriali attente: nel campo della regolazione, che va resa asimmetrica per far sì che non finisca per essere uno strumento che danneggi le piccole più delle grandi nella loro competitività, nelle strategie d'internazionalizzazione, dove i costi fissi pesano maggiormente sulle piccole che non sulle grandi, nell'alfabetizzazione universitaria in cui è necessario immaginare un laureato professionalizzato per le esigenze delle Pmi e non solo per le grandi imprese e multinazionali e, non ultimo, in quello della cybersecurity. Se è vero, e non sempre lo è, che le nostre grandi imprese possono 'cavarsela da sole' di fronte alle minacce d'invasioni informatiche, è certo che le Pmi sono vulnerabili e ciò è tanto più rilevante una volta preso atto dell'altissimo tasso d'innovazione presente in molte di esse e quindi dell'attrattività che costituiscono per fenomeni devianti a livello globale.

L'Italia non è normativamente scoperta a fronte di questi pericoli: nel 2011 è stata adottata una legge (11 novembre 2011, n. 180, recante 'Norme per la tutela della libertà d'impresa. Statuto delle Imprese'), che obbliga il Governo a presentare annualmente alle Camere entro il 30 giugno un disegno di legge per la tutela e lo sviluppo delle MicroPmi, dove potrebbero trovare organica disciplina tutte le misure strategiche essenziali di cui sopra. Purtroppo, sino a oggi, non è stata colta tale opportunità di dotare il sistema che rappresenta la parte più significativa della nostra economia di adeguato supporto, scelta necessaria per incrementare la capacità reale di crescita economica, di sviluppo e coesione sociale.

È evidente come vi siano altri strumenti, oltre a quello di aiuti diretti pubblici, per sostenere e proteggere le nostre Pmi nel loro processo di crescita e internazionalizzazione, con un evidente effetto volano per il Paese. Colpisce, in particolare, la scarsa presenza all'interno del sistema economico italiano, rispetto ai partner con i quali tradizionalmente ci paragoniamo, del settore della consulenza strategica e manageriale. I dati della tabella che segue, relativi al management consulting in percentuale del Pil, sono indicativi al riguardo: anche in valore assoluto il fatturato tedesco è quasi otto volte quello italiano, quello britannico il doppio. Sono due Paesi che usano questa 'soft intelligence' non solo a supporto diretto delle imprese nazionali ma anche finendo per diventare consiglieri di aziende e governi non nazionali, orientando le decisioni di questi inevitabilmente in una direzione favorevole al proprio Paese.

Eppure in Italia stenta a decollare una simile industria, così sinergica anche agli interessi strategici della nostra sicurezza nazionale. Val la pena chiedersi: come mai? La risposta ancora una volta si trova nella totale carenza di politiche degli appalti pubblici volte a sostenere la crescita di nostre piccole aziende nel settore della consulenza. Anzi, è evidente come non sia solo questione di carenza di supporto ma addirittura di scoraggiamento, visto il fil rouge che dalla stampa agli organi supremi di audit percorre il Paese, in una campagna volta a scoraggiare, al contrario di altre nazioni, una solida presenza di aziende di consulenza al fianco della Pubblica amministrazione.

Management Consulting: fatturato/PIL

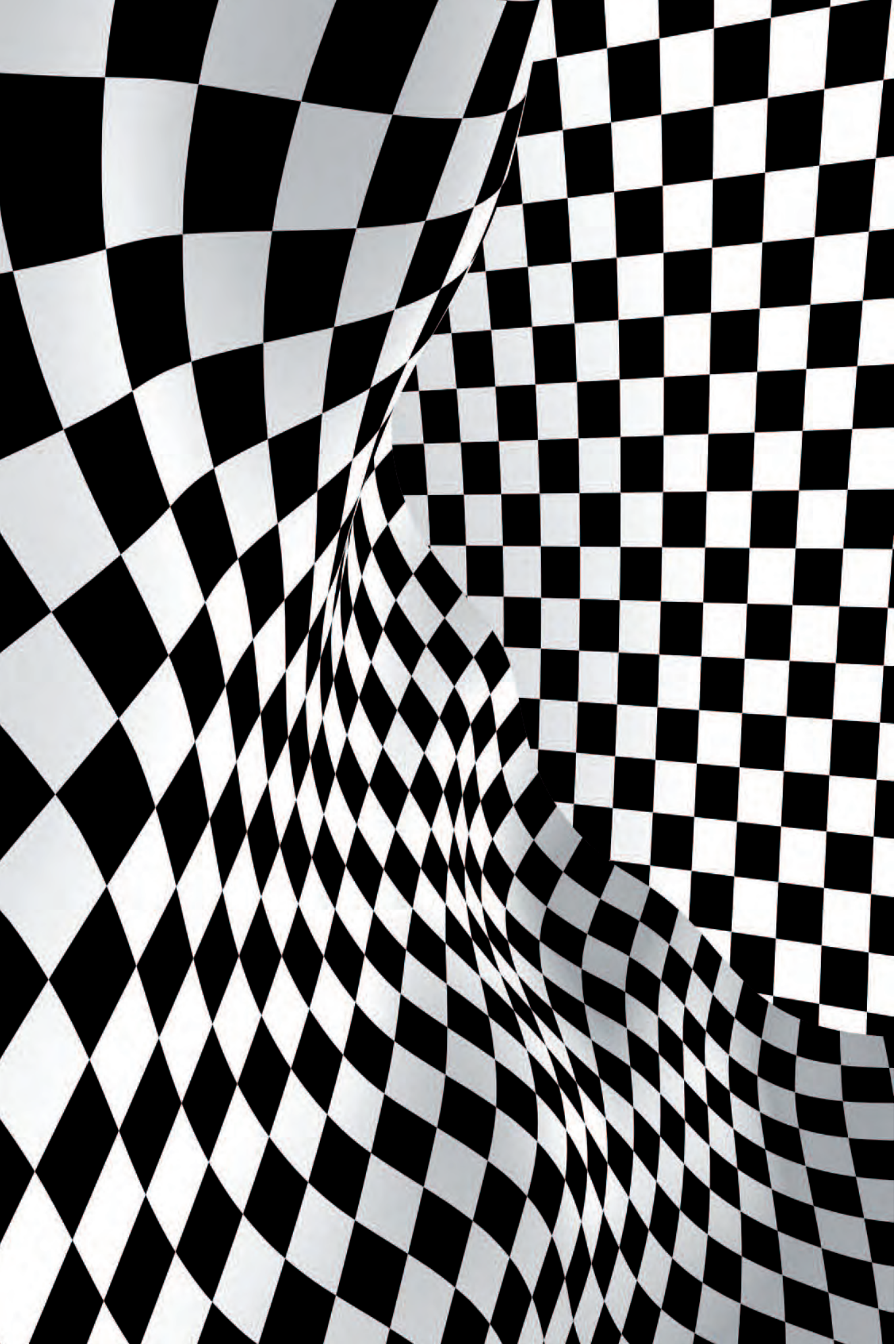
	2012	2013	2014	2015	2016	2017
Francia	0,24%	0,24%	0,25%	0,25%	0,26%	0,29%
Germania	0,81%	0,84%	0,86%	0,89%	0,92%	0,98%
Italia	0,20%	0,20%	0,20%	0,22%	0,23%	0,24%
Regno Unito	0,30%	0,32%	0,31%	0,29%	0,33%	0,34%

Feaco report of Management Consulting in Europe: <http://www.feaco.org/site-page/feaco-annual-survey-european-mc-market> [10-11-2017].

