INTERNET: IL NUOVO AMBIENTE STRATEGICO ASIMMETRICO

La prima teorizzazione di una rete continentale di computers collegati attraverso "nodi", ovvero un computer in grado di comunicare con altri, è dell'agosto 1962, battezzata Intergalactic Computer Network. Nel 1969 la Defence Advanced Research Projects Agency finanziò il progetto ARPANET, inizialmente con il collegamento di quattro "nodi" che rapidamente si ampliarono a "nodi" oltreoceano (1). Con il Transmission Control Protocol (TCP) e l'Internet Protocol (IP), la fine del 1980 fu l'alba di Internet. Parallelamente alla sua crescita nacquero i primi allarmi sul rischio militare di una decostruzione improvvisa dei confini che una parola nuova declinava: cyberspace (2). Era lo spettro di una forma di guerra mai immaginata, un attacco in grado di paralizzare le infrastrutture critiche di un Paese senza sparare un solo colpo. Negli Stati Maggiori statunitensi dilagò la sindrome di una «*cyber-Pearl Harbour*», rischio che nel 2019 Coats, direttore della National Intelligence Agency, definì non più una vaga minaccia ma una realtà: «the lights are blinking red» (*le luci rosse lampeggiano - ndr*) .

Subito su Internet di mossero le spine dorsali del commercio globale, rendendo il cyber-spazio non più "common good", il "bene collettivo" preconizzato da Licklider e Clark, ma una giurisdizione rivendicata da Stati e società commerciali, sovrapponendosi l'uno l'altra in un concetto ambiguo di proprietà, infrastruttura fisica e dati che la attraversano, dove i tentativi di controllo dei Governi si scontrano con il settore privato e viceversa in un trade-off tra informatizzazione e sicurezza. Da infrastruttura periferica a mondializzazione digitale irreversibile nell'architettura sociopolitica globale, Internet è diventata «*hybrid in nature*», costruendo una nuova «*architecture of world governance*» ("diffusion of power") asincrona con quella dell'ONU. Si evidenziarono le distopie circolanti da più di vent'anni sulla definizione di cyberwarfare, che sfocano le dinamiche e gli sconvolgimenti globali che il termine sottintende. La traduzione italiana "*guerra informatica*", ad esempio, è diminutiva perché riassume due concetti differenti:

- cyberwar, l'attacco cibernetico deliberato ai sistemi di comunicazione e di sicurezza di uno Stato e le sue contromisure cibernetiche (è cyberwar anche il cyber-spionaggio);
- cyberwarfare, l'insieme di cyber-attacchi (cyberwars) autorizzati senza limiti di impiego da un Governo contro infrastrutture informatiche nemiche.

Solo con gli inizi del nuovo secolo gli Stati Maggiori hanno iniziato ad analizzare i rischi del cyberspace e la potenzialità di cyberspace operations a protezione di infrastrutture critiche, difesa nazionale e governance, abbandonando l'assioma «the immediate threat is more corrosive than explosive» (*la minaccia immediata è più corrosiva che esplosiva - ndr*), che aveva permesso ai Governi di muoversi nel cyber-spazio hackerando banche, compromettendo elezioni politiche, rubando segreti militari e know-how industriali. Di fatto, l'area virtuale su cui si muove lo scambio economico e informativo globale si identifica in un acronimo dell'Army War College che definiva il post guerra fredda: *VUCA - Volatility, Uncertainty, Complexity, Ambiguity*.

