Scenari conflittuali, guerra elettronica e minacce nel cyber-space: sfide strategiche e organizzative nei futuri ambienti di combattimento

di Francesca Castaldo

1. Mutamenti di scenario belliconello spazio cibernetico: dalle capacità quasi simmetriche ai metodi non convenzionali

Gli interventi della NATO sono tradizionalmente avvenuti in caso di conflitti interstatali combattuti da attori statali aventi reciproche possibilità di attaccare con capacità quasi simmetriche (queste potevano includere i missili balistici, gli aerei anche pilotati remotamente, la guerra elettronica, le capacità cosiddette 'cyber' e anche gli armamenti anti-satellite).

Nelle ultime decadi lo scenario bellico si è reso via via più complesso per gli alleati, i quali, oltre che Stati, potevano trovarsi a dover fronteggiare anche entità non sovrane, esercitanti un significativo potere economico, politico, sociale come pure un'influenza a livello nazionale o persino internazionale.

La situazione attuale è molto articolata in quanto attori statali forniscono talvolta armamento avanzato ad attori diversi dagli Stati. Le implicazioni per i Paesi dell'Alleanza sono, così, esacerbate dalla proliferazione di armamento e tecnologie sofisticate anche tra attori non statali, come le organizzazioni terroristiche.

Predire gli scenari delle guerre del futuro è oggi molto difficile. Nondimeno, diversi studiosi ed esperti della materia sono concordi

nell'assumere che gli avversari del futuro avranno le *capabilities* e gli intenti di opporsi a, o persino distruggere, le operazioni (non solo aeree) della NATO[1]. Questi possederanno un livello tecnologico simile e rappresenteranno, conseguentemente, una seria minaccia per le Forze Alleate [W.J. Lynn, 2010; P.Rosenzweig, 2013].

In ambienti bellici imprevedibili gli esperti ipotizzano, inoltre, che in un futuro non lontano un determinato antagonista della Nato tenderà ad evitare "le forze" dell'Alleanza e a gravitare attraverso le aree di debolezza percepita [W.J. Lynn, 2010].

Allo stesso modo,è sempre più probabile che un avversario eviterà le operazioni militari convenzionali e attaccherà in modi considerati irregolari o asimmetrici [Q. Liang, W.Xiangsui, 2001].

Del resto, già oggi nemici sofisticati possono usare capacità belliche considerate asimmetriche, includendo guerra elettronica e cibernetica, al pari dei missili balistici e da crociera avanzati o di altri sofisticati metodi bellici [F. Castaldo, 2018a].

Negli ultimi anni v'è stato un sempre maggiore interesse per i conflitti attuati con mezzi 'non convenzionali' e, in particolare, tramite attacchi informatici in un'arena nota come "spazio cibernetico" (Cyber-Space). Esistono, in realtà, diverse concezioni dello spazio cibernetico, che è ancora, in parte, una frontiera inesplorata nell'ambito delle relazioni internazionali [J. Adams, 2001].

In questo lavoro faremo riferimento alla tradizione occidentale dominante, quella statunitense, che guarda al Cyberspace come ad una 'big matrix', una matrice organizzata di relazioni codificate e funzionali. In questa visione, di una tecnologia in grado di organizzare le relazioni, è implicita, oltre al tipico funzionalismo americano, la

[1] Le considerazioni fin qui espresse valgono anche per altre alleanze, quali le coalizioni internazionali che hanno operato nei più recenti teatri operativi.

'difesa dai nemici alle porte', che assediano la matrice o si sottraggono ad essa, in entrambi i casi coltivando intenzioni bellicose verso la roccaforte ben strutturata e organizzata, cui tocca, appunto, difendersi (Cyber-War).

Lo scenario di mantenimento dello *status quo ante*, incarnato dall'establishment digitale Usa, lascia intravedere forze capitalistiche che verranno a rompere gli equilibri odierni. Forze e capacità diffuse, frammentate, che gli esperti del settore e gli strateghi militari devono cominciare a coglieregià oggi nello scacchiere globale.

2. Le minacce nel cyberspace

Il cyberspace, dicevamo sopra,è sempre più teatro di conflitti attuati con mezzi non convenzionali. Tra questi, gli attacchi informatici di tipo intenzionale hanno, generalmente, come bersaglio la rete, i nodi o gli utenti, e vengono eseguiti iniettando rumore o *bit* di informazioni oppure manipolando i protocolli di comunicazione. Esistono, però, all'interno della rete anche attacchi che sfruttano le radiazioni e lo spettro elettromagnetico per disturbare o compromettere il funzionamento di un sistema, sfruttando cosi tecniche e risorse provenienti dalla guerra elettronica [Q. Liang, W.Xiangsui, 2001].

I sistemi utilizzati dalle Forze Armate usano per lo più lo spettro elettromagnetico in maniera rilevante e ciò li rende suscettibili alle minacce tipiche di questo ambiente, come l'ascolto passivo del canale per intercettazione di pacchetti comunicazione (*packetinjection*)[2],

[2] Il 'packetinjection' è un processo con il quale si vuole interferire in una connessione di retestabilita tra due utenti, costruendo ed iniettando 'pacchetti' e facendoli passare come parte del normale flusso di dati. Questo metodoconsente ad un'ignota terza parte di sabotare e/o intercettare elementi di comunicazione, appunto 'pac-

l'identificazione di nodi critici, il *trafficanalysis* nel caso di reti cifrate [A. Teti, 2018].

In termini generali, la minaccia *cyber* è particolarmente elevata per tutti quei sistemi connessi all'acquisizione delle informazioni - come i sistemi meteorologici, i droni per applicazioni civili, i sistemi satellitari, i radar per le comunicazioni civili e militari - e alla movimentazione fisica di persone e merci o, più in generale, al supporto al trasporto - come, ad esempio, i sistemi di controllo del traffico aereo e navale [J. Andress, S.Winterfeld, 2014].