Politiche di questo tipo – dalla cybersecurity alla consulenza strategica, dall'internazionalizzazione alle università professionalizzanti – se mai venissero applicate, necessiterebbero a loro volta di nuovi tipi di conoscenze, più interdisciplinari, più capaci di sviluppare competenze trasversali e social skills: una sfida essa stessa per la nostra formazione superiore dei giovani a livello terziario. Per governare la globalizzazione e renderla coerente con le esigenze di sicurezza interna ed esterna non bastano le parole: ci vogliono politiche di riforma precise, finora non solo mai attuate ma raramente dibattute, e investimenti e risorse che attraversino la Pubblica amministrazione tutta e il Comparto sicurezza in particolare, senza timore di spendere ma determinati a farlo bene. Il circolo virtuoso della crescita duratura e stabile è a un passo da noi, basta accorgersene e avviarlo.

BIBLIOGRAFIA

L. Pecchi et al., *Difendere l'Europa*, Chiarelettere, Milano 2017.



IN UN FOGLIO L'EVIDENZA

Eugenio Lo Sardo

Vorreste sapere chi ha ucciso John Fitzgerald Kennedy? Lo saprete tra pochi giorni. La verità è chiusa in qualche scatola di carta, posata su uno scaffale da circa sessant'anni. Ci credete? In verità vi sono buoni motivi per dubitarne. Si potranno certamente esplorare molti altri aspetti di quell'evento drammatico e cruciale della storia del mondo e, forse, si giungerà a scrivere una versione condivisa e inoppugnabile. Perché la documentazione, come molti sanno, non è di per sé oggettiva, non è un precipitato chimico addensatosi sul fondo della Storia, lungo una linea temporale uniforme e costante. Gli interventi sulle carte sono continui e ripetuti per le ragioni più varie. Sarebbe troppo lungo seguirne il percorso qui e ora. Basti pensare che una nota burocratica ha una struttura precisa, spesso basata su un attento artificio volto a proteggere l'estensore stesso. Chi scrive, soprattutto in determinati ambiti, sa che quel foglio potrà essere portato a prova e a testimonianza di un imperdonabile errore. I gesuiti affermavano: «negare semper, admittere numquam». È un motto per molti ancora valido. E allora, perché conservare e studiare questi abili artifici? La prima risposta è la seguente: nel gioco degli specchi, anche il più complesso, da qualche parte esiste l'oggetto che si riflette. Nei rimandi tra i vari archivi si consolida un'opinione, una

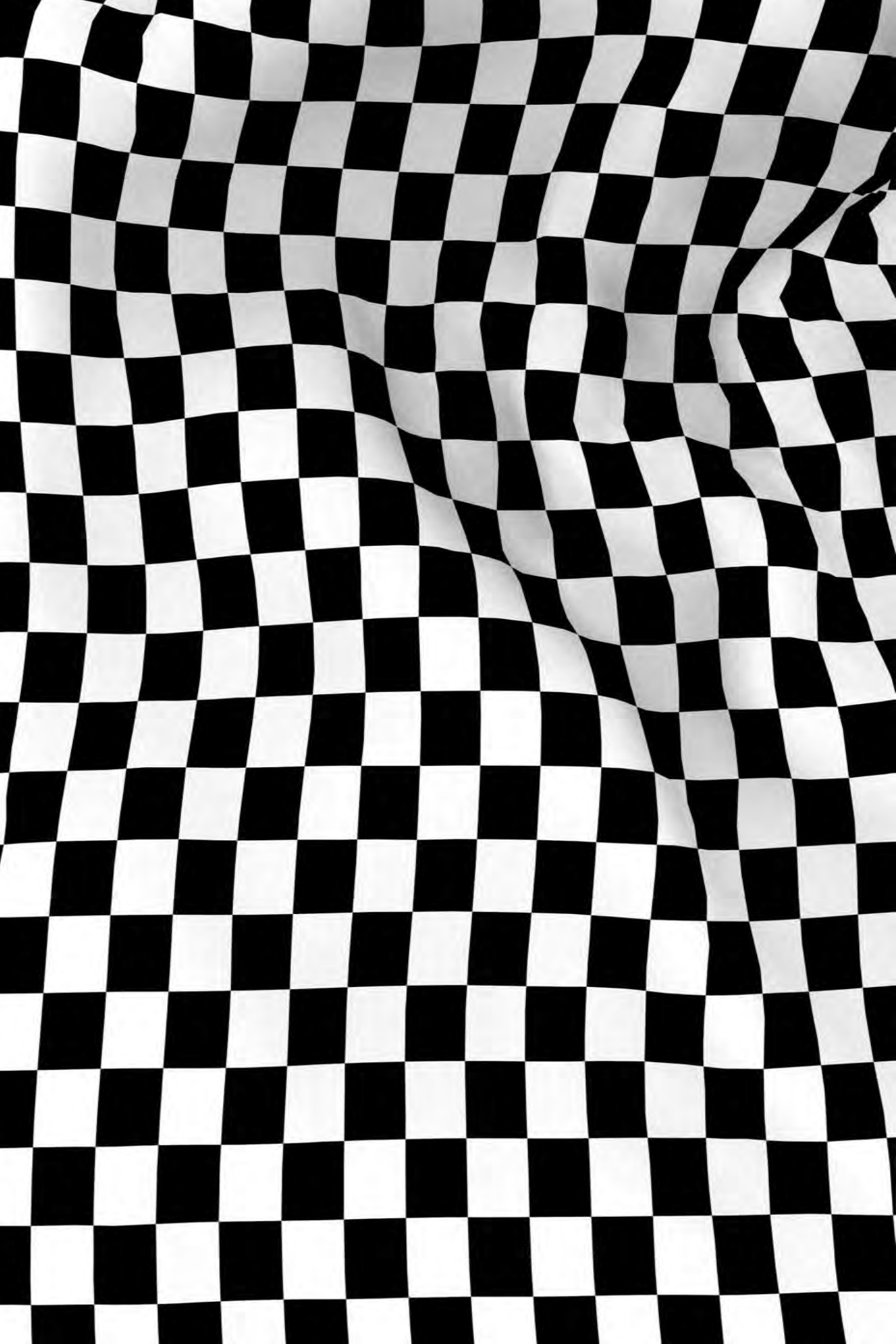
Prof. Eugenio Lo Sardo, sovrintendente all'Archivio Centrale dello Stato.

