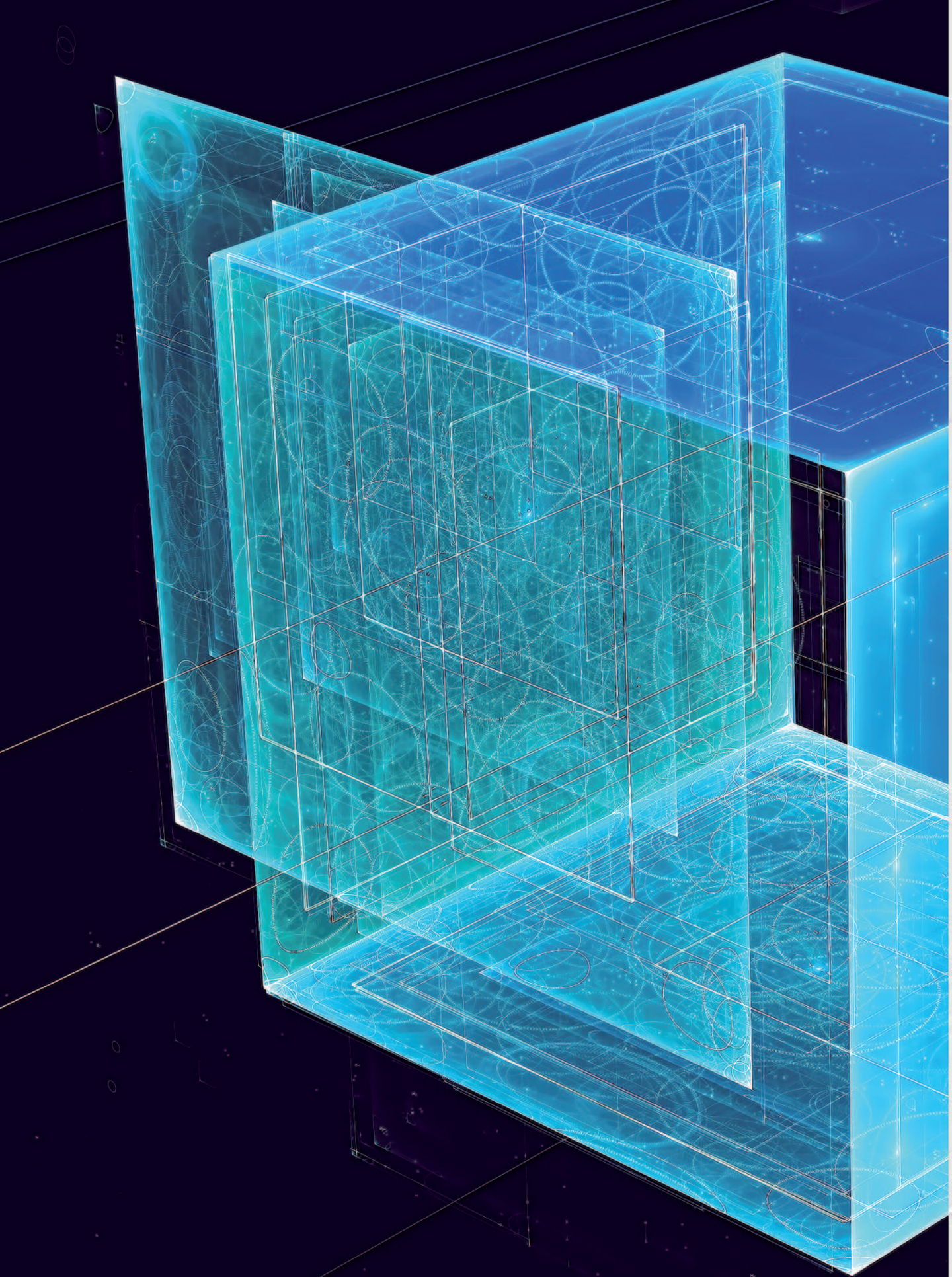