Dopo anni di incertezza gli Stati Uniti, che bene o male guidano ancora la difesa dell'Occidente, anche se relativizzata dall'attuale Presidenza Biden con una confusione strategica che potrebbe accelerare quell'"*imperial overstretch*" preconizzato da Paul Kennedy, sembrano ritrovare il monopolio tecnologico e militare in quel cyberspazio "armato" e apolare che è stato dominio incontrastato di Russia, Cina, Corea del Nord e Iran, le uniche con cyber capabilities emblematiche di una nuova liturgia della guerra, dimostrata, per la Russia, nelle elezioni presidenziali statunitensi del 2016. Internet ha permesso all'intelligence militare del Cremlino (Unità 26165 e 74455 del GRU) di mettere in atto una guerra di propaganda senza precedenti, un'operazione da manuale, massiccia e sofisticata di hackeraggio e profilazione mirata che ha raggiunto milioni di elettori, attraverso migliaia di bots (3) su forum e social networks, dimostrando la capacità di un Governo di lanciare operazioni invisibili su vasta scala atte a influenzare/destabilizzare la politica interna di un altro Governo. In particolare ha evidenziato la debolezza della intelligence community statunitense nel non avere percepito la minaccia che le simulazioni avevano largamente disegnato (l'intelligence è la scienza del "prima").

Cyber-attacchi sono stati lanciati quando non potevano essere utilizzate strategie tradizionali, di fatto delle proxy wars dove il "proxy" è Internet. L'esempio migliore è del 2014, quando la Corea del Nord ha hackerato la rete Internet della Sony Pictures, distrutto i suoi server e fatto passare alla stampa informazioni riservate, come rappresaglia per l'uscita del film "The Interview", una dissacrante commedia che racconta l'assassinio di Kim Jong-Un. Per mesi, Sony Pictures ha dovuto lavorare con carta e penna per ricostruire una nuova infrastruttura informatica (hardware, software e rete). Ancora nel 2016 gli hackers del Bureau 121, l'agenzia di guerra cibernetica creata nel 1998 da Pyongyang, sono riusciti a sottrarre decine di milioni di dollari da istituti bancari (Vietnam, Filippine, Bangladesh) per bypassare i tentativi di embargo imposti dagli Stati Uniti .

Per bilanciare la difficoltà interna di innovazione,

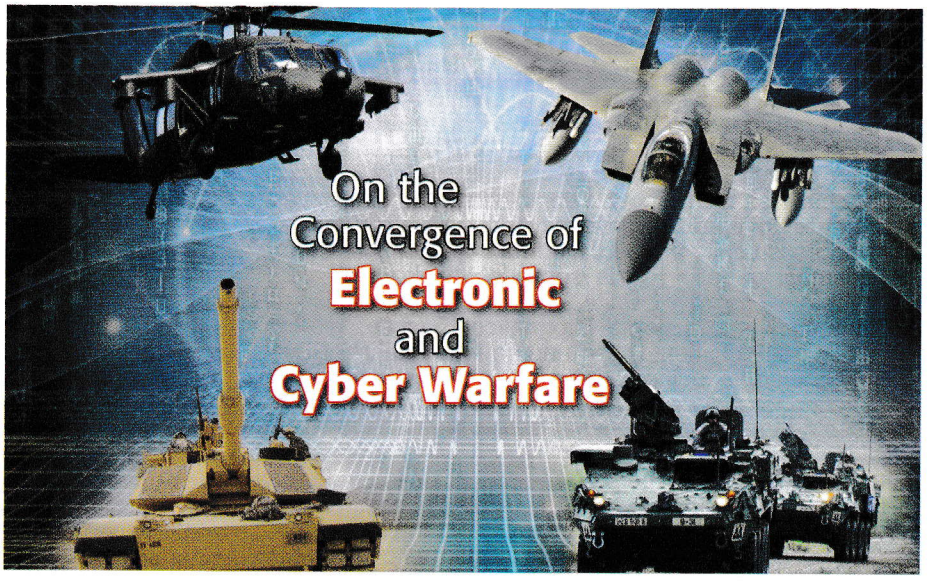
nell'ultimo decennio la Cina ha aumentato esponenzialmente la propria capacità di cybertheft (furto informatico), sottraendo proprietà intellettuali (brevetti e know-how) soprattutto a Stati Uniti, Gran Bretagna e Germania. È del 2003 il primo attacco in profondità di cyber-spionaggio scatenato da Pechino contro reti informatiche di Agenzie di Governo statunitensi (Redstone Arsenal, Sandia National Laboratories e NASA) e di Defense Contractors (Lockheed Martin), attacco che ha coinvolto anche la Gran Bretagna. Secondo un report del 2017 della *Commission on the Theft of American Intellectual Property*, le perdite dovute a cybertheft, gran parte attribuibili alla Cina, solo negli Stati Uniti valgono medialmente 500/600 miliardi di dollari l'anno. Tutte queste operazioni avvengono in quella "gray zone of conflict" che non è né guerra né pace, ma una guerriglia (guerra asimmetrica per eccellenza), una «fourth-generation warfare» su cui si muovono parallelamente operazioni militari tradizionali che attingono sempre più a cyber capabilities.