versione dei fatti. Se all'origine vi può essere un'omissione di chi scrive, nell'esegesi, fatta da altri contemporanei con affinati strumenti o successivamente dai ricercatori, può trovarsi una qualche verità. Alle volte la notizia emerge da una pagina di giornale o da un atto apparentemente minore come una denuncia per calunnia che nasconde un caso molto più consistente, addirittura un tentativo, vero o presunto, di colpo di Stato. Più si segue con scrupolo un'indicazione più si avranno probabilità di giungere a un'interpretazione valida, a una narrazione che sopravviverà nel tempo e s'installerà nelle memorie comuni.
L'intenso e sotterraneo lavoro di ricerca ha un'alta funzione sociale. In un recente libro si svelano, sulla base di nuovi elementi, i presunti mandanti dell'omicidio dei fratelli Rosselli. Perché è così importante saperlo? Non solo per gli aspetti di rilevanza penale – perché forse sono tutti defunti o emigrati in luoghi sicuri, o amnistiati – ma anche a un altro scopo: la trama della democrazia è fatta di fili brevi e sottili. Si spezza facilmente, va continuamente riannodata e risarcita. La democrazia non accetta angoli bui. Lo vediamo sempre di più ai nostri giorni in cui la richiesta di trasparenza e di onestà emerge come un flusso potente. Sono valori imprescindibili anche se, al contempo, se ne dimenticano altri come la felicità e il benessere.
Proprio il tema della felicità ci porta indietro nel tempo, nel Settecento, agli inizi del nostro percorso politico, quando si cominciarono a redigere e attuare le prime Costituzioni, nel Nord America, in Francia e altrove. Uno dei maggiori protagonisti di quella stagione fu il sommo filosofo Gaetano Filangieri. Nelle prime pagine della *Scienza della Legislazione* spiccano alcune note sui doveri del monarca, allora, dello Stato oggi: garantire la sicurezza e la tranquillità ai cittadini. «Confidenza nel governo; confidenza ne' magistrati; confidenza negli altri cittadini; sicurezza di non poter essere turbato, operando secondo il dettame delle leggi», questo scrive nelle prime pagine l'allora giovanissimo filosofo[1]. Perché è evidente che senza questi presupposti non si fonda una società e si aprono le porte alla barbarie. È superfluo parlare di felicità e di benessere se prevalgono gli istinti brutali, sia per gli interni conflitti sia per le aggressioni esterne. Gli apparati di sicurezza e di difesa sono gli organi deputati a questa funzione primaria, fisiologica nelle società avanzate. Ma le democrazie moderne non ammettono che i compiti assegnati a chi si occupa di sicurezza siano svolti senza la necessità di rendere conto delle azioni compiute: nessuno può ritenersi *legibus solutus*. Inoltre la società dell'informatica promette una soddisfazione immediata dei quesiti. Se posso acquisire subito, gratuitamente o quasi, i dati che cerco perché non devo ricevere delle pronte risposte da amministratori o agenti pubblici che pago con le mie tasse?

1. G. Filangieri, *La Scienza della Legislazione*, Grimaldi & C., Napoli 2003, p. 22.

Questa è l'equazione, tutto è disponibile con un clic. Si dimentica, come in un videogioco, che dietro a quel mondo virtuale ci sono delle persone, delle vite, degli uomini e delle donne. C'è gente che rischia la vita per compiere missioni pericolose o, più semplicemente, per tenere informato il nostro Governo recandosi in luoghi poco sicuri, in teatri di guerre dichiarate o striscianti. E la tranquillità di cui godiamo – passeggiare per le strade, andare a un concerto, viaggiare, recarsi al lavoro – si deve a un continuo lavorìo, spesso noioso e ripetitivo, d'intelligence, con controlli, carte d'archivio, esame di dati, analisi e filtraggio di notizie.

L'Italia, come e più di altri Paesi, ha vissuto nel corso del Novecento lunghi periodi in cui alcuni principi basilari del vivere comune si sono offuscati o sono stati efficacemente rimossi. Chi conosce i documenti sa quante volte la polizia fascista passasse a controllare Alcide de Gasperi, che non aveva compiuto alcun misfatto, sa cosa accadde a Benedetto Croce, svegliato nella notte a casa sua da una squadraccia poi dileguatasi o a Giacomo Matteotti, il capo dell'opposizione in Parlamento, o a un giovane studente di grande intelligenza, Giovanni Pugliese Carratelli, mandato al confino senza particolari motivi. Il primo dopoguerra ha prodotto una splendida Costituzione ma, per molti versi, non è stato un momento di compiuta democrazia. La posizione strategica dell'Italia, sul confine con il blocco sovietico, la presenza di un grande partito comunista, l'approfondirsi della divisione tra Nord e Sud, non hanno consentito la piena libertà di esprimersi senza fraintendimenti alle diverse parti sociali. Nel Mediterraneo vi erano molti più Paesi governati da una dittatura che repubbliche democratiche e il timore di scivolare sotto il tallone di un uomo forte o di un putsch non era ingiustificato. Poi ci fu la stagione oscura di orribili attentati, simili nel loro dispiegarsi da quelli raccontati in *The quiet American* (1955), splendido libro di Graham Greene. Piazza Fontana, piazza della Loggia... l'elenco è lunghissimo e con esso la scia di dolore, di sangue, di tragedia. Chi compì quegli attentati e perché? E, soprattutto, vi furono coinvolti settori dello Stato e vi furono complicità internazionali? Altri e più autorevoli autori, giudici e procuratori hanno dato delle risposte, alcune volte esaustive. Ma i processi sono durati decenni e molte domande non hanno avuto risposta. Si avanza nella penombra mentre si vorrebbe illuminare a giorno la storia del nostro Paese, perché rinasca quello spirito di speranza e di ottimismo che animava la generazione nata subito dopo le guerre risorgimentali e l'Unità d'Italia. Le iniziative con segno positivo non sono mancate e tra queste si annoverano la declassifica e il versamento di intere serie dei Servizi di sicurezza (nelle loro mutate denominazioni). Due presidenti del Consiglio, Romano Prodi e Matteo Renzi, hanno deliberato mettendo a disposizione tutti gli atti riguardanti il caso Moro o altri attentati e stragi.

