Minacce alla sicurezza

Cyberspazio e nuove sfide

GIANLUCA ANSALONE

Lo spazio cibernetico è sempre più il luogo della competizione strategica. La sua accessibilità a basso costo e la pervasività lo rendono il luogo ideale per la proliferazione di minacce vecchie e nuove.
Dalla militarizzazione all'attività delle reti criminali, il cybermondo rischia di essere il luogo del caos assoluto, se non adeguatamente governato da regole condivise. Per gli operatori di intelligence la tutela della sicurezza nazionale dalle minacce cibernetiche è una nuova, importante sfida.

Il XXI secolo si è aperto all'insegna di un marcato processo di distribuzione del potere. La moltiplicazione dei centri di comando e di influenza, come conseguenza della globalizzazione, sta erodendo la tradizionale sovranità dello Stato-Nazione, promuovendo attori non statali al rango di protagonisti delle relazioni internazionali. A favorire tale mutamento è, soprattutto, la moltiplicazione delle reti informatiche e degli strumenti di comunicazione.

La tecnologia è stata a lungo uno strumento al servizio del consolidamento delle gerarchie geopolitiche mondiali. Lo Stato-Nazione in grado di battere moneta per finanziare la sofisticazione dei suoi armamenti e la capacità di muovere guerra poteva imporre una supremazia relativa più o meno duratura. La moderna tecnologia legata alle Reti, soprattutto in virtù dei suoi bassi costi di acquisizione e di utilizzo, sta favorendo invece il decentramento geopolitico attraverso l'universalizzazione virtuale dell'uso del potere.

Internet, fin dal suo debutto nel 1989, ha rivoluzionato la vita degli Stati, delle imprese e dei cittadini. Sarebbe impossibile immaginare oggi un mondo senza la Rete.

Nel 1993 esistevano circa 50 siti Internet registrati in tutto il mondo. Nel 2010, soltanto in Cina, si sono registrati 400 milioni di nuovi utenti. Nel 1980 le telefonate trasmesse dai tradizionali fili di rame potevano 'traspor-

tare' appena una pagina di informazioni al secondo; oggi la fibra ottica è in grado di trasmettere 90.000 volumi in un secondo.

Ma questa rivoluzione ha un suo costo. Sul Web corre di tutto: reti criminali transnazionali, hackers, terroristi. Ma anche governi o imprese interessate a sottrarre al nemico o al concorrente il vantaggio competitivo di cui godono.

La ricerca del primato si sta rapidamente spostando sulla Rete e, presto o tardi, la collisione tra interessi potrebbe condurre ad una vera e propria guerra combattuta via internet.

Esistono già casi emblematici in tal senso, come l'attacco informatico subìto dall'Estonia nel 2007, Paese che vanta il maggior numero di operatori e di istituzioni connesse in Rete e che per diverse ore venne letteralmente 'spento' nei suoi servizi essenziali, dalla fornitura di acqua potabile alle transazioni bancarie. O quello subìto dalla Georgia nell'agosto del 2008, in concomitanza con l'avanzata dei carri armati russi, di fronte alla quale i siti internet della Presidenza della Repubblica e di tutti i Ministeri chiave del Paese vennero oscurati.

Lo spazio cibernetico è un nuovo, fondamentale, campo di battaglia e di competizione economica e geopolitica.

E, come accade in tutte le competizioni, ci saranno attori destinati a dominare ed altri destinati a soccombere.

Sotto questo profilo, gli Stati Uniti hanno molti più concorrenti e potenziali nemici di quanto non accada per altri tradizionali domìni, da quello economico a quello militare. Il Presidente Obama ha stimato in 1.000 miliardi di dollari la perdita netta nel 2009 per le aziende tecnologiche americane a causa di attacchi informatici, tra danni causati ai sistemi e sottrazione di marchi o brevetti. Nel suo consueto rapporto annuale al Congresso, il Direttore nazionale dell'Intelligence americana ha indicato la cyberguerra al primo posto tra le minacce alla sicurezza nazionale: essa è in grado di erodere il vantaggio competitivo degli Stati Uniti annullando gli impatti delle innovazioni e incidendo, addirittura, sugli stili di vita dei cittadini e delle imprese, costretti probabilmente in un prossimo futuro a rinunciare ad una porzione della loro libertà sul Web per mettere al riparo il Paese da danni più gravi.