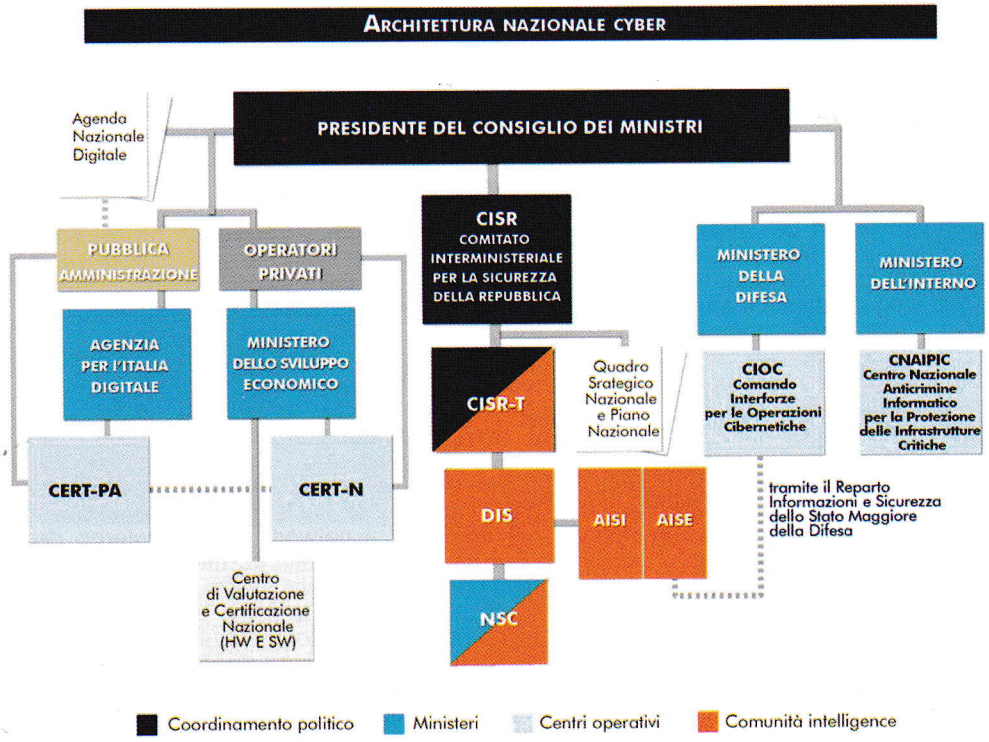
Nel bombardamento NATO del 1999 sulla Jugoslavia, una cyber unità del Pentagono ha mascherato l'arrivo degli aerei statunitensi hackerando i sistemi di difesa aerea della Serbia, e nella lotta contro l'ISIS ha utilizzato non meglio specificate cyberbombs (i dettagli sono ancora "classified"), confermate nel 2016 dal vice-Segretario della Difesa Work. «The first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains: Land, Air, Sea, and Space» (*il primo caso nella storia di attacco coordinato nel ciberspazio sincronizzato con le principali azioni di combattimento in altre aree di guerra: Terra, Aria, Mare, Spazio - ndr*), che declinò l'assioma della hybrid warfare «before the gunfire, cyberattacks» (*prima del fuoco delle armi, cyber attacchi - ndr*), fu l'invasione russa della Georgia nel 2008. Una «hacker militia» pseudo revanscista iniziò un profondo cyberattack - DDoS e SQL injection (4) - coordinato militarmente, silenziando gli accessi WEB e tutte le stazioni televisive della Georgia, così che la popolazione non si rese conto dell'arrivo dei carri armati russi, isolando contemporaneamente le catene di comando e controllo nonostante un tentativo di countering cyber attack a targets moscoviti da parte di hackers georgiani. L'assalto russo continuò contro le banche, costringendo il sistema di interscambio internazionale a chiudere ogni transazione con Tbilisi. Di fatto, la Georgia fu isolata per quasi tutta la durata del conflitto. Sempre alla Russia (Unità 74455) è imputabile l'hackeraggio che bloccò la rete elettrica ucraina nel 2015.