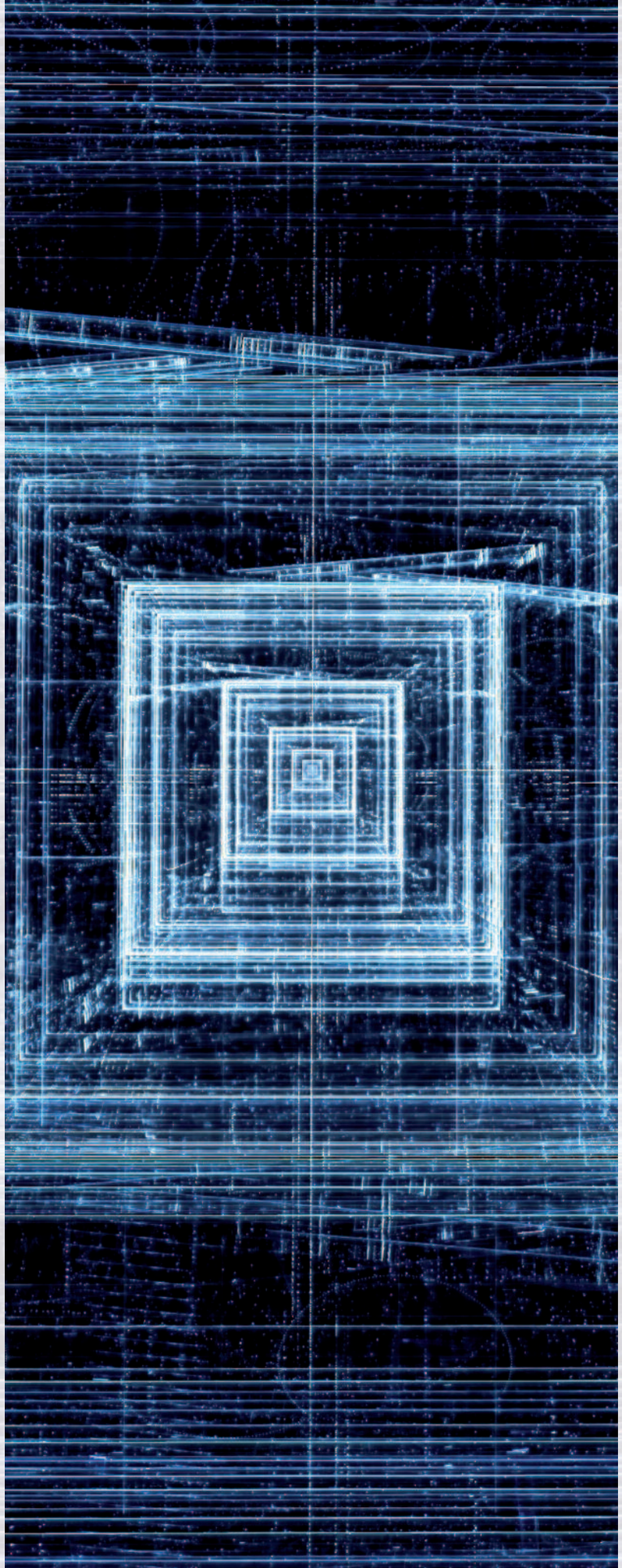


