Atti Convegno Cyber Crime Conference 2018 – Umberto Gori

Author : Redazione

Date : 28 maggio 2018

Strategie e manovre nello spazio cibernetico: l'uso delle *cyber weapons* nella conflittualità del XXI secolo

Il sistema internazionale ha subìto negli ultimi anni trasformazioni così radicali da rendere desueta, o comunque non più soddisfacente, una lettura del medesimo attraverso i classici paradigmi interpretativi. E' nata la politica *post-internazionale* caratterizzata da interdipendenze complesse e da *turbolenza*. La conseguenza è l'i*ncertezza*. Un'altra conseguenza è l'ampliarsi del concetto di *sicurezza*.

I c.d. *eventi inaspettati* sono sempre più frequenti e incidenti minori producono conseguenze abnormi. L'unico modo per dominare il mutamento e vincere la turbolenza è una sofisticata capacità di *resilienza* e un approccio proattivo ai segnali di futuro.

Questo è il contesto nel quale si è sviluppato lo *spazio cibernetico*, l'unico spazio creato dall'uomo e da questi modificabile. Esso offre alla 'superpotenze', diversamente da come accadeva in epoca di guerra fredda quando i conflitti bellici erano demandati agli Stati *proxy*, la possibilità di scontrarsi direttamente.

I grandi rivolgimenti nella politica internazionale sono stati originati da tre fattori: guerre, mutamenti nell'economia e sviluppi tecnologici, con conseguente trasferimento di *risorse*.

Nello stesso modo ed ancor di più, le tecnologie ICT stanno modificando in misura difficilmente quantificabile la dinamica delle relazioni fra Stati: rimodellano l'architettura del sistema internazionale, ne cambiano i processi tradizionali (la 'diplomazia digitale', ad esempio, determina una radicale trasformazione dei processi di comunicazione), rivoluziona la finanza, il commercio, la raccolta di dati sensibili per l'intelligence, crea nuovi problemi per la politica estera (si pensi a *WikiLeaks*), modifica ed accelera la percezione di eventi critici per la sicurezza. L'ICT inoltre, accessibile anche a entità sub-nazionali e a individui, rende questi ultimi possibili protagonisti del cambiamento, sottraendo agli Stati il tradizionale monopolio del

controllo e della forza.

In breve, in un mondo globalizzato ed in era cibernetica chi sarà più avanti nell'utilizzo delle tecnologie ICT dominerà il mondo.

In coerenza con l'era cibernetica, anche la guerra, da scontro fisico, è diventata *virtuale*. Tutto, oggi, si muove verso l'*intangibile*. Ed ecco le "nuove guerre" o "guerre post-moderne", come le chiama Mary Kaldor, guerre asimmetriche, a bassa intensità (si noti il procedere ad un sempre minor impiego della forza fisica), che non consentono una chiara distinzione fra 'interno' e 'internazionale', basate su rivendicazioni di identità piuttosto che di territorio (anche qui si va dal concreto all'astratto). In questa categoria rientrano anche le guerre nel cyberspazio che, dopo la terra, il mare, il cielo e lo spazio fisico, costituisce la quinta dimensione dei rapporti internazionali.

E' opportuno qui precisare subito quali siano le principali (sottolineo: le principali) modalità che oggi assume la conflittualità. Ad esempio, non parlerò di ciò che quasi certamente avverrà, e cioè il dispiegamento delle LAWS (*Lethal Autonomous Weapons Systems*). Il mondo anglosassone ha tre concetti che le individuano: *Information Warfare* (IW), *Cyber Warfare* (CW) e *Hybrid Cyber Warfare* (HCW). E' la NATO che nella sua dottrina sulle *Info Ops* considera sinonimi il concetto di 'Information Operations' e quello di 'Information Warfare'. Precisato ciò, la NATO definisce le Info Ops come "*una funzione militare mirante a creare effetti desiderati sulla volontà, comprensione e capacità dell'avversario*". Se una sola di queste caratteristiche non viene influenzata, viene a mancare la possibilità di agire nel modo voluto.