In relazione ai primi, l'utilizzo intensivo di reti di comunicazione e di tecnologie digitali per il controllo e lo scambio di grandi quantità di informazioni rende, di per sé, questi sistemi particolarmente esposti agli attacchi cibernetici.Si tratta però di sistemi che, nel nostro Paese, non sono stati concepiti con un controllo remoto 'security embedded' e che, quindi, necessitano nel tempo dello sviluppo di opportune modalità correttive.

L'Information & Communication Technology costituisce l'elemento fondante per il processamento, l'immagazzinamento e lo scambio di informazioni anche di quei sistemi connessi al trasporto [K. Geers, 2009].

Le attuali minacce nel *cyberspace* possonocompromettere la riuscita di una missione in quanto capaci di interferire in maniera malevola e silente con la connettività dei sistemi di comunicazione, nei servizi di integrazione della rete e in quelli offerti dalle applicazioni funzionali, andando a modificare o a rendere non più attendibili e/o

chetti', tra le due parti legittimamente in comunicazione tra loro; ciò può comportare un degrado e/o un impedimento nell'utilizzo protocolli di rete o di alcuni servizi (cui ci si riferisce con la locuzione 'denial of service').

disponibili le informazioni dei sistemi (come SIGINT[3] e C2[4]).Tali minacce possono operare sia su reti *wireless* sia su reti cablate, quindi hanno metodi di trasporto e frequenze differenti e possono utilizzare tecniche di attacco misto [J. Andress, S.Winterfeld, 2014].

In particolare, le infrastrutture critiche, come quella per la gestione del Traffico Aereo (Air Traffic Management), sistemi aperti e interdipendenti in cui l'informazione è l'essenza, sono esposte, dal punto di vista cyber, ad una variegata tipologia di minaccia, dagli effetti inaspettati e potenzialmente molto gravi: 'Advanced persistentthreat' (Apt)[5], che consiste nella possibilità di studiare e pianificare nel tempo un attacco cibernetico come effetto sorpresa; 'Denial of

[3] SIGINT (acronimo di SIGnals INTelligence ovvero "Spionaggio di segnali elettromagnetici") è l'attività di raccolta di informazioni mediante l'intercettazione e analisi di segnali, sia emessi tra persone (ad esempio comunicazioni radio) sia tra macchine (è il caso dell'ELINT, lo spionaggio di segnali elettronici) oppure una combinazione delle due.

[4] C2 è l'abbreviazione di "Command e Control" e si riferisce, in senso generale, ai sistemi di comando e controllo all'interno di una missione militare. Questo termine è di uso comune anche nel settore della sicurezza informatica e nel contesto della *cyberwar*, dove si riferisce all'influenza che un attaccante ha su un sistema informatico compromesso che riesce a controllare. L'analisi avanzata delle metodologie di comando e controllo può essere utilizzata per identificare gli aggressori, associarne gli attacchi ed interrompere le attività malevole in corso.

[5] Minaccia consistente in un attacco mirato, volto ad installare una serie di *malware* all'interno delle reti del bersaglio al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni di valore dalle reti dell'ente obiettivo.

services' (DoS)[6], nella forma sia di attacchi cyber che di disturbi elettromagnetici;'interferenza', ovvero inserimento nello spettro elettromagnetico per ostacolare le operazioni (in quanto le modalità di attacco cyber si possono miscelare con attacchi e tecniche più tradizionali di guerra elettronica); 'Take control of system', ossia l'importazione di dati falsi e corrotti, con inserimento di *malware*[7]e con l'accesso e l'introduzione nei sistemi, anche manuale, attraverso l'intervento umano [K. Geers, 2009].

Il controllo del traffico aereo può facilmente diventare l'obiettivo di entità ostili, in quanto infrastruttura che partecipa al sistema dell'aviazione civile, tradizionale obiettivo simbolico delle forze del terrore. Le infrastrutture critiche(o di servizio critico), hanno, d'altronde, per loro stessa natura,una *mission*di valenza nazionale che deve essere assolutamente salvaguardata, proteggendo e garantendo i servizi che erogano, per cui l'uso sempre più richiesto di droni, robot e sistemi *unmanned* nel teatro operativo dovrà, esso pure, *a fortiori*, tenere in considerazione l'evoluzione delle minacce provenienti dal dominio cibernetico, riducendoauspicabilmente, fin dalla fase di design preliminare, tutte le possibili vulnerabilità [F. Castaldo, 2018b].

Il largo impiego delle tecnologie digitali applicate alle comunicazioni e all'informazione ha accresciuto a dismisura i rischi legati al *cyber-crime*, che oggi costituisce una delle maggiori minacce alla si-

[6] Attacco volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse ed il sovraccarico delle connessioni di rete dei sistemi server.

[7] Termine derivante dalla contrazione di *malicious software*, riferito ad un programma inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

curezza: una minaccia 'ibrida', che cioè ha impatti potenziali in ambito militare ma anche in quello civile ed industriale [D.H. Gray, A.Head, 2009].

L'impiego di tecniche informatiche ibride, ciò malgrado, è ancora marginalmente trattato e solo ultimamente sta ottenendo l'attenzione del mondo accademico e dell'industria, oltre che, naturalmente, delle Forze Armate. L'emergere della cyber-security sta delineando, in altri termini, un sempre più forte avvicinamento tra interessi militari ed economici. Minacce in campo informatico che utilizzano mezzi non convenzionali possono, difatti, influenzare decisioni e determinare effetti catastrofici anche nelle sfere economiche e sociali [J.A. Green, 2015].