Paesi come la Russia, Israele, l'Iran o la Corea del Nord sono già in grado di dispiegare armate di cybercombattenti, pronti a scatenare attacchi asimmetrici per sabotare le reti di comunicazione e le infrastrutture critiche nazionali, mettendo in ginocchio gli avversari senza sparare nemmeno un colpo.

I due 'vicini scomodi', India e Pakistan, si scambiano continue scaramucce informatiche.

Insomma: economisti, analisti, operatori di sicurezza e governanti dovranno misurarsi sempre di più con una dimensione virtuale della politica e dell'economia.

Una dimensione ricca di incognite ma non del tutto oscura. Esistono, infatti, alcune considerazioni che si possono svolgere in merito alle caratteristiche di questo nuovo 'cybermondo'.

Primo: esso è in costante evoluzione. La pervasività della Rete corre di pari passo con lo sviluppo delle infrastrutture informatiche e l'ampiamento dei rapporti politici, commerciali ed economici tra Stati.

Secondo: quando l'interdipendenza non è governata genera naturalmente vulnerabilità. Nel caso delle reti di internet si tratta di quelle minacce cui si è già fatto cenno, di carattere individuale o statuale. In tal senso, accanto ai domìni tradizionali di cielo, mare, terra e spazio il 'cybermondo' può essere utilizzato come uno strumento strategico. Il potere cibernetico può essere usato, infatti, in pace e in guerra; è 'coperto', relativamente economico e consente sia l'offesa che la difesa.

Terzo: il cyberspazio non è che l'ultima evoluzione di un percorso tecnologico iniziato secoli fa. La macchina da stampa, il telegrafo, il telefono e le tecnologie di comunicazione senza fili hanno altrettanto rivoluzionato le società e le economie. Ma, a differenza di tutti i suoi predecessori, il cyberspazio non è solo uno strumento di comunicazione ma un mezzo per creare, accumulare e manipolare informazioni.

Per tutte queste ragioni, il potere cibernetico è tatticamente e tecnicamente distinto dagli altri strumenti del potere militare ma non ne è estraneo. Al contrario, esso allarga lo spettro degli attori e delle vulnerabilità strategiche.

Ad un'estremità di questo spettro c'è l'individuo, attore primario e utente privilegiato della Rete.

Per secoli, la reputazione individuale è stata un caposaldo della convivenza civile; con il tempo, essa si è trasferita dal chiuso delle mura domestiche alla piazza fino ad essere, oggi, in balìa dell'agorà virtuale, esposta a pericoli di manipolazione, discredito, offesa.

Le reti criminali e di spionaggio rappresentano un ulteriore sottobosco oscuro del mondo cibernetico. Di solito è il crimine organizzato ad innovare formule e tecniche per aprire una breccia nei sistemi informatici, al fine ovviamente di trarne un profitto.

Le reti organizzate di spionaggio – statale e industriale – di solito seguono, utilizzando quei medesimi varchi.

La scarsa alfabetizzazione informatica e digitale degli utenti è la principale causa della relativa facilità con cui hackers ben addestrati possono penetrare i sistemi di singoli utenti o di grandi società.

I nostri dati vengono costantemente trasferiti da laptop o chiavette USB attraverso reti wireless e conservati in 'nuvole' che si trovano chi sa dove.

Ciò non fa che moltiplicare i possibili punti di dispersione e i bersagli dei potenziali attacchi. Paradossalmente, i dati sono oggi meglio tutelati nell'archivio cartaceo di un pubblico ufficiale zelante che sul disco rigido di un PC.

Anche gli Stati stanno utilizzando lo spazio cibernetico in maniera sempre più strategica.