Nel 2009 è stata scoperta una rete di cyber spying (GhostNet) distribuita su 1295 computer infettati da un trojan (gh0st RAT) in 103 Paesi, la cui infrastruttura di controllo era su server dell'isola di Hainan (Cina). Tutti i targets erano di alto profilo: ambasciate, Ministeri degli Esteri, organizzazioni non governative. La certezza dell'attribuzione delle responsabilità rimase difficile per la capacità con cui gli hackers avevano coperto le proprie tracce, grazie ad una botnet che coinvolgeva decine di Stati.

La dipendenza totale da Internet ha insito il rischio di un cyber attacco alle reti di comando e controllo militare, che interdirebbe la capacità di proiezione esterna difensiva o di contrattacco, lasciando disconnesse le proprie forze sul campo. In questa ottica, gli Stati Maggiori avanzati concentrano le ricerche sullo sviluppo di cybertools (cyberweapons) gestiti al di fuori del cyberspazio da una Intelligenza Artificiale (AI), in grado di superare l'uso esclusivo di una rete (ad esempio Internet), risolvendo il diallelo strategico del "cyber first strike": un sistema attaccato si auto-protegge disconnettendosi immediatamente dalla rete nel momento subito successivo alla percezione dell'attacco, rendendo impossibile un contro-attacco e quindi il proseguimento del conflitto. Un cybertool esterno ad una rete e controllato da una AI "addestrata", potrebbe prevenire/ridurre un cyberattack tracciando il malware e disabilitando la fonte, con la capacità di scatenare effetti dirompenti sul nemico disattivando e/o modificando le sue reti e gestendo contemporaneamente attacchi convenzionali sottostanti anche altamente sofisticati. Questa necessità si è evidenziata nel 2005 con gli hacking-attacks al Pentagon's Transportation Command di mano cinese, probabilmente anche russa e forse iraniana (APT33) (5), rivolti soprattutto a testare le difese delle sue reti. Ne ammise la necessità anche il Segretario alla Difesa statunitense Gates, quando fu costretto a confermare nel 2008 l'attacco di hackers russi penetrati in profondità nel SIPRNet, il network segreto interno del Pentagono. Per tre settimane tutta la rete fu chiusa e ci vollero 14 mesi per bonificarla dal worm. E un cybertool avrebbe evitato che nel 2011 la base in Nevada, che gestisce i voli da remoto della flotta statunitense di droni *Predator* e *Reaper*, fosse attaccata da un trojan di key-logging (6) sfuggito allo *Host-Based Security System*, che registrò tutte le istruzioni trasmesse ai droni in missione sull'Afghanistan, ritrasmettendole all'esterno su rete aperta (Internet). La fonte non fu mai rintracciata, né fu mai quantificato il volume di dati ultrasegreti rubato.

Va sfatato un postulato caro agli Stati Maggiori occidentali: la cyberwarfare non fa vittime. È vero che nessuna guerra cibernetica ha ancora mietuto vittime nel senso classico della definizione di guerra, ma quando e se si scatenerà avrà vittime collaterali anche maggiori. Il cyber-battlefield non sarà più uno spazio definito, ma coinvolgerà l'intera Nazione attaccata. Prima mossa di un cyber-attack sarà il tentativo di un cut-off totale dei suoi Comandi militari con un worm contro le sue reti elettriche, con il rischio che il malware utilizzato possa diffondersi oltre gli obiettivi previsti con un cut-off generalizzato che colpirebbe ospedali, catene di approvvigionamento di beni di prima necessità e impianti domestici, ovvero tutto quello che è connesso alla rete. Non è uno scenario remoto: nel 2017 Petya, una famiglia di malware russa destinata a compromettere il sistema produttivo ucraino diffusa attraverso un semplice software di contabilità, si è trasmessa a macchia d'olio via Internet anche alle azien-





de occidentali fornitrici di Kiev. Il conglomerato marittimo danese Maersk (trasporto, cantieristica, energia), solo per il suo settore, ha stimato danni tra i 200 e i 300 milioni di dollari.