Alcune di esse sono in stretta interazione con il fattore "umano", l'elemento più sensibile e più debole per la sicurezza delle informazioni. Nell'era cibernetica, inoltre, le minacce sono molto più numerose e diversificate rispetto a quelle di una volta; ciò richiede, come vedremo, dei mutamenti a livello delle strategie da utilizzare.

Rispetto a quelle tradizionali, le minacce informatiche presentano peculiarità come l'asimmetricità, la trasversalità, l'incessante mutevolezza e l'opacità o invisibilità. Ci riferiamo con questi due ultimi termini alla constatazione che la possibilità nel cyberspace di effettuare attacchi da notevoli distanze renda*ipso facto*molto difficile localizzare la sorgente dell'attacco.Il dominio cyber, in altri termini, è permeato dal cosiddetto "problema dell'attribuzione", per cui è molto difficile addossare la colpa di un attacco ad un colpevolee sovente, sostengono gli Esperti, nemmeno gli Stati Uniti hanno le risorse e lo status legale per validare l'identità di chi attacca o per attuare contromisure. Qualsiasi contrattacco rapido, infatti, può colpire l'obiettivo sbagliato mentre esitare potrebbe voler dire aumentare la propria vulnerabilità e dare al contempo vantaggi ulteriori all'attaccante [J. Andress, S.Winterfeld, 2014].

A livello organizzativo si assiste, conseguentemente, ad una considerevole compressione temporale, ovvero ad un accorciamento del processo decisionale, per cui i *decision maker* si trovano a dover prendere decisioni sotto stress, e quindi sub-ottimali o addirittura ad impatto negativo, e ad intraprendere dei corsi d'azione non pianificati in risposta a determinati ed improvvisiattacchi, con conseguenze potenzialmente nefaste.Tutto ciò, nel mondo delle imprese, oltre che naturalmente in ambito Difesa, si traduce nell' urgenza di acquisire - laddove non già possedute -"capacità dinamiche" come la tempestività, la flessibilità, il pensiero creativo, su cui si potrebbero fare molte considerazioni ma la cui trattazione esula dagli obiettivi di questo articolo[8].

3. I sistemi di difesa nella *cyberwar*

Nel Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, emanato durante il governo tecnico Monti, si enuncia che gli attacchi cibernetici più sofisticati non solo sono potenzialmente in grado di danneggiare o paralizzare il funzionamento di gangli vitali dell'apparato statale e la fornitura di servizi essenziali ai cittadini, ma possono avere anche effetti potenzialmente distruttivi, se impiegati per indurre il malfunzionamento delle infrastrutture critiche (ad esempio reti di controllo del traffico aereo, dighe, impianti

[8] Sul tema delle capacità dinamiche si veda, in particolare,Teece D.J., Pisano G., Schuen A.(1997), *DynamicCapabilities and Strategic Management*, «Strategic Management Journal», 18(7), pp.509-533;Aaker D.A., Mascarenhas B. (1984), *The need for strategicflexibility*, «Journal of Business Strategy», 1984, 5(2), pp.74-82.

energetici), generando danni materiali ingenti e la potenziale perdita di vite umane [Presidenza del Consiglio dei Ministri, Dicembre 2013].

Risulta, pertanto, chiaro come lo studio di possibili minacce all'integrità di sistemi e reti di interesse nazionale sia fondamentale per definire le necessarie linee di difesa.

Ci muoviamo, oggi più che mai, in contesti di rapida evoluzione della tecnologia e delle insidie associate ad essa, che impongono sempre più la necessità di ricorrere a sistemi di protezione dalla minaccia cibernetica, che è in continua e tipologicamente variegata evoluzione.

Abbiamo precedentemente riferito che le attuali minacce, infatti, operanosia su reti *wireless*che su reti cablate, hanno metodi di trasporto e frequenze differenti e possono utilizzare tecniche di attacco misto. Gli antagonisti nel *cyberspace*, inoltre,possono, compromettere la riuscita di una missione interferendo inmaniera malevola e silente con la connettività dei sistemi di comunicazione, con i servizi di integrazione della rete e con quelli offerti dalle applicazioni funzionali, andando a modificare o a rendere non più attendibili e/o disponibili le informazioni dei sistemi [A. Klimburg, 2017]. In simile scenario conflittuale saranno protagonisti i nuovi radar 'Active ElectronicallyScanned Array' (AESA)[9] combinati con dispositivi 'Digital Radio Frequency Memory' (DRFM)[10].

[9] Si tratta di radar a scansione elettronica attiva.

[10] Si tratta di dispositivi nati per svolgere funzioni di guerra elettronica di tipo 'attaccoattivo'. Un sistema che utilizza la DRFM è in grado di memorizzare in formato numerico un segnale radio o a microonde in ingresso, per poi poterlo ricostruire con la migliore fedeltà possibile ed eventualmente ritrasmetterlo. Nell'applicazione di contromisure elettroniche (jamming), le tecniche DRFM sono tipicamente usate

Il *cybercrime* costituisce attualmente una delle maggiori minacce alla sicurezza, sia in ambito militare che civile. La *cybersecurity* costituisce la risposta a tale minaccia. Essa si pone l'obiettivo di garantire confidenzialità, integrità e disponibilità dell'informazione [J. Andress, S. Winterfeld, 2014].

L'attenzione tecnologica, conseguentemente,sta evolvendo negli ultimi tempi verso gli apparati cifranti che permettono di proteggere la confidenzialità e, quindi, la segretezza delle informazioni scambiate.

Le future comunicazioni sicure saranno realizzate su una rete Ip nera (ovvero cifrata), che si appoggerà sulla rete internet commercialmente disponibile al fine di veicolare traffico in segretezza: gli sforzi andranno nella direzione di rendere interoperabili gli apparati cifranti Ip [W.J. Lynn, 2010].