Esso garantisce, infatti, risultati altrettanto efficaci di strumenti militari convenzionali ma ad una frazione dei costi. Il che, in un momento di austerità generale nei bilanci pubblici, rappresenta una decisa e sensibile innovazione.

La creazione in seno al Pentagono del primo Cyber-Command, forte di ben 9000 uomini, è la principale espressione di questa nuova tendenza.

Il fatto che il cyberspazio non abbia confini e non conosca sovranità implica la necessità di azioni immediate per scongiurare il pericolo di una cyber-anarchia, la militarizzazione di questo spazio, la possibilità per gli Stati di ospitare o sponsorizzare reti criminali, terroristiche o di spionaggio via Web.

Fino ad oggi, almeno sei diverse agenzie delle Nazioni Unite hanno provato ad intraprendere un percorso di codifica di regole condivise, per una governance globale della Rete.

I risultati, però, sono scarsi e deludenti. Molti governi occidentali considerano l'accesso alla Rete e la sua assoluta libertà addirittura come un diritto umano fondamentale.

Secondo l'UNESCO, il diritto d'assemblea via web sarebbe equiparabile alle previsioni dell'articolo 19 della Dichiarazione dei diritti dell'uomo. Dall'altro lato vi sono governi che, pur non essendo pregiudizialmente contrari ad un accordo internazionale, ritengono che la Rete debba essere vigilata e che l'accesso ad Internet possa essere legittimamente impedito se mette a repentaglio la stabilità politica o l'ordine pubblico. Secondo questi governi, ciascuno Stato deve avere il diritto di controllare contenuto e accessi all'interno del proprio spazio internet 'sovrano'.

Queste due posizioni rimangono per ora distanti ed inconciliabili. E i governi non sono gli unici attori in campo: movimenti di opinione, partiti politici, entità come Anonymous sono – e saranno sempre più – in grado di influenzare il dibattito relativo alla Rete e, quindi, la possibilità che si arrivi presto ad un codice di condotta internazionale.

In molti altri settori stiamo drammaticamente sperimentando le conseguenze di un'assenza di governance condivisa, come nel caso degli enormi squilibri finanziari e degli effetti dei debiti sovrani. Nel mondo della globalizzazione i problemi e le minacce sono comuni e, allo stesso modo, richiedono ricette e soluzioni condivise.

Le stesse considerazioni valgono per le tecnologie dell'informazione. Occorre fare in modo che la globalizzazione diventi sempre più un 'win-win game' e che non lasci una pericolosa distinzione tra vincitori e vinti.

Nel pieno della Guerra Fredda, subito dopo il picco di tensione per la prospettiva di un Olocausto nucleare, Stati Uniti e Unione Sovietica avviarono un processo di progressiva distensione, basato sullo smantellamento di una parte dei rispettivi arsenali atomici e la limitazione dei cosiddetti armamenti strategici.

Oggi è necessario quello stesso spirito ed una iniziativa analoga in grado di prevenire la caotica militarizzazione del cyberspazio e la proliferazione di minacce asimmetriche attraverso le tecnologie di Rete.

Dei tentativi – finora vani – messi in campo dalle Nazioni Unite si è già fatto cenno.

Di recente, la NATO, prima nel corso del Summit di Lisbona quindi nel più recente Summit di Chicago, ha messo al centro dell'attenzione gli aspetti della sicurezza legati al cyberspazio. Ciò ha avuto il merito di rilanciare con forza l'attualità e la vitalità del legame transatlantico. La cooperazione tra le due sponde dell'Atlantico si va allargando dai campi tradizionali a quelli più innovativi in una maniera e con un'efficacia che è difficile eguagliare per qualsiasi altro foro multilaterale.

Non si tratta di reinventare la ruota. Esistono buone pratiche già consolidate in campo diplomatico, economico e sociale che possono essere applicate anche a questo nuovo settore strategico.

Per il momento, lo spazio cibernetico rimane però una terra nullius. È esattamente l'assenza di regole che rende questo spazio appetibile per perseguire scopi criminali o aggressivi in termini politici, economici, sociali o religiosi.