INTERESSE NAZIONALE, INTELLIGENCE E STRATEGIE NELL'ERA CIBERNETICA

Umberto Gori

Per esaminare in modo corretto il ruolo che la cyber intelligence (CybInt) può avere nella difesa dell'interesse nazionale (In) occorre preliminarmente definire in maniera univoca i due concetti. In particolare, si metteranno in risalto i vari livelli, tattico, operativo e strategico della CybInt e le varie articolazioni dell'In. Saranno esaminate le quattro categorie di bersagli nei confronti dei quali andrà applicata l'attività di CybInt: e cioè gli Stati presumibilmente avversari, gli Stati 'amici', i gruppi terroristici e quelli criminali. Per ognuna di tali categorie saranno individuati i comportamenti da tenere sotto controllo, nonché le modalità e gli strumenti di analisi. Tutto questo processo richiede una marcata collaborazione non solo a livello internazionale ma soprattutto tra settore pubblico e settore privato, superando rigidità e diffidenze.

In un incontro introdotto dall'allora Presidente del Casd, generale Carlo Jean, e riprodotto nel volume degli Atti (*Il sistema Italia – Gli interessi nazionali italiani nel nuovo scenario internazionale* 1997) a cura del CeMiSS, l'ambasciatore Ludovico Incisa di Camerana affermò che «intorno alla politica estera il modello italiano, nel suo insieme, si presenta come l'opposto del modello più efficiente, quello britannico. Basta pensare alla collaborazione esistente in Inghilterra, nell'ambito della classe dirigente, tra diplomazia, Servizi informativi (MI5 e MI6), mondo intellettuale (giornali e centri di ricerca) [...]. Questa collaborazione [...] si basa su una diffusa consapevolezza degli interessi del Paese. Il modello italiano viceversa è caratterizzato da una separazione netta tra diplomazia, intelligence, mondo intellettuale né si intravede un possibile cambiamento. L'ipotesi per ora più realistica e ragionevole è, a medio termine, un lavorìo culturale paziente, un'intelligence aperta, articolata su centri di studio e istituti di ricerca, su osservatori, in sintesi, in grado di segnalare e misurare il livello di rispondenza dei programmi operativi agli interessi nazionali».



Occorre dire che, a distanza di quasi vent'anni, molte cose sono cambiate in meglio, oltre che nella legislazione, per iniziativa del Dis che ha iniziato una costante interazione con le Università e gli Istituti di ricerca. Ne fa fede, fra l'altro, il recente volume I*ntelligence e interesse nazionale*, che raccoglie gli atti di due convegni della Società Italiana di Scienza Politica (Sisp), che ha visto gli interventi e la collaborazione di personalità di diversa estrazione, fra le quali i massimi vertici della comunità italiana d'intelligence.

È ormai opinione comune che solo la diffusione della cultura dell'intelligence possa consentire di superare le vecchie diffidenze nei confronti dei Servizi d'informazione e che in un sistema democratico l'intelligence abbia bisogno della collaborazione e delle competenze della società civile e dell'ambiente accademico.

Premesso che il concetto d'interesse nazionale si colloca nel contesto del paradigma realista delle relazioni internazionali, è da rilevare che durante tutto il periodo della Guerra fredda e fino al 1991 esso trovava la sua definizione nella difesa dalle minacce convenzionali e nucleari della controparte tramite l'adesione incondizionata, o quasi, alle alleanze e coalizioni occidentali.

Dopo il riemergere degli interessi particolaristici dei diversi Stati per il venir meno dell'assetto bipolare, la definizione è diventata più problematica, dato che per la concretezza del concetto occorre far riferimento ad altre minacce e ad altre vulnerabilità. Ancor più difficile il problema si poneva per l'Italia in quanto la sconfitta subita nella Seconda guerra mondiale e la narrativa del periodo fascista avevano reso tabù la locuzione 'interesse nazionale'. Un'ulteriore complicazione sorge per i localismi e le costruzioni sovranazionali che indeboliscono la ricerca della sicurezza di tipo Westfaliano.

L'Italia, per un periodo di oltre quarant'anni ha indirizzato la sua politica estera nella direttrice dei 'tre cerchi' concentrici – Europa, Nato, Nazioni Unite – che sono sopravvissuti anche se, per la verità, oggi non rispondono più completamente alle esigenze di tutela degli interessi nazionali. È sufficiente considerare l'odierna strategia degli Stati Uniti e automaticamente della Nato nei confronti della Russia, quella della Germania e di conseguenza dell'Unione Europea nei confronti dell'oleodotto South Stream e di altre delicate questioni nonché le iniziative autonome di Francia, Gran Bretagna e Stati Uniti contro la Libia per comprendere che tutto ciò è andato e va contro gli interessi del nostro Paese. In sintesi estrema, il multilateralismo, finora 'stella polare' dell'Italia, non sembra più in grado di assicurare protezione completa ai nostri legittimi interessi. Con ciò non vogliamo certo rinunciare alla speranza di una rinascita dello spirito di cooperazione internazionale e di integrazione a livello europeo, ma sta di fatto che, se vogliamo difendere nostre legittime posizioni, dobbiamo porci il problema di una strategia di lungo periodo, che a oggi non esiste.