L'architettura delle infrastrutture protettive poggia - oggi - su tre presupposti fondamentali: la sicurezza, utile a proteggere gli *asset* critici da minacce note ed emergenti, la vigilanza, vantaggiosa per aumentare la consapevolezza della minaccia e la localizzazione delle attività antagoniste, e la resilienza, fondamentale per potenziare la capacità di pronta reazione agli attacchi.

per ingannare i radar creando falsi bersagli, risultando così tra le più efficaci nell'ambito della cyberwar.

Come visto precedentemente, i sistemi che utilizzano in modo intensivo reti di comunicazione e tecnologie digitali per il controllo, nonché scambio di grande quantità di informazioni sono particolarmente esposti agli attacchi cibernetici, attacchi da cui è peraltro assolutamente necessario difendersi o, meglio, resistere, essere resilienti, recuperare.

Ci riferiamo alla resilienza nel dominio cibernetico con riguardo all'introduzione di misure atte a resistere agli attacchi informatici preservando le capacità funzionali di un dato sistema. I sistemi sono, quindi, resilienti allorquando resistono agli attacchi informatici preservando le capacità funzionali e, quando, in caso di soccombenza, sono in grado di ripristinare le proprie funzionalità nel più breve tempo possibile.

Le nuove generazioni di cifranti saranno riprogrammabili: invece di contenere il tradizionale singolo algoritmo di cifratura, implementeranno intere suite crittografiche. I futuri sistemi di difesa cyber potrebbero essere *self- configuring* e *selfhealing*: sistemi quindi che si auto configurano e si autoriparano [D.H. Gray, A. Head, 2009].

La sinergia di *safety, security* e *resilience* sembra essere oggi la risposta per eliminare o ridurre la portata di tutte le minacce e i rischi insiti nel dominio ciberneticoe sul concetto di resilienza è imperniata la disciplina della cybersecurity [J.Caravelli, N.Jones, 2019].

La ricchezza delle riflessioni e teorizzazioni sui rapporti concettuali tra *safety*, *security* e *resilience*richiederebbe un'approfondita disamina, che travalica gli intenti di questa trattazione. Per lo scopo che si prefigge il presente articolo sia sufficienteaffermare qui che*security* e *safety*costituiscano ormai,nel contesto del cyberspazio, un binomio imprescindibile che contribuisce alla *resilience* delle infrastrutture critiche. È dunque necessario affrontarne congiuntamente le problematiche, per evitare carenze progettuali, ottimizzare le risorse messe in campo e migliorarne l'efficacia.

4. Dalla *cyber-defence* alla *cyber resilience*: una sfida organizzativae culturale

Le tecnologie e la Rete sono alla base dei sistemi complessi che assicurano la corretta esecuzione di settori strategici e sensibili di uno Stato, come quelli dell'energia, dei trasporti, della finanza.

Conseguentemente, la sicurezza cibernetica di un Paese rappresenta una delle sfide più significative per tutti i governi: si tratta di proteggere la sensibilità delle proprie informazioni, delle infrastrutture critiche e degli *asset*industriali, tecnologici e scientifici che sono alla base dell'economia. Le stesse guerre già oggi avvengono in una forma definita 'ibrida', ovvero con una componente rilevante di attacchi elettronici [Q. Liang, W. Xiangsui, 2001].

L'uso pervasivo di smartphone e tablet nella vita di tutti, così come la rapida diffusione di oggetti grandi e piccoli, tutti connessi alla rete, rende chiaro come la cyber-security sia oggi un interesse nazionale generale. In considerazione di ciò, i governi di tutto il mondo hanno cominciato a contrastare e mitigare le minacce e i rischi derivanti dall'utilizzo della rete e delle tecnologie dotandosi, tra le altre cose, di appositi strumenti legislativi [J.Caravelli, N. Jones, 2019].

La prosperità economica di un sistema-Paese si misurerà anche in base al grado di sicurezza che saprà dare al proprio spazio cibernetico. Un tema di particolare rilevanza, in questo momento storico, alla luce delle diverse vicende internazionaliche hanno riguardato fughe di dati, intrusioni informatiche e intercettazioni del traffico internet, a cui ci riferiamo con la locuzione 'Datagate'.

La sicurezza cibernetica contribuisce allo sviluppo economico dei sistemi sociali odierni, al pari del diritto alla salute, e perciò garantire la *cyber-security* delle istituzioni e delle industrie strategiche di un Paese rappresenta una sfida cruciale per la politica e l'intelligence del terzo millennio.Per operare efficacemente in una frontiera così deli-

cata è necessario compiere però un salto culturale. Ora, tutti i settori produttivi - industrie, servizi, finanza e pubblica amministrazione - sono esposti ad aggressioni telematiche finalizzate a bloccarne le attività o a trafugarne dati fondamentali con ripercussioni nel funzionamento delle infrastrutture ed impatti talvolta devastanti: basti pensare, per renderne un'idea, ad un attacco alle architetture informatiche su cui si poggiano i servizi di trasporto aereo e navale oppure alla manipolazione del dosaggio degli agenti chimici di depurazione dell'acqua dei grandi acquedotti urbani. Proteggersi nel cyberspazio, così come nei luoghi fisici, è sempre più vitale, per i suoi riflessi economici, oltre che, naturalmente, per quelli intrinsecamente legati alla sicurezza nazionale [W.J. Lynn, 2010].

In base alle osservazioni finora svolte, pare che nel contesto tecnologico attuale nessuna organizzazione possa prescindere da un corretto piano di *cybersecurity* e *cybersafety* per la protezione delle proprie infrastrutture critiche [K. Geers, 2009].