Più grave, per i rischi connessi, fu il primo atto storico di cyberwar. Nel 2010 Stuxnet, un worm intelligente multitask di architettura estremamente complessa, ufficialmente senza paternità ma di mano quasi certamente israelo-statunitense, infettò i controlli logici Siemens delle centrifughe della centrale nucleare iraniana di Natanz. Per un errore, Stuxnet si trasmise via Internet in tutti i Paesi fornitori degli impianti industriali del programma atomico di Teheran, ma il rischio maggiore fu una Černobyl iraniana al riavvio delle centrifughe. L'attacco cyber russo alla Georgia del 2008 rischiò di diventare un confronto diretto Stati Uniti-Russia. Per rompere l'accerchiamento cyber di Tbilisi, Google ospitò su un suo server in California il sito ufficiale del Presidente Saakashvili, mentre quello del Ministero della Difesa fu ospitato ad Atlanta su un network privato (Tulip Systems) e quello del Ministero degli Esteri su un server estone. Se uno dei malware utilizzati dalla Russia nell'attacco, sfuggito al controllo come Stuxnet o Petya, avesse colpito a cascata la flotta server ospitante gli spazi digitali georgiani, gli Stati Uniti lo avrebbe considerato un attacco alla propria sicurezza nazionale, reagendo di conseguenza. Nell'aprile 2007 l'Estonia subì il primo esempio di «*politically motivated digital attacks*» che coinvolse tutta la popolazione, una rappresaglia russa perché il Governo aveva deciso di abbattere il memoriale dell'ingresso delle truppe dell'Armata Rossa nella piazza Tõnismägi di Tallinn nella seconda guerra mondiale: il "*Soldato di bronzo*"). L'Unità 26165 del Cremlino mise offline tutto il suo sistema informatico (banche, giornali, Ministeri e Parlamento) con una serie di attacchi DDoS, dimostrando la vulnerabilità di una società altamente interconnessa alla rete (7).

Se fino ad oggi le cyberwars non hanno fatto vittime fisiche, il rischio di coinvolgimento di civili si è elevato in modo esponenziale perché sempre più infrastrutture a tutti i livelli, politico-economico-sociale-finanziario-militare, tendono ad essere interconnesse e interdipendenti, dalle reti elettriche, agli ospedali, all'Internet of Things (8) e al meno avveniristico di quanto si pensi Internet of bodies (9), tutti obiettivi potenziali. In una Internet-war perdono significato i due fondamenti del diritto internazionale, *Jus ad bellum* e *Jus in bello*, permanendo unicamente il labile «plausible deniability» (*negazione plausibile*).

Strutture avanzate governative e private, consapevoli delle minacce della rete, hanno sperimentato sistemi "air gap" (*intercapedine*), isolando fisicamente una infrastruttura informatica critica dalle reti Internet, che però deve ricevere aggiornamenti esterni (software/dati) su reti. È quindi possibile saltare il "gap" tramite risonanza acustica, sfruttando le radiazioni magnetiche a bassa frequenza o usando tecnologie ottiche come il LaserShark di ultima generazione (10) (2021). Alcuni Governi hanno creato reti Internet proprie, con risultati contrastanti. Ne è un esempio il Great Firewall cinese (11), progettato per la censura preventiva dell'accesso a Internet, dimostratosi eludibile da reti virtuali private (VPN). Lo stesso vale in Iran, dove le Autorità hanno istituito una rete restrittiva "ḥalāl" (lecita), anche questa bypassabile da reti VPN. Non sempre l'investimento nella cybersecurity è stato considerato primario, nonostante le perdite colossali, miliardi di dollari di proprietà intellettuale sottratti ogni anno non solo alle aziende private, ma anche alla Difesa, che ne ha indebolito il profilo strategico, costringendola a riprogettare i piani di cyber-difesa, ignorando nella maggior parte dei casi quanto e fino a dove l'avversario era penetrato in profondità nei suoi sistemi. Le soluzioni adottate per contrastare le vulnerabilità delle reti non hanno garantito fino ad oggi sicurezza, rendendo contradditoria («nonsense») la declinazione di una cyber-strategy in un sistema globale anarchico (global cyber anarchy).