In passato l'obiettivo era quello di influenzare le 'capabilities' e, solo in secondo luogo, la volontà. Oggi si cerca di influenzare la volontà, ma anche la comprensione, o interpretazione, della realtà da parte dell'avversario, nonché – ovviamente – le 'capabilities' condizionanti la comprensione e l'applicazione della volontà. Fra gli strumenti e le tecniche delle Info Ops appaiono preminenti le *operazioni psicologiche* (*Psy Ops*); le *misure ingannevoli* che presuppongono la capacità di immedesimarsi nel modo di pensare dell'avversario; le *Operations Security* che riguardano l'identificazione delle informazioni vitali che potrebbero consentire all'avversario di attaccare le vulnerabilità esistenti; le *Computer Network Operations* che consistono nell'attaccare, bloccare e utilizzare i computer avversari a fini di intelligence; la *guerra elettronica* che riduce al minimo l'uso della forza; la mera presenza militare e, quando necessario, la distruzione fisica dei sistemi di comando e controllo.

La *Cyber Warfare*, a sua volta, è la conseguenza della rivoluzione ICT e della digitalizzazione. Sempre a livello internazionale ne viene data la seguente definizione: "*un insieme di attività da parte di uno Stato tese ad introdursi nei computer o nelle reti di un altro Stato al fine di danneggiare o bloccare gli uni e le altre*". Altre definizioni includono fra gli attori, a mio avviso correttamente, anche soggetti non statuali.

Tali attività consistono in attacchi cibernetici contro infrastrutture critiche e sistemi militari come il C4ISTAR (*Command, Control, Communications, Computer, Information/Intelligence, Surveillance, Targeting Acquisition, Reconnaissance*), nonché nel rubare o alterare dati classificati di natura politico-militare o economico-finanziaria. Ciò che caratterizza la Cyber

Warfare, che si sviluppa in ambiente unicamente virtuale, è la sua potenziale *letalità*, o capacità distruttiva di cose o persone. Per capirci: il DDoS in Estonia può essere considerato il primo esempio di Information Warfare. L'attacco tramite Stuxnet alle centrali Iraniane, invece, il primo esempio di Cyber Warfare.

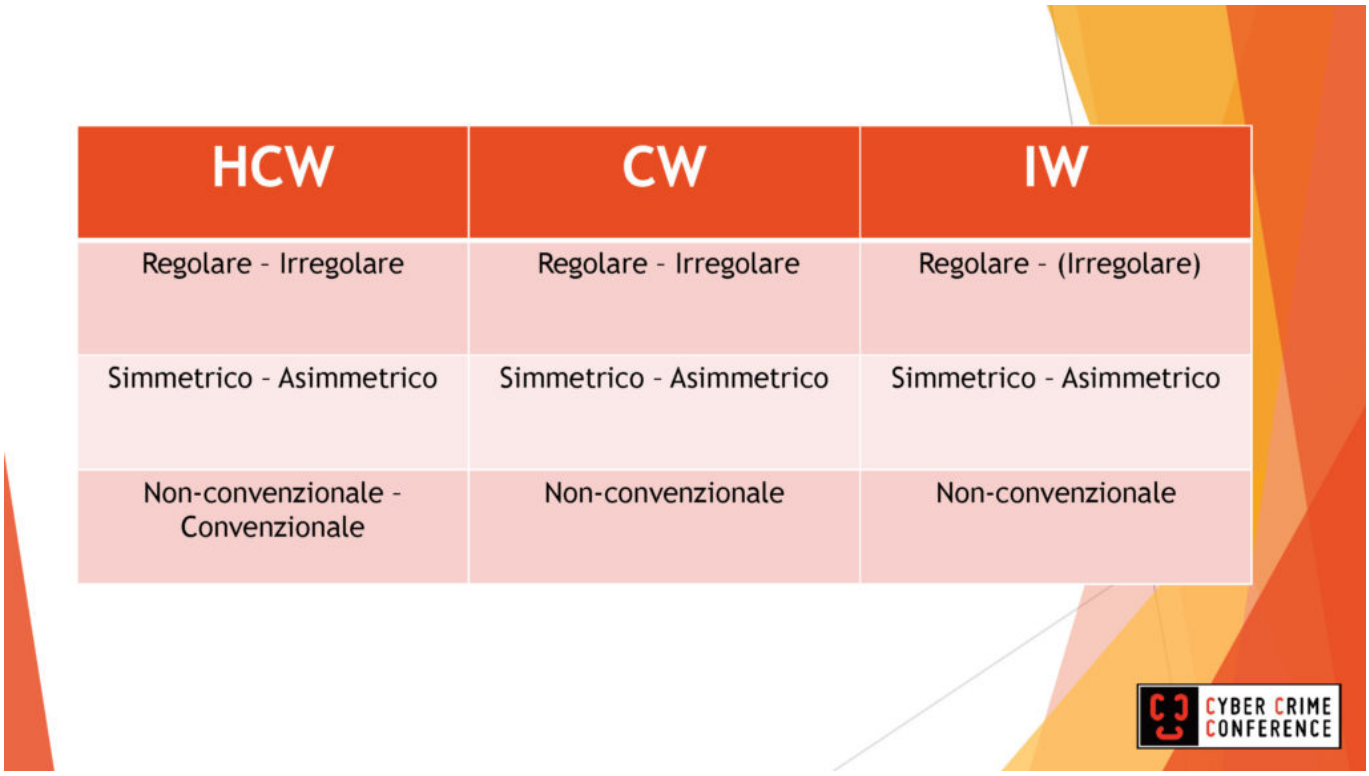
Ho l'obbligo di precisare che neanche gli Stati Uniti hanno definito in modo univoco cosa sia la Cyber Warfare.