A livello aziendale, oltre che naturalmente governativo-istituzionale, è divenutoimprescindibile investire sullo sviluppo tecnologico per aumentare la resilienza cibernetica in un contesto di evoluzione, o di passaggio, dalla *cyber-defence* alla *cyber-resilience*, laddove la *cyber defence* cerca di evitare che gli avversari violino i sistemi mentre la *cyber resilience* mira a rendere i sistemi del cyber spazio più difficili da sfruttare.

L'insieme di *security, safety e resilience* sostiene la realizzazione della *mission* aziendale contro eventi avversi, intenzionali o accidentali. In realtà ci si potrebbe spingere a sostenere che *safety, security* e*resilience*stiano evolvendo fino a diventare parti essenziali della*stessa mission* di un'organizzazione.

Attualmente tale sinergia è oggetto di studi sempre più approfonditi. È comunque evidente come sia richiesto un approccio multidisciplinare e non settoriale [J.A. Green, 2015].

Safety, security e*resilience* hanno, tuttavia, numerose declinazioni, in dipendenza dal campo di applicazione: Automotive, Aerospace, Transportation; diventa, pertanto, difficile proporre e creare sinergie che, però, sono il vero valore aggiunto per un'organizzazione. Il punto di partenza dovrebbe essere la definizione di concetti e pratiche comuni ai diversi settori.

E' importante che ci sia un approccio cooperativo alla sicurezza, una supervisione delle tecnologie dei *vendors* stranieri, un maggior controllo della sicurezza dell'intera catena logistica, una valutazione accurata degli impatti degli eventi *cyber* sulle infrastrutture critiche, oltre che una raccomandazione per i costruttori dei sistemi di difesa a progettare futuri sistemi pensando alla sicurezza e alla resistenza ad attacchi cyber sin dal loro concepimento e per tutto il ciclo di vita; realizzare, quindi, sistemi intrinsecamente sicuri e resilienti al fine di ridurre il danno derivato dalla malevola intrusione.

Per seguire la tecnologia mutevoleè necessario altresì sviluppare approcci nuovi per mitigare le conseguenze dei cyber attacchi [J.Andress,S. Winterfeld, 2014].

In particolare, per trattare efficacemente gli aspetti legati alla sicurezza in ogni ambito sociale sarebbe auspicabile assumere un'ottica sistemica, per evitare inutili duplicazioni a livello dei sottosistemi e non lasciare aree di vulnerabilità.

Uno degli indirizzi operativi contenuti nel Piano Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, stabilisce la promozione e diffusione della sicurezza informatica, la formazione e l'addestramento, divenendo pertanto aspetto fondamentale della linea di difesa nazionale dagli attacchi informatici e presente in quasi tutte le *cyber-strategies* emanate a oggi in diversi Paesi [Presidenza del Consiglio dei Ministri, 2013].

La sicurezza informatica inizia con il comportamento responsabile di ogni individuo che opera su sistemi personali e aziendali; per-

tanto, si pone l'esigenza di un'attività di promozione della cultura della sicurezza informatica diretta non solo al personale specializzato che opera nel settore, ma ad un più ampio pubblico di privati cittadini, personale delle Pubbliche amministrazioni e imprese [U. Gori, 2015].

5. Cybersecurity: una sfida cruciale nel terzo millennio. Riflessioni sull'ambiente strategico e sulla strategia

Una riflessione sull'ambiente strategico conduce a constatare come la maggioranza delle strutture cibernetiche siano di proprietà privata in uno spazio (il cyberspazio) senza confini.

Con l'avvento dell'era digitale, i conflitti - come hanno sostenuto diversi Autori - tenderanno ad essere sempre più immateriali e virtuali sicché il potere statuale stesso risiederà sempre meno sul territorio, con le risorse naturali, e sulla cosiddetta 'potenza militare' e sempre più sulle idee e sulle conoscenze[J. Adams, 2001; J.A. Green, 2015].

Ora, se è noto che la forza non possa essere usata quando il nemico è ignoto o invisibile, nell'ambiente cibernetico l'obiettivo, non potendo essere il bersaglio, diviene la mente del nemico, come teorizzavaSunTzu nel suo trattato sulla guerra,dove veniva enfatizzata l'importanza dell'intelligence e dell'inganno [R. Fracasso, 1994].

L'avvento delle ICT ha provocato una evoluzione negli stessi strumenti di intelligence e nel tipo di manovre belliche.

Nella *cyber war*, la strategia stessa è cangiante, in quanto deve seguire e reagire a contesti situazionali mutevoli, per cui l'uso di stratagemmi è massimamente usato.

Dopo che la tecnologia ha aggiunto agli ambiti tradizionali della conflittualità una quinta dimensione, quella del cyberspazio, è mutata, poi, l'idea stessa di manovra, intesa tradizionalmente come la disposizione delle forze per assicurare vantaggi di posizione sia prima

che durante le operazioni di combattimento [U. Gori, 2016]. Nei domini della conflittualità noti sono le forze in gioco ad essere movimentate, laddove nel cyberspazio ad essere spostate sono le basi da cui proviene un attacco: è questo, tra l'altro, a determinare il problema dell' 'attribuzione' cui abbiamo accennato poc'anzi.