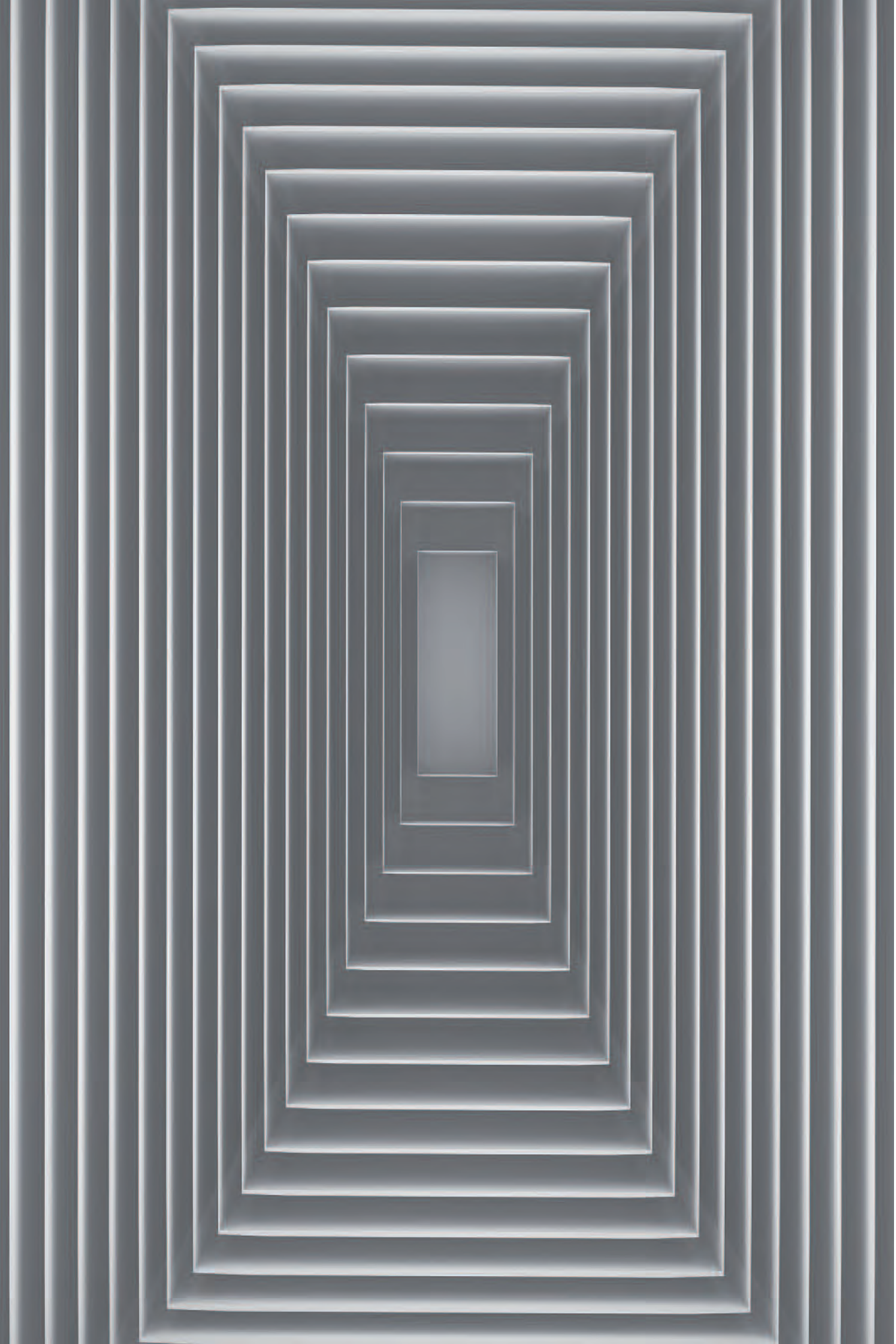


Le carte relative, selezionate dagli organi competenti, sono ora a disposizione dei cittadini. Tra queste, di particolare importanza vi sono quelle prodotte dai Servizi segreti che hanno svolto un lavoro pionieristico dettando la linea ad altri organi di grande tradizione. Il problema riguardava le notizie sensibili, tutelate dalle normative vigenti, contenute in alcune note che, per tale motivo, non possono essere integralmente disponibili per i ricercatori. La soluzione è stata quella di versare tutto il patrimonio all'Archivio centrale dello Stato, sia in forma digitale che cartacea. La parte digitale è consultabile ma contiene delle obliterazioni che preservano i dati sensibili. La parte cartacea sarà a tutti disponibile alla scadenza dei termini stabiliti per legge.

Sono fonti straordinarie, malgrado la loro parziale decontestualizzazione, e assumeranno ancor più valore dal punto di vista storiografico quando altri archivi si aggiungeranno, permettendo una più chiara comprensione della nostra storia recente.

Non tutti i dubbi si sono dissipati e tantomeno le diffidenze. Ma l'apertura al confronto ha dato avvio a un continuo e fitto dialogo tra i rappresentati della società civile e dei famigliari delle vittime delle stragi e gli organi preposti alla sicurezza. Si è costituito un archivio di notevole consistenza e ci si è dotati di strumenti aggiornati e modernissimi per esplorarlo. In breve, si è ragionato su una problematica complessa, non in modo astratto e narcisistico, ma operando in modo dialettico, anche conflittuale a momenti, nel tentativo di sceverare e comporre le ragioni di chi chiede – giustamente – più trasparenza e di chi pone limiti che attengono alla sua stessa efficacia e funzionalità operativa.

Sono state prove di democrazia, dibattiti a volte accesi e serrati che altrove, per motivi politici, non possono svolgersi. È un lento ritessere gli invisibili legami che rendono il nostro Paese una comunità forte, intelligente e solidale.



06

IL PERCORSO EVOLUTIVO DEGLI STUDI SULL'INTELLIGENCE IN ITALIA

Mario Caligiuri

Nell'ultimo decennio, anche il nostro Paese è stato interessato da una marcata trasformazione della percezione dell'intelligence cui hanno concorso molteplici fattori. Tra questi, la ridefinizione dell'attività dei Servizi dopo la fine della Guerra fredda, la diversità dei tempi decisionali richiesti dalla globalizzazione, l'egemonia delle multinazionali finanziarie, l'invadenza della criminalità, la sovrabbondanza informativa e la sorveglianza di massa, le conseguenze degli attentati dell'11 settembre, le severe ricadute della crisi economica mondiale, il fenomeno migratorio, il rafforzamento della lotta al terrore che dal 2015 ha invaso l'Europa. Da qui una triplice trasformazione dell'intelligence: da luogo oscuro dello Stato ad arma segreta delle democrazie, da sistema di previsione del futuro a strumento di interpretazione del presente, da metodo per pochi a processo di trattamento delle informazioni per tutti. In tale quadro si colloca la legge di riforma del settore.