Il problema sta nella difficoltà di stabilire a quale livello e con quali modalità un attacco cibernetico diventa un atto di guerra al quale si possa rispondere col massimo della potenza disponibile. A mio avviso - l'ho già ampiamente argomentato in passato - un cyber attacco è un 'atto di guerra' se comporta morti e/o distruzioni fisiche e se risponde a logiche di *Realpolitik*. In quest'ultimo caso è verosimile che l'attacco provenga da un attore ad alta organizzazione sistemica (leggasi Stato).

A prescindere dal problema dell'*attribuzione* e dalla conseguente difficoltà di *retaliation*, è solo a livello strategico che il problema trova una soluzione. Ad attacchi di livello inferiore l'unica risposta è la *resilienza* e la *deterrence by denial*.

Il terzo concetto entrato nell'uso è quello di *Hybrid Cyber Warfare*, anche se l'*ibridità* non è un fenomeno nuovo, di per sé. Con esso si è di fronte ad una strategia militare che 'mescola' guerra convenzionale, irregolare e cibernetica. Secondo la NATO, la Hybrid Warfare è in grado di "*simultaneously employ conventional and non-conventional means adaptively in pursuit of /one's/ objectives*". In altre parole, si usano mezzi convenzionali e non convenzionali, cinetici e non cinetici, *hard* e *soft power*.

L'ibridità, insomma, non è sinonimo di nuove tecniche, ma è l'uso di tutti i fattori di potenza, come suggerisce anche l'acronimo DIMEFIL (Diplomatic, Information, Military, Economic, Financial, Intelligence e Law Enforcement). Non tanto diversamente da quanto si insegnava, già mezzo secolo fa, all'allora Scuola di Guerra di Civitavecchia dalla Cattedra di Strategia Globale.



La coppia Regolare/Irregolare si riferisce alle forze statali e non-statali; Simmetrico/Asimmetrico si riferisce ai fattori di potenza; e Convenzionale/non-Convenzionale si riferisce al tipo di armi utilizzate.

Sono note le caratteristiche peculiari dello spazio cibernetico e la grande pluralità di soggetti che operano e confliggono in tale dominio. Dati tali mutamenti radicali, è possibile o conveniente utilizzare ancora i princìpi della vecchia e cara strategia cui siamo abituati?

La strategia è il portato di una cultura specifica ed è sensibile alle caratteristiche del terreno di competizione.

Due sono le principali tradizioni culturali che si affrontano: quella occidentale che si rifà a Clausewitz e quella orientale (in particolare Cinese) originata dall'antichissimo insegnamento di Sun Tzu.