Il perseguimento dell'interesse nazionale presuppone senso di appartenenza e coesione nazionale, equivalente, credo, a ciò che Luca Ansalone definisce come «percezione di sé'» («Formiche», 12 maggio 2012). Nello stesso tempo postula l'individuazione delle minacce odierne e delle vulnerabilità, che sono molto più numerose e diversificate di quelle di una volta. Ciò implica avere un'idea e una politica di sicurezza nazionale articolate secondo aree e problemi e declinate secondo priorità condivise anche con l'intelligence.

Una sintesi delle varie definizioni di sicurezza ci consente di dire che essa è assenza di minaccia ai valori fondamentali e assenza di paura che tali valori possano essere minacciati. È la cosiddetta dimensione oggettiva e soggettiva della sicurezza. Per una comunità politica i valori fondamentali sono il mantenimento della propria identità culturale, della propria integrità ordinamentale e del proprio benessere economico-sociale. Tali valori, in quanto vitali, non sono negoziabili. Per dirla in termini più concreti e più esaustivi, la sicurezza è definita dalla natura delle minacce[1].

Non ritengo sia necessario, opportuno e neanche possibile, come da qualcuno suggerito, inserire una definizione del concetto di interesse nazionale fra le norme costituzionali: in primo luogo perché tale definizione sarebbe frutto di compromessi politico-ideologici e poi perché il concetto, oltre a essere valutabile oggettivamente in base alla collocazione del Paese nello spazio fisico e, parzialmente, in base alla sua storia politica e culturale e perciò sostanzialmente stabile, ha una dimensione soggettiva e mutevole secondo le maggioranze politiche e le evoluzioni della politica internazionale[2]. Tanto è vero che, nel testo della Costituzione del 1948, il concetto, poi espunto con legge costituzionale 18 ottobre 2001, n. 3, appare solo fugacemente negli articoli 117 e 127, senza, peraltro, una definizione dei suoi contenuti. Del resto, neanche nel G*lossario* del Dis sul linguaggio degli organismi informativi è dato riscontrare una tale definizione.

1. Per una definizione del concetto di sicurezza secondo i diversi paradigmi interpretativi delle relazioni internazionali, vedi Gori 2004, pp. 155 ss.
2. A*mplius*, in Gori 2015, p. 608. Vedi anche Gori 1997, pp. 148-160.

Riterrei sufficiente un minimo di buon senso e di buona volontà per convenire su alcuni dei contenuti dell'interesse nazionale, con riferimento a quella parte di essi che sono connaturati alla dimensione oggettiva del concetto. Per il resto, sembra logico che siano il Parlamento e il Governo in carica, liberamente eletti, ad avere il diritto-dovere di elaborare una strategia coerente con le mutevoli esigenze della realtà internazionale. Una strategia rigorosa, che io interpreto come un piano d'azione completo, nel senso che devono essere esplorate tutte le possibili soluzioni di una certa situazione con tutte le loro relative conseguenze, attribuendo a ogni soluzione possibile, e quindi a ogni relativa conseguenza, un quantum di utilità. Qui entra in gioco, in misura determinante, l'apporto dell'intelligence e dei suoi scenari.

È altrettanto ovvio che l'interpretazione dell'interesse nazionale deve essere compatibile, pena l'irrilevanza e il velleitarismo, con il livello dei propri fattori di potenza, materiali e immateriali. L'avvento dell'Ict, la tendenza dei conflitti a essere sempre più virtuali e la conseguente emersione della noosfera causano un mutamento nelle basi del potere statuale che dipende sempre meno dal territorio, dalla potenza militare e dalle risorse naturali e sempre di più dalle conoscenze e dalle idee che costituiscono, pertanto, un potenziale valido aiuto per una media Potenza come l'Italia. Dopo la Rivoluzione negli affari militari (Rma) gli Stati assistono, infatti, anche a un progressivo mutamento nella prassi e nelle regole della diplomazia in direzione di un sempre maggiore impiego del soft power più utilizzabile da parte di uno Stato di medie dimensioni, a condizione di avere, appunto, una strategia.