Prof. Mario Caligiuri, docente universitario.

IL CONTESTO CULTURALE

Nel 2003, nell'ambito di una riflessione sullo stato dell'arte degli studi sull'intelligence in Italia, rilevavo una serie di ritardi nello sviluppo della cultura della sicurezza, sul piano accademico, editoriale e culturale[1].

Nel nostro Paese – in ambito accademico – si registravano meno di dieci iniziative che riguardavano, per lo più indirettamente, gli *intelligence studies*, allocati negli ambiti di scienze politiche, criminologia e comunicazione pubblica. In particolare, erano attivi:

- per le scienze politiche, un master in Geopolitica e sicurezza globale presso La Sapienza di Roma, uno in Peacekeeping e Security Studies a Roma Tre e un altro in Peacekeeping Management a Torino, nonché un corso nell'ambito delle Relazioni internazionali a Firenze;
- per la criminologia, un corso di perfezionamento in Tecniche di analisi e di intelligence presso La Sapienza e altri di perfezionamento in Sicurezza e criminologia a L'Aquila;
- per la comunicazione pubblica, l'insegnamento, rivolto all'intelligence, di Teoria e tecniche della comunicazione pubblica all'Università della Calabria; un master in Intelligence & Security presso la Link Campus della Malta University e uno in Scienza delle investigazioni presso la Ludes di Lugano.

Tali iniziative erano il frutto dell'attenzione di singoli docenti che, nei rispettivi atenei, avevano orientato gli studi verso l'intelligence: tra questi, vanno ricordati Umberto Gori, Francesco Sidoti e Francesco Bruno. Da allora, i settori di studio dell'intelligence si sono ampliati, con un'ovvia prevalenza della dimensione cyber. Oggi, in Italia, sono quattro le aree principali di approfondimento, riferite per lo più ai master in ambito Cyber Security, criminologia, intelligence economica e Big Data Analytics. In particolare, sono da segnalare:

- per la cybersecurity, quelli in Cybercrime e Informatica forense e in Sicurezza delle informazioni e informazione strategica, presso Sapienza; quelli in Sicurezza informatica e cybersecurity e in Ingegneria della sicurezza, attivati alla Link Campus; quelli in Cybersecurity a Pisa, in Ethical Hacking all'Università della Calabria e in Cyber Defence a Modena e Reggio Emilia;
- per la criminologia, quelli in Criminologia e scienze strategiche, presso Sapienza; in Criminologia e diritto penale. Analisi criminale e politiche per la sicurezza urbana, alla Federico II di Napoli, in Scienze criminologiche, investigative e scienze della sicurezza, presso il Suor Orsola Benincasa sempre a Napoli; in Scientific Intelligence, scienze comportamentali criminologiche e applicate alle investigazioni e all'intelligence presso la Link Campus; in Criminologia e psicologia investigativa attivato a Foggia; in Scienze criminologiche e forensi, investigazione e sicurezza organizzato a Viterbo; il corso di perfezionamento e aggiornamento professionale in Criminologia e sicurezza nel mondo contemporaneo all'Università telematica Niccolò Cusano;

1. Caligiuri 2003, pp. 85-108.

– per l'intelligence economica, il master in Business Intelligence e Big Data Analytics presso Milano-Bicocca, e quella in Intelligence economica di Tor Vergata;
– per ciò che attiene al processo di analisi dei dati, il master in Data Science and Business Analytics alla Bocconi; in Data Science a Bologna; in Big Data Analytics and Social Mining a Pisa; in Analisi dati per la business intelligence e Data Science a Torino; in Data intelligence e strategie decisionali alla Sapienza.

In aggiunta a tale offerta formativa specialistica, altri percorsi sono stati disegnati secondo un approccio multidisciplinare, come: il master in Intelligence dell'Università della Calabria; quello in Intelligence e sicurezza della Link Campus; il corso di perfezionamento in Intelligence e sicurezza nazionale organizzato a Firenze.

Altri itinerari formativi correlati agli studi d'intelligence si occupano di analisi comportamentale, come i master in Analisi comportamentale e scienze applicate all'intelligence e in Homeland Security della Link Campus; quelli che riguardano la criminalità organizzata e il terrorismo internazionale come il master in Scenari internazionali della criminalità organizzata a Milano; in Analisi, prevenzione e contrasto della criminalità organizzata e della corruzione a Pisa; in Strategia globale e sicurezza organizzato alla Sapienza. Alcuni master, come quello in Studi strategici e sicurezza internazionale all'Università Ca' Foscari di Venezia, sono collegati a istituti militari. Corsi di laurea dove l'intelligence ha formato per la prima volta oggetto d'insegnamento sono quelli di Scienze dell'investigazione, organizzati a L'Aquila e poi a Perugia. Attualmente, l'intelligence è studiata anche nei corsi di laurea in Scienze della difesa attivati a Torino, Enna e Modena-Reggio Emilia, e nel corso di laurea magistrale in Data Science a Milano-Bicocca.

Nel quadro delle iniziative didattiche incentrate sulle tematiche d'intelligence va segnalato il ruolo dell'Università della Calabria che ha inserito l'intelligence nei corsi di studio (nell'a.a. 1999-2000), organizzato master accademici, istituito un centro studi universitario[2], dato impulso a collane editoriali, promosso convegni scientifici, stimolato innovative tesi di laurea, realizzato un sito internet accademico[3], sensibilizzato i rettori italiani sull'importanza dello studio dell'intelligence[4], indetto un'università d'estate.

2. Nel 2008 il Centro di documentazione scientifica sull'intelligence dell'Università della Calabria, dal 2017 denominato Laboratorio sull'intelligence dell'Università della Calabria.
3. Nell'aprile 2017 è stato attivato il sito <www.intelligencelab.org> promosso dal Laboratorio sull'intelligence.
4. Nell'aprile 2016 si è tenuto un seminario presso la Crui a Roma in cui è stata presentata l'esperienza degli studi sull'intelligence maturata nell'ateneo calabrese. Da questo seminario è scaturito, nel novembre successivo, il protocollo d'intesa tra il Dis e la Crui.