Quale di queste due tradizioni è maggiormente applicabile alle guerre asimmetriche e 'liquide' del mondo cyber?

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. Per il Generale prussiano la guerra è un atto di forza, il massimo della forza, per costringere il nemico a sottomettersi alla nostra volontà. La guerra, anche se "continuazione della politica con altri mezzi", è, di per sé, un 'gioco' a somma zero (come, ad esempio, il gioco degli scacchi).

La cultura occidentale - la nostra cultura - è insomma abituata a reagire alle sfide in modo diretto, di puntare sull'obiettivo principale per conseguire il successo, secondo l'insegnamento Clausewitziano dello *Schwerpunkt*, tradotto come "centro di gravità" (più precisamente, 'punto focale').

La tecnologia, ed 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 e ignoto (problema dell'*attribuzione*). Inoltre, come sosteneva Giulio Douhet, "la forma di qualsiasi guerra dipende dai mezzi tecnici a disposizione".

L'insegnamento di Sun Tzu, coerente con l'antichissima cultura cinese, enfatizza invece l'importanza dell'uso dell'intelligence e dell'inganno. Per l'antico stratega il generale più bravo è quello che vince le guerre senza combattere e causare perdite di vite umane nel proprio esercito e in quello avversario. L'obiettivo è 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 più antico del mondo, il *go*, basato su una scacchiera dove interagiscono pietre nere e bianche di uguale 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. L'obiettivo è quello di acquisire parti sempre più estese del territorio in modo da assicurarsi, col tempo, una solida posizione strategica. E' ciò che sta facendo la Cina con le isole artificiali nell'oceano Pacifico. Usa la strategia di lungo periodo al posto della forza. In breve, per il pensiero militare cinese la strategia deve sfruttare la naturale tendenza delle cose e prepararsi a cambiare terreno di gioco.

A differenza del pensiero militare occidentale che vede l'ambiente strategico secondo una visione Newtoniana con precise leggi fisiche e sfrutta i princìpi di massa e di manovra, 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.

La cultura orientale reagisce cioè alle sfide in modo indiretto, con la strategia basata sugli effetti, secondo l'antico insegnamento di Sun Tzu, utilizzando il contesto, l'ambiente, il quadro generale. In altre parole, per gli occidentali l'obiettivo è il bersaglio; per gli orientali l'obiettivo è un intero sistema. Se si considerano i pericoli come sistemi e non come problemi a sé stanti si contribuisce ad aumentare la resilienza delle strutture. Ed è la resilienza a definire la sicurezza del XXI secolo.

In altre parole ancora - come è stato sottolineato - anziché imporre il proprio piano strategico alla realtà (modo occidentale), lo stratega cinese non pianifica, ma valuta e calcola, a partire da un esame minuzioso delle forze presenti, i fattori favorevoli all'uno e all'altro campo dai quali deriverà la vittoria. Lascia cioè che lo sviluppo implicato si attui da sé. L'effetto dell'azione è quindi ineluttabile e non probabile*. Solo per l'Occidente la strategia è una teoria dell'azione.* Per l'Oriente l'azione disturba la naturale evoluzione delle cose.

Sembra doversi concludere che l'approccio orientale è più adatto a gestire la conflittualità *non-cinetica*, mentre quello occidentale riesce meglio a risolvere i conflitti che necessitino di impiegare strumenti bellici tradizionali.

Anche il concetto tradizionale di *manovra*, visto come la disposizione delle forze per assicurare vantaggi di posizione, ha subìto modifiche nel cyberspazio. Una *manovra cibernetica* consiste nell'applicare la forza – nel nostro caso un *software*, o *algoritmo* – per acquisire, compromettere, distruggere risorse computazionali e informative al fine di ottenere un vantaggio competitivo. Ma mentre nei domìni tradizionali della conflittualità sono le forze ad essere movimentate, nel cyberspazio sono le basi da cui proviene l'attacco a poter essere spostate. Ed è questo uno dei motivi – come già accennato – a creare il problema cd dell'attribuzione.