Le manovre offensive, che nel dominio cibernetico consistono nell'applicare un software o un algoritmo per acquisire, compromettere, distruggere risorse informative o computazionali, hanno caratteristiche peculiari: sono invisibili, raggiungono l'obiettivo istantaneamente, hanno un raggio d'azione illimitato, possono acquisire il controllo di sistemi altri e sono capaci di compromettere i sistemi di comando e controllo dell'avversario fornendo dati fasi e manipolati. Del pari, le manovre cibernetiche difensive hanno - nel cyberspazio - connotazioni particolari, come la difesa con obiettivo mobile o quella che si avvale di esche.Tali manovre sono, talvolta,usate anche nei confronti di Paesi alleati ed amici, manovre che, impunite nel cyberspazio, sarebbero considerate spesso veri e propri atti di guerra in ambienti convenzionali [J.Andress, S.Winterfeld, 2014].

Per gestire la conflittualità nell'arena cibernetica, com'è stato osservato da Vittorio Gori, si rivela molto proficuo l'approccio militare orientale, il cui pensiero è stato storicamente caratterizzato dal prendere in considerazione la relazione tra le cose, gli elementi, e quindi, per estensione, il network, la rete, e la cui stessa strategia viene *ab initio* concepita in modo da sfruttare il naturale andamento delle cose, laddove il pensiero militare occidentale, il cui ambiente strategico sfrutta i noti principi di massa e manovra, pare riuscire meglio a risolvere i conflitti che richiedono l'impiego di strumenti bellici tradizionali [U. Gori, 2016].

6. Per una deterrenza di successo nel cyberspazio

Se per decenni i paesi della Nato hanno potuto contare su alte capacità di difesa integrata e su efficaci sistemi deterrenti, negli ultimi anni è divenuto sempre più difficoltoso stimare o predire le stesse minacce alla sicurezza [P. Rosenzweig, 2013].

In uno scenario complesso come quello sin qui delineato, una deterrenza di successo nel *cyberspace*non può che essere, necessariamente, la risultante dello sforzo complessivo di un governo per la difesa dei propri militari, del settore pubblico e privato, e dei partner e alleati internazionali.

Un'analisi delle *cyber-strategy* rese pubbliche a livello internazionale consente di evidenziare delle tendenze strategiche anche a livello europeo. Nello specifico, le linee comuni dello sviluppo del pensiero strategico di matrice europea sono tracciate lungo i binari della necessità di: focalizzarsi sulle problematiche relative alla criminalità informatica; incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici; stabilire trattati, leggi e regole di condotta nazionali e/o internazionali ad hoc; sviluppare i rapporti diplomatici e rafforzare le partnership internazionali; rafforzare la condivisione delle informazioni (anche tra pubblico e privato), l'*earlywarning*[11] e la capacità di *incidentresponse*[12].

[11] Ci si riferisce a quei sistemi di allerta dalle minacce incombenti o, per estensione, servizi di sicurezza finalizzati alla raccolta, all'analisi e alla divulgazione di informazioni in merito alla vulnerabilità tecnologica.

[12] L'*incidentresponse* può essere definito come un insieme di procedure e risorse utilizzate per reagire ad incidenti informatici.Qualunque azienda deve dotarsi di un piano di risposta agli incidenti o incidentresponseplan, che le consenta di far fronte efficacemente a situazioni di questo tipo. Nessuna organizzazione, grande o piccola, che disponga di una rete informatica, più o meno complessa, connessa ad Inter-

Ciascuno Stato dovrebbe, idealmente, affrontarei nodi cibernetici insieme ai Paesi che hanno interessi simili, siano essi partner, alleati o amici, a partire da una piattaforma comune.

In altri termini, emerge sempre più evidentemente l'impossibilità, per il singolo Paese, di affrontare isolatamente l'imprevedibilità di rischi di immani proporzioni, come quelli delle guerre cibernetiche del futuro [J.Caravelli, N. Jones, 2019]. Ne consegue che le opzioni praticabili per la deterrenza nel cyberspazio comprendano, da un lato, il rafforzamento della difesa (mediato attraverso la *cybersecurity*) e dall'altro il perseguimento di partnership nonché l'avanzamento di politiche e soluzioni legislative.

Con particolare riferimento a queste ultime opzioni, alcuni studiosi ed esperti del settore hanno evidenziato la necessità e l'urgenza di pervenire ad una riorganizzazione della struttura istituzionale, con la contemporanea creazione di una figura esecutiva di natura politica che abbia le competenze necessarie per tradurre in piani pratici la strategia nazionale di difesa cibernetica [Great Britain, Ministry of Defence, 2004]. Il fatto che alcuni Paesi, come ad esempio il Regno Unito - dove, dal 2010 opera, all'interno del gabinetto del Primo Ministro un "Office of cyber security and *information assurance"* che coordina i programmi di sicurezza informatica gestiti dal governo - si siano mossi in questa direzione, mostra chiaramente l'importanza dell'attuare strategie nazionali consapevoli su questo tema. L'Italia, per quanto possa apparire arretrata, sul tema della *cybersecurity* non lo è affatto: nel 2013 fu varato dall'allora governo tecnico di Monti un DPCM che individuava e disciplinava la *governance* della cyber-

netpuò sentirsi al sicuro di fronte al rischio di attacchi informatici e diventa quindi necessario che si prepari in modo tale da rilevarli prima possibile, rimuoverne le cause, contenere gli effetti e ripristinare i sistemi allo stato originario.

security del nostro Paese[13]. Veniva concepita, sostanzialmente, la creazione di un'architettura gravitante sul vertice dell'Esecutivo del Paese e sul CISR (Comitato Interministeriale per la Sicurezza della Repubblica), e che faceva del 'Consigliere Militare del Premier' l'attore principale del 'Nucleo per la Sicurezza Cibernetica', esercitando un ruolo politico di coordinamento interno e di rappresentanza del Premier all'esterno. Gli organismi informativi dell'Intelligence ovviamente affiancavano il Consigliere, continuando in tal modo a giocare un ruolo predominante. A partire da quel Provvedimento furono poi subito dopo emanati un 'Piano nazionale per la protezione cibernetica e la sicurezza informatica' e un 'Quadro Strategico nazionale per la sicurezza dello spazio cibernetico'. Il governo successivo, riconoscendo il valore del lavoro svolto, nel 2015 emanò una direttiva strategica volta a migliorare gli standard di sicurezza[14]. In particolare, venivano indicati due principi fondamentali cui riferirsi: un maggiore e più efficace coordinamento, nonché l'integrazione delle funzioni dei diversi soggetti pubblici e lo sviluppo delle relazioni con il settore privato, realizzando un efficace e capillare partenariato con tutti gli operatori non pubblici a cui è affidato il controllo di infrastrutture informatiche e telematiche da cui dipendono ormai funzioni essenziali per il Sistema Paese e per la fruizione dei diritti fondamentali degli individui.