Un significativo cambio di passo è poi segnato dall'apertura dell'intelligence al mondo accademico, nello spirito della legge di riforma 3 agosto 2007, n. 124, che affida al Dis le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale[5]. In tale ambito si collocano: i molteplici incontri svolti negli atenei italiani, che hanno portato alla sottoscrizione di 18 accordi di collaborazione (un dato significativo al riguardo è costituito dalle prime assunzioni di operatori dell'intelligence dalle università, con particolare riferimento alla sicurezza informatica); il protocollo d'intesa firmato con la Crui per promuovere lo studio dell'intelligence nelle università; l'accordo con il ministero dell'Istruzione, dell'università e della ricerca finalizzato a sostenere la cultura della sicurezza nelle scuole, l'approfondimento delle tematiche d'intelligence nelle alte scuole delle Forze di polizia.

Per quanto attiene alle iniziative editoriali, la prima collana di studi sull'intelligence è stata promossa nel 2002 dall'editore Rubbettino. I volumi iniziali sono stati I*ntelligence. Spie e segreti in un mondo aperto* di Robert D. Steele e A*becedario* di Francesco Cossiga. Dal 2009, lo stesso editore ha pubblicato numerosi saggi sulla materia tra cui quelli della collana del Centro di documentazione scientifica sull'intelligence dell'Università della Calabria, con testi che hanno dato spazio al ruolo dell'intelligence con riferimento, tra l'altro, al contrasto alla 'ndrangheta, al cyberspazio e all'ambito economico, definendo la visione multidisciplinare della materia. La prima rivista di cultura sull'intelligence «Per Aspera ad Veritatem» è nata per iniziativa del Sisde nel 1995 e ha proseguito le sue pubblicazioni fino al 2004, rappresentando il primo esperimento del genere in Europa. Dal 2005, la rivista ha cambiato il titolo in «Gnosis. Rivista italiana di intelligence». Ora diretta dall'Aisi ed edita dal marchio Argos, la rivista è pubblicata spesso unitamente ad agili opere sull'intelligence che coniugano il rigore scientifico all'esigenza divulgativa.

Per quanto riguarda, infine, le iniziative culturali, dal 1981 l'Istituto Gino Germani svolge un'azione di stimolo degli studi sull'intelligence in Italia con iniziative e convegni. Analogo ruolo è assolto dalla Link Campus, molto attiva anche sul piano dell'offerta accademica. Il primo sito internet privato che si è occupato di intelligence è stato «Silendo», che dal 2005 approfondisce i temi delle relazioni internazionali e della sicurezza nazionale. Nel 2009 è sorta la Fondazione Icsa, dedicata alla sicurezza, alla difesa e all'intelligence, con la promozione di convegni, ricerche e pubblicazioni.

5. A tale riguardo, una funzione significativa svolge anche il sito istituzionale <www.sicurezzanazionale.gov.it>, che presenta sezioni nelle quali si promuovono collaborazioni con le università, approfondimenti e letture. Attraverso il sito è possibile avanzare candidature di ammissione al Comparto intelligence.

La rivista «Formiche», in particolare nella sua versione on line, ha inserito il tema dell'intelligence tra gli argomenti di punta. La rivista «Limes» ha pubblicato nel 2014 un numero monografico dal titolo A *che servono i Servizi*. Ma il ruolo dell'intelligence viene oggi affrontato in tanti ambiti, dal G7 University di Udine[6] alla Borsa mediterranea sul turismo archeologico di Paestum[7].

IL PERCORSO DEGLI STUDI

Le pubblicazioni sono sempre più numerose e non più confinate alle ricostruzioni storiche o alla disciplina legislativa. Senza pretesa di completezza, proverò a delinearne contenuti e tendenze, precisando da subito che il tema del segreto di Stato è tra quelli più investigati. Sul piano della riflessione giuridica, pregevole è il volume I *servizi di informazione* e il *segreto di Stato*[8] che compendia un'attenta ed esaustiva analisi di ogni aspetto della legge di riforma del 2007. Di particolare interesse il recente testo di Marco Valentini sui valori costituzionali della sicurezza, argomento finora poco dibattuto in Italia[9] e, per gli aspetti divulgativi, i volumi di Aldo Giannuli. Da notare anche i contributi di approfondimento che portano la firma di operatori dell'intelligence: dopo Fulvio Martini, si possono annoverare altri ex direttori dei Servizi, come Mario Mori e Luigi Ramponi, ed ex appartenenti ai medesimi Organismi. Un lavoro di scavo storico molto interessante è quello di Virgilio Ilari[10] e Stefano Musco[11]. Continua, inoltre, a essere nutrito il filone delle ricostruzioni delle controverse attività dei Servizi nazionali ed esteri, dal Mossad al Secret Service britannico, dalla Cia all'intelligence d'Oltrecortina. Tra i tanti, spiccano i contributi di Rosario Priore[12] e Mimmo Franzinelli[13], che offrono una chiave di lettura di alcune vicende d'Italia, e di Emanuele Macaluso[14] e Nicola Tranfaglia[15], che gettano uno sguardo d'insieme sui cosiddetti

6. Nella tavola rotonda E*ducation and Sustainability*, svoltasi nel mese di giugno 2017 nell'ambito del G7 University di Udine, alla presenza di rettori provenienti da 20 Paesi esteri, si è affermato che un mondo più sostenibile è innanzitutto un universo con più sicurezza e che l'intelligence può essere uno strumento decisivo per garantirla.

7. L*a tutela del patrimonio culturale, la difesa dell'arte e il ruolo dell'intelligence* è il titolo della manifestazione conclusiva della XX Borsa mediterranea del turismo archeologico, svoltasi il 29 ottobre 2017 a Paestum.

8. Mosca et al. 2008.

9. Valentini 2017.

10. Ilari 2009. Di particolare interesse è la parte terza: L*a sicurezza interna*, pp. 443-602.

11. Musco 2014.

12. De Prospo – Priore 2001.

13. Franzinelli 2009.

14. Macaluso 2014.

15. Tranfaglia 2011.

'poteri occulti'. Altri testi significativi pubblicati negli ultimi dieci anni riguardano la morte di Nicola Calipari e la più eclatante attività di intercettazioni della storia della Repubblica, cioè quella di Telecom. L'intelligence è stata inoltre incrociata con la geopolitica e con la magistratura, ma pure inquadrata nell'ambito della teoria del complotto, delle fonti aperte, della dimensione economica, dello scambio internazionale delle informazioni. Un'area in grande espansione è quella del cyberspazio, con contributi che hanno visto Umberto Gori tra i più attenti osservatori[16]. D'interesse, altresì, le tesi di laurea e dei master incentrate su tematiche afferenti all'intelligence, che potrebbero confluire in un archivio in rete di grande utilità. L'intelligence, insomma, sta ampliando il suo perimetro, per inglobare, accanto ai profili tradizionali, altre aree come i Big Data, la filosofia, gli scenari previsionali, le operazioni psicologiche, il metodo scientifico, la guerra delle informazioni. Si tratta, dal mio punto di vista[17], di una galassia in costante espansione che potrebbe richiedere presto utili iniziative di confronto e di coordinamento.