Il luogo della virtualità assumerà, quindi, nei prossimi anni caratteristiche di minaccia concreta alla sicurezza internazionale e a quella delle singole Nazioni.

Il contributo di decisori politici, apparati di intelligence e industrie dovrà essere unitario e mirare alla promozione di un progetto globale che sia in grado di conciliare libertà di utilizzo delle Reti e sicurezza.

Per l'Italia si tratta di una straordinaria opportunità: la perdita della rendita di posizione geopolitica, seguìta alla fine della Guerra Fredda ha comportato, per il nostro Paese, un gap notevole in termini di innovazione strategica.

Sul fronte della sicurezza cibernetica disponiamo però di asset rilevanti. Si tratta, forti anche della nostra piena partecipazione al modello di sicurezza suggerito dalla NATO sia a Lisbona che a Chicago, di immaginare un'architettura centralizzata ed efficiente per la sicurezza delle nostre infrastrutture critiche. La nostra proiezione mediterranea renderebbe una tale capacità preziosa per l'intera comunità euroatlantica.

Ma, giova ricordarlo, per raggiungere un tale obiettivo è necessario promuovere con urgenza una riflessione approfondita sulla compatibilità tra risorse disponibili e obiettivi strategici. In altre parole: l'Italia non dispone di un documento di sicurezza nazionale condiviso, attraverso il quale indi-

viduare priorità di spesa e di intervento per confermare un ruolo all'altezza delle sfide che attraversano questo inizio di XXI secolo.

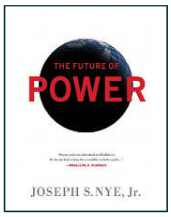
Ci si dovrà arrivare, auspicabilmente, presto. Ma di fronte alla portata di una tale sfida, le forze della sicurezza sono da subito chiamate ad un'autentica rivoluzione culturale, prima che operativa.

Come per il contrasto a numerose altre minacce emerse dopo la fine dell'equilibrio bipolare, le parole d'ordine sono: coordinamento e chiarezza delle linee di comando e controllo. Soprattutto, tra le diverse realtà investigative e tra le agenzie che, anche nel nostro Paese, si occupano a vario titolo di protezione delle infrastrutture critiche. Ma perché la minaccia legata al cyberspazio non sia sottovalutata, è anche necessario che i grandi operatori economici, che a pieno titolo costituiscono una parte essenziale del sistema-Paese, siano coinvolti nel processo di definizione di adeguate misure di tutela della sicurezza e si attrezzino, essi stessi, con risorse e professionalità per essere la prima linea della difesa da potenziali attacchi.

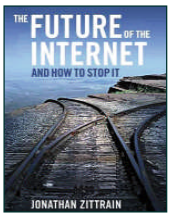
Fino ad oggi, grazie anche all'attività svolta dal Comitato Parlamentare per la Sicurezza della Repubblica (CoPaSiR) e dalla pronta disponibilità del Governo ad una stretta collaborazione, sono già stati raggiunti importanti risultati. Il cyberspazio e le sue implicazioni per la sicurezza nazionale sono al cuore degli interventi normativi di riassetto organico e tematico volti a rafforzare l'operatività e la piena rispondenza tra le capacità del sistema di sicurezza e la natura delle nuove minacce.

L'attribuzione di un ruolo di coordinamento al Dipartimento Informazioni per la Sicurezza (DIS) in materia di analisi e contrasto alle minacce cibernetiche è un passaggio essenziale; pur salvaguardando le specificità operative delle due Agenzie, esso servirà a garantire unitarietà di intenti e una pianificazione strategica adeguata ma, anche, a ridurre duplicazioni e sovrapposizioni che, in una matassa così difficile da dipanare, come quella della Rete Internet, rappresenterebbero un limite esiziale all'efficacia delle politiche messe in campo.

Per approfondimenti l'autore suggerisce...



The Future of Power
Autore: Nye Joseph jr
Editore: Public Affairs - New York, 2011



The Future of the Internet
Autore: Zittrain Jonathan
Editore: Yale University Press, 2008