[13] Si tratta del DPCM Monti del 24 gennaio 2013 che ha costituito l'architettura nazionale in materia di sicurezza cibernetica fino alla sua abrogazione e sostituzione con il 'Decreto Gentiloni', approvato il 17 febbraio 2017 (DPCM 17 febbraio 2017).

[14] Direttiva 1° agosto 2015 del Presidente del Consiglio dei Ministri - Sistema di informazione per la sicurezza della Repubblica.

Per quel che concerne le opzioni legali per un'efficace deterrenza, è opportuno sottolineare come, adifferenzadegli altri domini, dove la legislazione in materia bellica ha potuto perfezionarsi lungo interi decenni, nel cyber-spazio il progresso tecnologico sia stato esponenzialementre le corrispondenti normative domestiche nonché il diritto internazionale siano decenni indietro [J.A. Green, 2015].

Questa situazione, legata anche alla natura globale del mondo *cyber*, costituisce un ostacolo, peraltro, alla ricerca degli attori criminali: la penuria di norme ha condotto ad una sostanziale zona grigia sfruttata allo stesso modo da attori statali e non statali. alleati avevanoNel 2011Cina, Russia e altri Paesi avevano presentato all'Assemblea generaledelle Nazioni Unite un Codicedi Condottaper la sicurezzacibernetica internazionale delle informazioni come un possibile punto di partenza per lo sviluppo di queste norme [S. Mele, 2018].

Le diverse nazioni hanno, tuttavia, differenti priorità ed interessi nel perseguimento della standardizzazione del cyber-spazio; laddove gli Stati Uniti cercano di garantire la libertà di accesso, migliorando la sicurezza delle reti, altri Paesi, come Russia e Cina, si concentrano maggiormente sul rischio, per la loro stabilità politica, della libertà di accesso. In una situazione come questa, in cui permangono inevitabili divergenze di interessi nonché diversità culturali, nondimeno occorrerebbero progressi in direzione del rafforzamento della sicurezza complessiva nell'ambiente del *Cyberspace* [W.J. Lynn, 2010].

Una delle aree su cui maggiormente si è arenato il processo legislativo inerente alla difesa cibernetica negli ultimi anni è quella del cosiddetto 'reporting', ovvero della comunicazione in emergenza degli attacchi ai propri sistemi informativi da parte delle imprese. Le offensive degli ultimi anni ad aziende note come Sony Pictures, Jp Morgan, Target, per citarne alcune, hanno fatto emergere questo problema in tutta la sua evidenza. Questi attacchi hanno mostrato la vul-

nerabilità dei sistemi di protezione, portando al furto di milioni di dati personali e informazioni private [A. Klimburg, 2017].

Quali sono gli uffici cui rivolgersi e attrezzati per mantenere il livello di segretezza richiesta dalla gestione di eventi critici aziendali di tale natura? Si tratta di un nodo importante in quanto legato alla stessa organizzazione statuale. Se, infatti, è il controspionaggio a dover gestire le notizie di reati cibernetici, e la risposta conseguente, ne deriva che la *cyberdefence*costituisca un tema molto delicato perché mette in contatto diretto tutte le imprese (tutte, ma in particolar modo quelle 'strategiche' come trasporti, energia, banche) con gli apparati dello Stato, epicentro operativo della sicurezza politica. I gruppi del potere economico si rapportano cautamente con i centri di potere degli Stati di tutto il mondo in un rimbalzo di richieste di gestire e risolvere le proprie vulnerabilità [J.Caravelli, N. Jones, 2019].

Il rischio latente è che imprese, anche grandi, finiscano nella rete di cyber-criminali che promettono loro di gestire le criticità informatiche lontano dallo sguardo 'intrusivo' degli Stati. Sarebbe sufficiente che ciò avvenisse in pochi segmenti chiave del mercato globale per causare *disruption* sistemiche della sovranità statale. Ciò esalta l'importanzadi una legislazione fondata sulla cooperazione strutturata pubblico-privato [J.A. Green, 2015].

Un'altra area da migliorare è senz'altro, come anticipato, quella della politica e delle opzioni legali. La politica, per sostenere una cyber deterrenza dovrebbe avere obiettivi chiaramente indicati, credibili e coerenti.Ciò a sua volta richiederebbe l'impiego di maggiori risorse per affrontare la problematica, per aumentare ad esempio le capacità di attribuzione ed evolvere verso un dominio del *cyberspace* più robusto e sicuro.

In definitiva, gli attacchi nel cyberspace sono possibili perché le reti e i sistemi hanno imperfezioni. Se i governi fossero in grado di

eliminare o quantomeno di ridurre questi difetti, ulteriori opzioni di deterrenza si renderebbero disponibili.