PROSPETTIVE DEGLI STUDI D'INTELLIGENCE IN ITALIA

I master e i corsi di laurea nelle università, i think tank e lo stimolo del Dis stanno contribuendo ad aprire interessanti prospettive di sviluppo per gli studi d'intelligence anche in Italia. Le dimensioni cyber ed economica sono quelle di maggior rilievo dato che i conflitti del futuro saranno prevalentemente di tale natura e si combatteranno attraverso il web e sulla base delle informazioni. Un'area di straordinario interesse è anche quella dell'intelligenza artificiale[18], il cui controllo, secondo Putin, potrebbe determinare il governo del mondo[19]. In stretta correlazione con l'esigenza di gestire una considerevole mole di informazioni, per estrarne valore al fine di supportare differenti tipi di analisi, assumerà sempre più rilievo la figura del *data scientist* che, in un certo senso, rappresenta la sintesi della formazione multidisciplinare propria dell'intelligence, che tende a selezionare le informazioni rilevanti per comprendere la realtà.

16. Gori – Germani 2011.

17. Con i miei scritti, incrocio l'intelligence con l'intelligenza artificiale, il dominio del Cyberspazio, la guerra delle informazioni e altri temi innovativi.

18. M. Caligiuri, L*a robotica nella trasformazione dell'ordine mondiale*:, <http://www.limesonline.com/cartaceo/la-rivoluzione-dellintelligence-cibernetica?prv=true> [10-11-2017].

19. M. Rovelli, P*utin sull'intelligenza artificiale*: «Chi sviluppa la migliore, governa il mondo» <http://www.corriere.it/tecnologia/economia-digitale/17_settembre_04/putin-sull-intelligenza-artificiale-chi-sviluppa-migliore-governa-mondo-musk-rilancia-l-allarme-c2a46c9c-916f-11e7-8332-148b1c29464d.shtml?refresh_ce-cp> [10-11-2017].

Pertanto, anche promuovendo la cultura della sicurezza nelle scuole, si potrebbero dedicare all'intelligence specifici corsi di laurea, ponendo le basi per lo sviluppo delle professioni per la sicurezza e per una consapevole partecipazione sociale. In tale ambito, l'aspetto pedagogico è centrale, tanto che negli Usa opera da anni un'associazione internazionale sull'educazione all'intelligence[20].