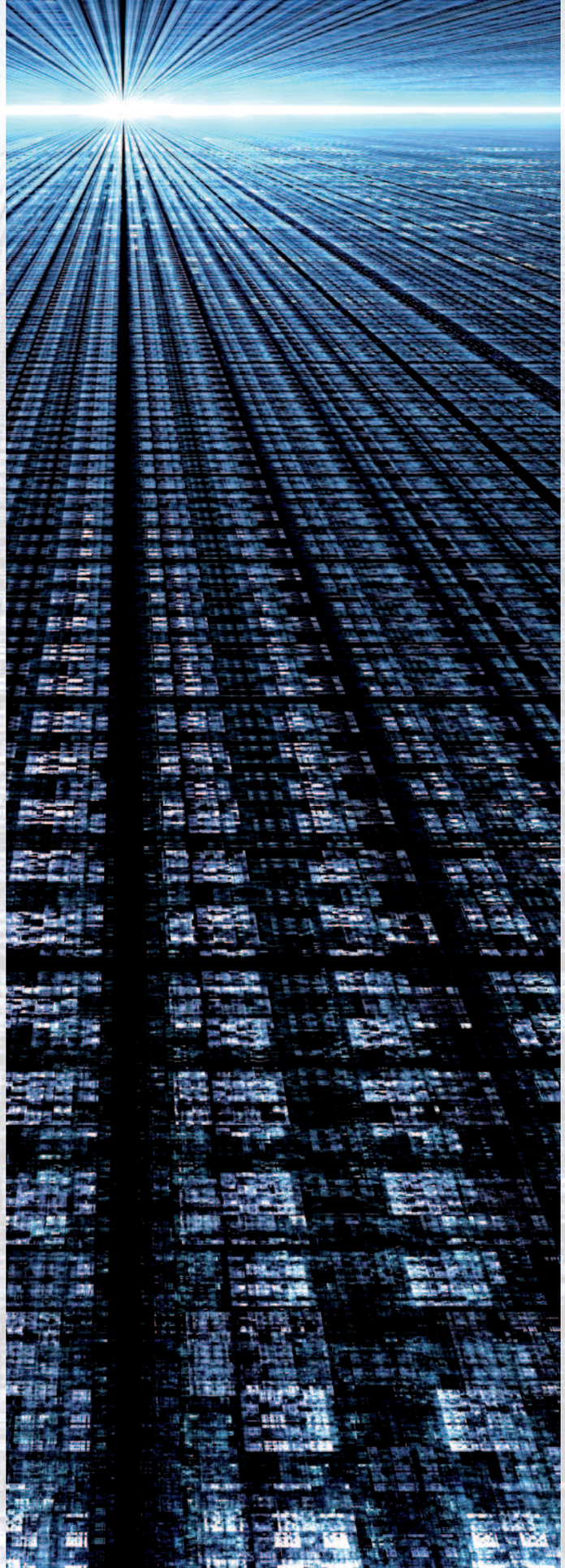
Anche l'interesse nazionale sta cambiando: esso è visto sempre più in termini di competitività e competizione economica, di influenza culturale e regionale. Occorre però avere un forte know-how tecnologico e la padronanza di strumenti Ict per poterlo perseguire. L'era cibernetica provoca dei mutamenti anche nelle strategie da utilizzare nei confronti delle minacce di ogni tipo. Mi riferisco, in primo luogo, all'evoluzione negli strumenti dell'intelligence che, per operare nello spazio virtuale, diventa cyber intelligence. Qui occorre definire quanto più esattamente possibile il concetto in questione, anche perché, in campo cibernetico, il lessico lascia a desiderare e non sempre a un termine corrisponde un solo significato[3].