Inoltre, le manovre cibernetiche hanno caratteristiche che le distinguono dalle manovre attuate nei conflitti terrestri, marittimi, aerei e spaziali. Eccole, brevemente enunciate:

Velocità. Le CyM raggiungono l'obbiettivo istantaneamente. Ciò favorisce chi agisce per primo. Però è anche vero che una modifica nella struttura difensiva dell'obbiettivo, attacco durante, rende praticamente impossibile per l'attaccante modificare la manovra in tempi talmente brevi da non essere scoperto. La modifica, infatti, non è automatica ma richiede una elaborazione umana.

Invisibilità. Questo elemento caratteristico rende problematica l'attribuzione di responsabilità.

Portata operativa. Diversamente da ciò che accade nelle manovre cinetiche, limitate dalla geografia fisica e dalla distanza, le CyM hanno un raggio d'azione illimitato.

Accesso e controllo. L'acquisizione e il controllo di sistemi altri dai propri consente di lanciare attacchi che rendono difficile o impossibile l'attribuzione. Ciò non accade nelle operazioni cinetiche quando vengono conquistate basi avanzate.

Evoluzione dinamica. L'evoluzione rapidissima ed incessante della tecnologia produce mutamenti continui nelle tattiche, tecniche e procedure. Diversamente da ciò che succede nei conflitti cinetici, non c'è molto spazio per la pianificazione.

Rapida concentrazione. Gli attacchi possono espandersi rapidamente da uno a innumerevoli punti senza alcuna allerta possibile, come accade, ad esempio, con i DDoS. Negli attacchi cinetici, invece, è praticamente impossibile concentrare le forze di nascosto, soprattutto nell'era dei satelliti. Inoltre, l'uso dei DDoS può servire a distrarre l'attenzione da altri attacchi più insidiosi.

Non-serialità. Agli attacchi seriali (attacco/contro-attacco) tipici degli scontri cinetici si contrappongono, nello spazio cibernetico, attacchi *in parallelo* contro molteplici obbiettivi che creano effetti non-lineari, tattici, operativi e strategici nello stesso tempo e mettono in grande difficoltà le strutture aggredite.

E veniamo alle principali forme di cyber manovre *difensive.* Esse non si distanziano, sostanzialmente, da quelle in uso in ambiente cinetico. Unica peculiarità, che non si ritrova altrove, è la difesa con obbiettivo mobile (*Moving Target Defense)*. Questo tipo di cyber manovra difensiva consiste nel modificare continuamente determinate caratteristiche, compresi i sistemi di resilienza, del *target* sotto attacco per rendere più difficile e costoso l'attacco stesso. E' una forma di difesa, questa, che può offrire possibilità di contrattacco.

Altre due forme di CyM difensive sono quella 'perimetrale' e quella 'in profondità'. La prima cerca di creare anelli difensivi per prevenire gli attacchi e proteggere i propri *asset*. La seconda cerca anche di rafforzare i sistemi interni. Sia l'una che l'altra, però, presentano, a differenza della difesa con obbiettivo mobile, la vulnerabilità di essere difese *statiche.* Tipico è l'esempio dell'Estonia che nel 2007, con difese statiche, subì il blocco dei servizi per molti giorni, contrariamente a ciò che fece due anni dopo la Georgia che trasferì, sia pure con un po' di ritardo, i propri siti su *servers* di altri Paesi amici e alleati.

Ulteriore tipo di cyber difesa è quella *ingannevole* di cui un esempio noto è la creazione di *honeypots* che consentono alla parte attaccata di scoprire le tecniche e i metodi dell'avversario.

Ovviamente, tutte queste manovre, offensive e difensive, possono implicare, ed implicano, problemi di sovranità e di diritto internazionale. A prescindere dalla problematica questione di una possibile e consensuale definizione di ciò che debba essere un 'confine' nello spazio cibernetico, è doveroso sottolineare che, nonostante il cyberspazio sia considerato un *global commons*, un sano realismo ci dice che ancora per molto tempo la situazione sarà caratterizzata da forte ambiguità e dalla prevalenza di abusi e della forza sul diritto. E ciò anche nei confronti di Paesi amici ed alleati, a differenza delle manovre cinetiche che non possono essere usate a danno di quelli. In ambiente convenzionale, infatti, atti che restano impuniti nel cyberspazio verrebbero spesso considerati atti di guerra.