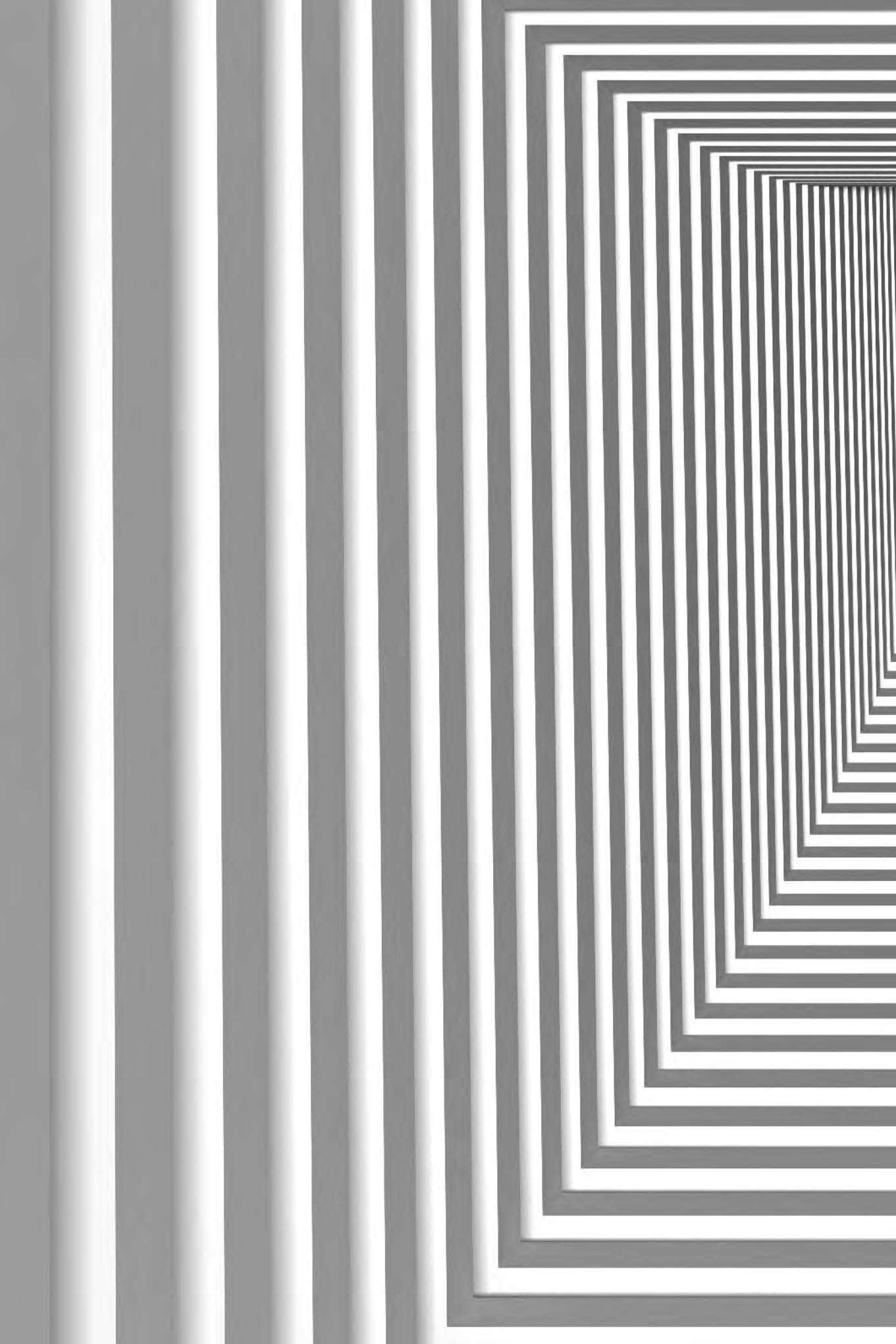
CONCLUSIONI

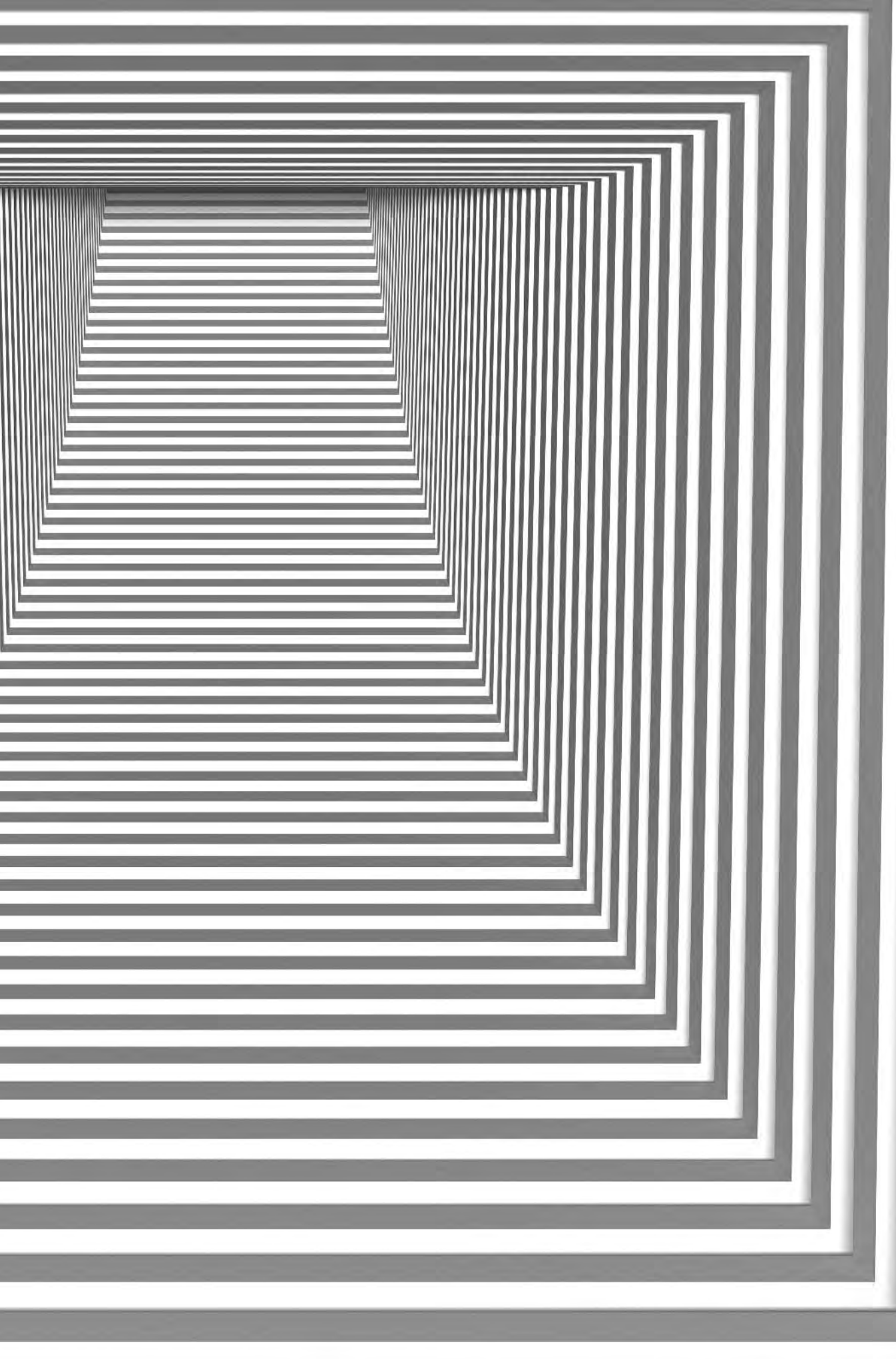
Nel 2003 auspicavo la nascita di una cultura italiana dell'intelligence[21]. Ora l'idea sta maturando. Ci sono ancora ritardi, in alcuni settori assai gravi, ma l'impegno si sta progressivamente ampliando. E poiché la società contemporanea «necessita sempre più della creazione di scenari di senso e quindi di 'scienziati' e sempre meno di 'spie'»[22], l'elevazione dell'intelligence a disciplina accademica può rispondere a un'effettiva esigenza della Nazione.

20. Si fa riferimento all'International Association for Intelligence Education: <http://www.iafie.org> [25-11-2017].
21. Caligiuri 2003, pp. 99-106.
22. Maniscalco 2016, p. 235.

BIBLIOGRAFIA

M. Caligiuri, *Università e intelligence. Un punto di vista italiano*, «Per Aspera ad Veritatem» 25 (2003).
S. De Prospo – R. Priore, *Chi manovrava le Brigate Rosse? Storia e misteri dell'Hyperion di Parigi, scuola di lingue e centrale del terrorismo internazionale*, Ponte alle Grazie, Milano 2001.
M. Franzinelli, *Il piano Solo. I servizi segreti, il centro-sinistra e il «golpe» del* 1964, Mondadori, Milano 2009.
U. Gori – L.S. Germani (a cura di), *Information warfare* 2011. *La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Franco Angeli, Milano 2011.
V. Ilari, *Storia militare della prima Repubblica* (1943-1993), Widerholdt Frères, Invorio 2009.
E. Macaluso, *I santuari. Mafia, massoneria e Servizi segreti: la triade che ha condizionato l'Italia*, Castelvecchi, Roma 2014.
M.L. Maniscalco, *Gli intelligence studies in Italia. A proposito del volume Intelligence e scienze umane. Una disciplina accademica per il* XXI *secolo*, «Democrazia e Sicurezza», 1 (2016).
C. Mosca et al., *I servizi di informazione e il segreto di Stato*, Giuffrè, Milano 2008.
S. Musco, *Storia dello spionaggio antico. Teoria e strategie di intelligence dagli albori alla caduta dell'Impero romano*, Aracne, Roma 2014.
N. Tranfaglia, *La «santissima trinità». Mafia, Vaticano e Servizi segreti all'assalto dell'Italia* 1943-1947, Bompiani, Milano 2011.
M. Valentini, *Sicurezza della Repubblica e democrazia costituzionale*, Editoriale Scientifica, Napoli 2017.





L'edizione Sicurezza è libertà. Intelligence e cultura della sicurezza a dieci anni dalla riforma è stata composta con i caratteri tipografici Novarese nelle versioni Regular, Italic, Bold, Semibold; Vinkel nelle versioni Thin, Extra Light, Light, Regular, Italic, Bold; Palatino nelle versioni Regular, Italic e Bold, ed è stampata su carta On Offset da 120 gr. delle Cartiere Polyedra, con inchiostri Novavit F100 delle Industrie KE.

On Offset è una carta naturale senza legno di qualità superiore prodotta con fibre vergini di eucalipto. On è un marchio Paperlin.

Finito di stampare in Italia
nel dicembre MMXVII