3. Per i motivi che rendono necessaria l'armonizzazione delle definizioni dei concetti utilizzati nel settore, vedi Gori 2012, pp. 13-18.

Definiamo la cyber intelligence come il complesso di attività programmate e applicate per identificare, seguire, misurare e monitorare informazioni sulle minacce digitali, nonché dati sulle intenzioni e sulle attività di entità avversarie o in competizione. Tali attività, che si svolgono con strumenti cibernetici nel cyberspazio, a differenza delle altre forme di intelligence hanno la particolarità di condividerne con lo spazio fisico l'uso di HumInt, l'intelligenza umana che si manifesta, in misura ancor più accentuata, per lo meno nella fase di pianificazione, nella network intelligence (NetInt), basata su concetti e princìpi di programmi tipo Deep Packet Inspection (Dpi), capaci di identificare in tempo reale i protocolli utilizzati e i metadati (dati sui dati) ed estrarre i contenuti informativi che corrono sulla rete, analizzandone nel contempo le relazioni reciproche. Questi programmi, così potenti e utili al punto che molti di essi sono classificati, costituiscono un formidabile strumento euristico, potendo contribuire all'attività di *early warning* e di previsione inerente a ogni forma di intelligence.

Ad avviso di chi scrive, la cyber intelligence si pone al vertice dei vari tipi di intelligence in quanto adotta un approccio globale e multidisciplinare di integrazione e fusione delle informazioni. La correlazione di queste ultime rappresenta un netto vantaggio per i soggetti, pubblici e privati, che devono ormai analizzare e processare quantità sterminate di dati (*big data*) e di metadati. In futuro, la B*ig Data* A*nalytics* permetterà controlli automatizzati in tempo reale e capacità previsionali con l'individuazione di correlazioni nascoste. Tutto ciò offre alle analisi d'intelligence delle possibilità incommensurabilmente superiori. Nello stesso tempo, questa proliferazione incessante di dati potrà essere all'origine di seri problemi per quanto riguarda la democrazia e la privacy, ma è una questione che esula dalla presente trattazione.

In secondo luogo, mi riferisco alla cultura strategica più adatta a essere impiegata nello spazio virtuale. Due sono le strategie che si contrappongono: quella occidentale, che si rifà a Clausewitz, e quella orientale – in particolare, cinese – originata dall'antichissimo insegnamento di Sun Tzu. Le idee di Clausewitz erano e sono coerenti con la realtà di un contesto internazionale caratterizzato da Stati sovrani, divisi da confini politici, risultato dell'esito di precedenti conflitti, che si combattevano con armi cinetiche. La guerra, per il generale prussiano, è un atto di forza, il massimo della forza, per costringere il nemico alla sottomissione. È un 'gioco' a somma zero (come, ad esempio, il gioco degli scacchi). La tecnologia, e in



particolare la Ict, ha sconvolto tutto. Il cyberspazio non ha confini e la stragrande maggioranza delle strutture cibernetiche sono di proprietà privata. E la forza non può essere usata quando il nemico è invisibile o ignoto (problema dell'attribuzione).

L'insegnamento di Sun Tzu, invece, enfatizza l'importanza dell'uso dell'intelligence e dell'inganno. Per l'antico stratega, il condottiero più bravo è quello che vince le guerre senza combattere e senza causare perdite di vite umane nel proprio esercito e in quello avversario. L'obiettivo non è il bersaglio, ma la mente del nemico e il quadro strategico può mutare sfruttando il potenziale insito nelle situazioni e circostanze e utilizzando vari stratagemmi. Il gioco di società di riferimento è il *go*, basato su una scacchiera dove interagiscono pietre nere e bianche di eguale importanza che rappresentano lo *yin* e lo *yang*, elementi complementari e interdipendenti, che penetrano nel territorio altrui in un movimento tranquillo simile a quello dell'acqua. In questo gioco, come in guerra, è quasi impossibile vincere al cento per cento e azioni troppo aggressive possono portare al disastro. Il fine ultimo è di acquisire parti sempre più estese del territorio in modo da assicurarsi, col tempo, una solida posizione strategica. È ciò che sta facendo la Cina con le isole artificiali nell'oceano Pacifico, perseguendo una strategia di lungo periodo al posto della forza. In breve, per il pensiero militare cinese la strategia deve sfruttare la naturale tendenza delle cose. A differenza dal pensiero militare occidentale – che vede l'ambiente strategico secondo una visione Newtoniana con precise leggi fisiche e sfrutta i princìpi di massa e manovra sullo *Schwerpunkt* – il pensiero orientale prende in considerazione la relazione fra le cose, e cioè il network, la rete, che è poi la struttura stessa del mondo cibernetico. Ciò significa che l'approccio orientale è più adatto a gestire la conflittualità non-cinetica, mentre quello occidentale riesce meglio a risolvere i conflitti che richiedano l'impiego di strumenti bellici tradizionali.