7. Considerazioni conclusive

Il cyber, abbiamo visto, può essere un *domain*incredibilmente dirompente, distruttivo: può distruggere persino l'hardware, può disabilitare le infrastrutture critiche e ciò potrebbe portare alla perdita di vite umane. In ogni campo gli USA godono di un notevole vantaggio militare ma hanno concorrenti di pari livello in quello informatico, che è un terreno ancora in gran parte inesplorato e nel quale è molto più facile inserirsi, un "levelplayingfield", come lo ha definito in un'intervista il generale Martin E. Dempsey[15], Chairman of the Joint Chiefs of Staff e principale consigliere militare del presidente Barack Obama, ovvero un terreno in cui gli attori sono tutti sullo stesso piano e nel qualegli Stati Uniti non riescono a tradurre la loro superiorità tecnologico-militare così evidente nei classici settori della difesa cinetica.

[15] In un'intervista del 2015 il generale Dempsey, parlando delle minacce alla sicurezza di USA ed Europa, sostenne che gli USA "faces a levelplayingfieldagainst cyber threats", riferendosi, in particolare, alle vulnerabilità provenienti dalle infrastrutture civili e dal mondo del business, a dispetto delle formidabili capacità di difesa militari.

Da quando il cyber-spazio è divenuto dominio di warfare[16], garantire un approccio strategico alla sicurezza diquesto settore, pianificarne la crescita, valutare i rischi a breve, medio e lungo termine, nonché svolgere attività previsionali sulla sua evoluzione, rappresentano un compitoormai imprescindibile, da porre come prioritario nell'agenda politica di un buon governo, soprattutto oggi che la *cybersecurity*rappresenta per tutti una delle sfide più impegnative per il sistema globale.

Riferimenti bibliografici

Aaker D.A., Mascarenhas B. (1984), *The need for strategic flexibility*,«Journal of Business Strategy», 1984, 5(2), pp.74-82.

Adams J. (2001), *Virtual Defense*, «Foreign Affairs», 80(3), pp.98-112.

Andress J., Winterfeld S. (2014), *Cyber Warfare: Techniques, Tactics and Tools for SecurityPractitioners*, Elsevier, Waltham.

Caravelli J., Jones N. (2019), *Cyber Security: Threats and Responses for Government andBusiness*, Praeger Security International, Westport, Connecticut.

Castaldo F.,*Fronteggiare il nemico in arene competitive turbolente: l'importanza della fiducia e delle capacità dinamiche nelle alleanze strategiche*, «Rivista Italiana di Conflittologia», n.35, 2018.

[16] Quando, nel settembre 2010,all'indomani del caso del *malware*Stuxnet, l'allora vicesegretario della Difesa americano William J. Lynn III qualificò pubblicamente il cyber-spazio come "il quinto dominio della conflittualità" (dopo terra, mare, aria e spazio), le minacce provenienti dalle tecnologie digitali e da Internet finirono sotto una enorme lente di ingrandimento, il *cyber-space* divenne dominio di *warfare* e, conseguentemente, si cominciarono a dirigere gli sforzi, non solo nel settore della Difesa, verso la creazione di strategie di deterrenza atte a prevenire eventuali conflitti nel cyberspazio.

Castaldo F.,*I sistemi di gestione del traffico aereo e l'incombente minaccia del crimine: la necessità di un modello organizzativo cyber security centric*,«Rivista Italiana di Conflittologia», n.36, 2018.

Fracasso R. (1994), *L'arte della Guerra*, Traduzione integrale di SunTzu (V-IVsec. A.C.), *Bingfa*, Newton Compton Editori, Roma.

Geers K. (2009), *The Cyber Threat to National Critical Infrastructures: Beyond Theory*, «The Information Security Journal: A Global Perspective», 18(1), pp.1-7.

Gori U., Lisi S. (2014) (a cura di), *Information Warfare 2013. La protezione cibernetica delleinfrastrutture nazionali*, Franco Angeli, Milano.

Gori U. (2015), *Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business*, Franco Angeli, Milano.

Gori U. (2016), *Interesse nazionale, intelligence e strategie in era cibernetica*, «Gnosis», 2, pp.87-93.

Gray D.H, Head A. (2009), *The importance of the internet to the post-modern terrorist and its roleas a form of safe haven*, «European Journal of Scientific Research», 25(3), pp.396-404.

Great Britain. Ministry of Defence (2004), *Delivering Security in a Changing World: Future Capabilities*.

Green J.A. (a cura di) (2015), *Cyber Warfare. A multidisciplinary analysis*, Routledge, New York.

Klimburg A. (2017), *The Darkening Web: The War for Cyberspace*, Penguin Press, New York.

Liang Q., Xiangsui W. (2001), *Guerre senza limiti. L'arte della guerra asimmetrica tra terrorismo eglobalizzazione*, Libreria Editrice Goriziana, Gorizia.

Lynn W.J. (2010), *Defending a New Domain: The Pentagon's Cyberstrategy*, «Foreign Affairs», 89(5), pp. 97-108.

Mele S.(2018), *Se Macron rilancia la Francia nellospaziocibernetico*, «AirPress», n.95, pp.60-61.

NATO Standardization Agency (2012), *NATO Glossary of Terms and Definitions* (AAP-06).

Presidenza del Consiglio dei Ministri (Dicembre 2013), *Quadro Strategico Nazionale per laSicurezza dello Spazio Cibernetico*.

Rosenzweig P. (2013), *Cyber Warfare. How Conflicts in Cyberspace Are Challenging America andChanging the World*, Praeger, Santa Barbara.

Teece D.J., Pisano G., Schuen A. (1997), *Dynamic Capabilities and Strategic Management*, «Strategic Management Journal», 18(7), pp.509-533.

Teti A. (2018), *Cyber Espionage e Cyber Counterintelligence: Spionaggio e Controspionaggiocibernetico*, RubbettinoEditore, SoveriaMannelli (CZ).