Negli ambienti militari degli Stati Uniti c'è un dibattito in corso circa alcuni problemi relativi al possibile utilizzo di armi cibernetiche offensive a livello operativo e tattico. E' un dato di fatto che gli strumenti cibernetici offrono ai responsabili operativi e tattici la possibilità di ottenere risultati ai loro propri livelli a sostegno di una strategia. Sono emerse ed emergono, però, preoccupazioni sull'ammissibilità di usare le CyM offensive a livelli inferiori a quello strategico, anche se si riconosce che esse sarebbero meno costose di quelle cinetiche e che i loro effetti potrebbero essere reversibili.

Le manovre strategiche sono infatti autorizzate dai vertici politici e militari, mentre i comandanti sul campo non possono attendere, per assolvere al loro compito, autorizzazioni che tardano ad arrivare. La soluzione di questo problema potrebbe consistere, quando tecnicamente possibile, nell' attivazione di misure *net-centriche.*

È l'informazione, insomma, e la velocità con la quale essa si diffonde, la caratteristica dell'ICT che consente di superare le asimmetrie nei fattori di potenza. Sono il livello tecnologico e la conoscenza dell'avversario che compensano anche l'inferiorità numerica delle forze convenzionali. L'ICT permette fra l'altro l'integrazione fra le forze di terra, di mare e di aria, per non parlare dello spazio fisico e di quello virtuale, con la conseguenza di razionalizzare l'impiego delle forze e degli strumenti con conseguente riduzione dei costi. Tutto ciò, insieme con l'innovazione tecnologica nei sistemi d'arma, consentirà di parlare di 'rivoluzione negli affari militari' (RMA), filosofia sulla quale s'innesterà, per concretizzarla, la *Network Centric Warfare* che si sviluppa su tre livelli: quello strategico, con il controllo di tutte le dimensioni del terreno di scontro; quello tattico, con la capacità di superare in velocità l'avversario; e quello 'strutturale', con i sensori che consentono lo scambio dei dati in tempo quasi 'reale'.