In terzo luogo, mi riferisco alle manovre cibernetiche. Dopo che la tecnologia ha aggiunto una quinta dimensione agli ambiti della conflittualità, anche il concetto tradizionale di manovra – visto come la disposizione delle forze per assicurare vantaggi di posizione prima e/o durante azioni di scontro o di combattimento – ha subìto modifiche nel cyberspazio. Mentre nei domìni tradizionali della conflittualità sono le forze a essere movimentate, nel cyberspazio sono le basi da cui proviene l'attacco a essere spostate. Ed è questo uno dei motivi che crea il problema dell'attribuzione. Inoltre, le manovre cibernetiche offensive, che consistono nell'applicare un software o algoritmo per acquisire, compromettere, distruggere risorse computazionali e informative, hanno – a differenza delle manovre cinetiche – le seguenti caratteristiche: raggiungono l'obiettivo istantaneamente; sono invisibili; hanno un raggio d'azione illimitato; possono acquisire il controllo di sistemi altri dai propri; possono compromettere i sistemi di comando e controllo dell'avversario, sia direttamente che indirettamente, fornendo dati falsi o manipolati ecc.

Anche le manovre cibernetiche difensive hanno connotazioni particolari come, ad esempio, la difesa con obiettivo mobile (*Moving Target Defense*) o quella che si avvale di *honeypots*. Inoltre, le manovre cibernetiche sono usate anche nei confronti di Paesi amici e alleati; manovre che spesso, impunite nel cyberspazio, sarebbero considerate atti di guerra in ambiente convenzionale.

Infine, le caratteristiche dell'era cibernetica restringono drasticamente i tempi del ciclo Osservare, Orientare, Decidere e Agire (Ooda), con il risultato di dover prendere decisioni sotto stress e quindi non ottimali, o addirittura a impatto negativo, unico rimedio essendo decisioni preprogrammate in risposta a fattispecie diversificate di attacchi.

Moltissime altre considerazioni potrebbero essere fatte, ad esempio, sulla resilienza, sulla *deterrence by denial*, o sulla Network Centric Warfare e le sue declinazioni europee, ma la trattazione si allungherebbe in misura indebita[4]. Si auspica che quanto detto possa costituire motivo sufficiente di riflessione

G

4. Su alcuni di questi punti, vedi Gori 2014, pp. 5-29.

BIBLIOGRAFIA MINIMA

U. Gori, *Il sistema Italia. Gli interessi nazionali italiani nel nuovo scenario internazionale*, Franco Angeli, Milano 1997, pp.148-160.

U. Gori, *Lezioni di Relazioni Internazionali*, Cedam, Padova 2004 (II edizione).

U. Gori, *Riflessioni propedeutiche alla cyber intelligence*, in Gori – Germani (a cura di) 2012, pp. 13-18.

U. Gori – L.S. Germani (a cura di), *La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Franco Angeli, Milano 2012.

U. Gori, *Le nuove minacce cyber*, in «Informazioni della Difesa» (2014), pp. 5-29.

U. Gori, *Intelligence e interesse nazionale. A mo' di prefazione*, in Gori – Martino 2015.

U. Gori – L. Martino (a cura di), *Intelligence e interesse nazionale*, Aracne, Ariccia (Roma) 2015.