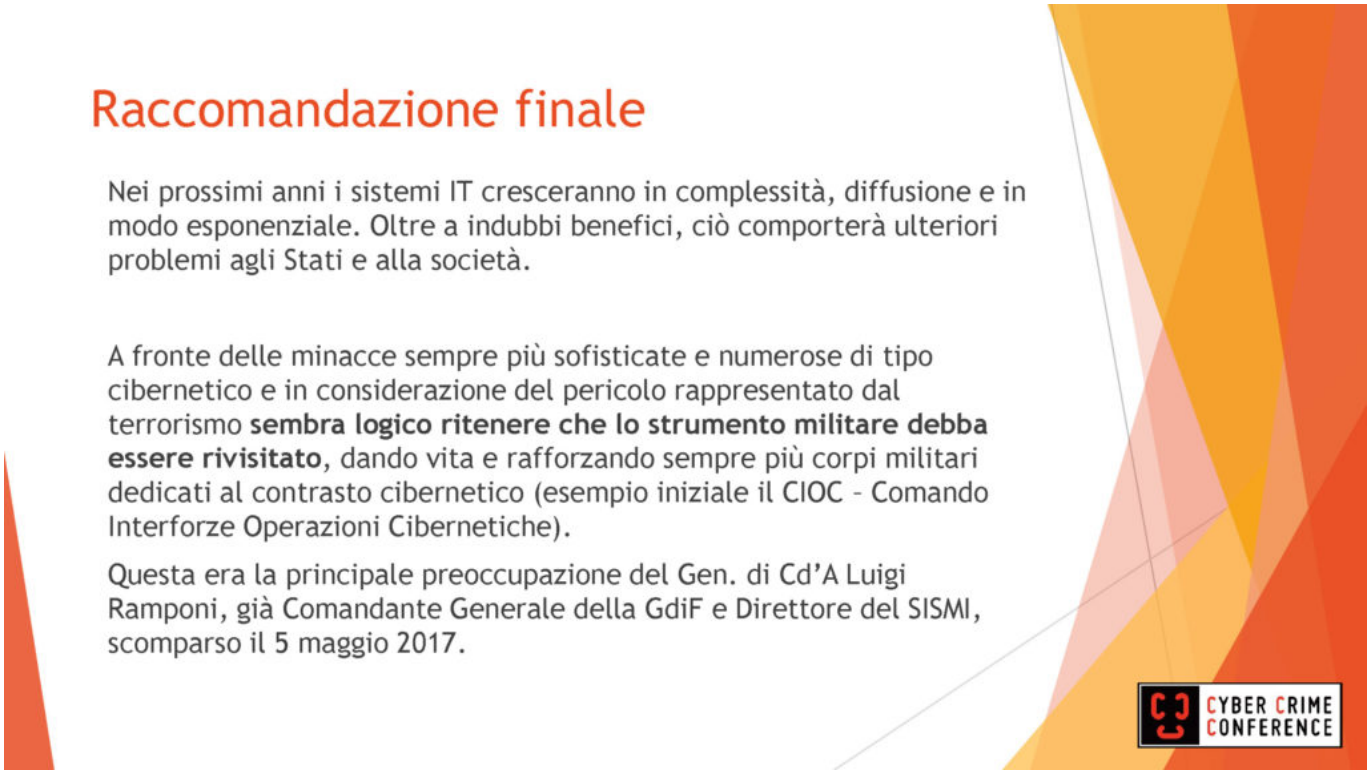
In Italia la NCW ha assunto la forma, meno dispendiosa, della NEC (*Network Enabled Capabilities*) che consente di rendere progressivamente net-centriche piattaforme e mezzi *già esistenti.* Il progetto di 'Forza NEC' dell'esercito italiano è concepito per essere funzionale a tutti i tipi di conflitto, da quelli ad alta intensità alle forme di contrasto al terrorismo transnazionale. Insomma, anziché concepire la NCW come una filosofia per ottenere la superiorità militare come fanno gli Stati Uniti, gli Stati europei guardano alla NEC come ad un modo per accrescere l'efficacia degli strumenti bellici ed ottenere i risultati ricercati.

Per gli Stati europei la guerra 'in rete' ha costi alti, è complessa e sottostà al rischio di perdere efficacia in caso di neutralizzazione anche di una sola funzionalità. Come dimostrano le *lessons learned* dalle operazioni in Afganistan ed Irak, alla fine il fattore umano fa la differenza. Nei conflitti a bassa intensità, inoltre, e soprattutto nel caso di conflitti asimmetrici, la tecnologia perde di valore, se non altro perché non è difficile fornire false informazioni a chi sull'informazione basa la propria superiorità.

Concludo per non andare oltre il tempo concessomi.

A fronte delle minacce sempre più sofisticate e numerose di tipo cibernetico, e in considerazione dell'incombente pericolo rappresentato dal terrorismo, sembra logico ritenere che lo strumento militare debba essere rivisitato. Ai sistemi d'arma tradizionali dovrebbero aggiungersi, a costo di razionalizzare altrove, strumenti più adatti a contrastare gli attacchi di

nuovo tipo, dando vita e rafforzando sempre più corpi militari dedicati al contrasto cibernetico, sia con ulteriori capacità d'intelligence e incrementando, piuttosto, le capacità di difesa anti missile, il numero dei droni d'attacco e da ricognizione e la quantità di forze sòpeciali interforze con relativo supporto di elicotteri e, infine, attuando una maggiore integrazione tra le FF.AA.in funzione anti-terrorismo. Il CIOC (*Centro Interforze Operazioni Cibernetiche*) è un utile e lodevole inizio).



Questo è ciò che pensava una personalità con la quale ho avuto il privilegio di lavorare per anni, il Gen. di Cd'A Luigi Ramponi, già Comandante Generale della GdiF e Direttore del SISMI, scomparso il 5 maggio scorso. Questa è stata la Sua accorata raccomandazione al Governo e al Parlamento fino agli ultimi giorni di vita e io ritengo un mio preciso dovere trasmetterla a tutti Voi.

Umberto Gori - Professore emerito, Università degli Studi di Firenze