Solo nel 2010 l'Italia ha evidenziato il problema della minaccia cibernetica, intesa come militarizzazione della rete, con una Relazione sulla politica dell'informazione per la sicurezza sulla necessità di una pianificazione strategica a livello nazionale con una «*ridefinizione delle attività delle strutture esistenti*» e una «*rimodulazione delle attuali competenze e responsabilità*». Interpretando con un approccio semplificato il concetto statunitense di Network Centric Warfare (NCW, guerra netcentrica), la Difesa costruì presso lo SMD il progetto CERT (*Computer Emergency Response Team, Comando C4 Difesa, 2004*). Dopo l'ondata di attacchi di cyber-spionaggio contro obiettivi nazionali strategici (diplomazia, difesa, aerospazio, telecomunicazioni, energia), ma anche realtà imprenditoriali minori, Roma adottò con due anni di ritardo la "Direttiva NIS" europea (12). Per indolenza di policymakers e CEO di bassa capacità di imprenditoria cybersecurity, burocrazia cronica, vertici militari tra acronimi sovente fantasma, inconcludente il partenariato pubblico-privato per la costituzione di un Cyber Range nazionale, nonostante gli allarmi in crescita (13), l'Italia continua a mancare di una struttura di cyberwarfare sinergica operante ad ogni livello (prevenzione, difesa,

attacco), anche per la difficoltà di ibridazione cyberdefense-cybersecurity dove le competenze militari e civili si sovrappongono. Se è migliorata la capacità di identificare una minaccia e di contrastarla (sicurezza passiva), è ancora carente e frammentata la funzionalità di attacco, fatto che la pone al 13° posto nel Regional Rank europeo.

Nello stesso quadro multilaterale UE, la coesistenza tra azioni comunitarie e intergovernative rende problematico definire un ambito preciso di azione della difesa cibernetica, ciascun Membro interpretandola con metriche diverse, senza dimenticare che l'infrastruttura del cyberspazio è principalmente di proprietà di aziende private esterne alla UE. Due esempi chiariscono la dissimmetria integrativa. In Francia, 5° nel Regional Rank europeo, l'*École spéciale militaire de Saint-Cyr Coëtquidan* che forma i quadri della *Armée de Terre* è allineata sul mitologema di Thomas Rid: «la cyberguerre n'a pas d'autonomie stratégique, elle ne peut exister par elle-même, elle n'est que l'interprétation de la guerre des hommes par les moyens du cyber» (*la cyber guerra non richiede autonomia strategica, può esistere per sé medesima, essa non è che l'interpretazione della guerra umana tramite il cyber spazio - ndr*). La «*cyber security strategy*» della Gran Bretagna, 1° nel Regional Rank europeo, è invece allineata con la dottrina statunitense di un NCW ancora più integrato (14). Con un cash down di quasi due miliardi di sterline per il quinquennio 2016-2021 «*to strengthen the UK's cyber ecosystem*» , che segue quello di poco sotto il miliardo del quinquennio precedente, Londra è «*the world's third-ranked cyber power, behind only the United States and China*».

Nel 1999 Qiao Liang e Wang Xiangsui pubblicavano la loro visione della prossima guerra futura: un "*ambiente strategico asimmetrico*" con azioni iniziali non militari senza limiti (finanza e attacchi informatici) per destabilizzare l'equilibrio del nemico, provocando disordini sociali e il collasso del suo governo. L'intervento militare era previsto solo a risultato ottenuto. Premonitore di un cyber multi-battlefield? Forse, dato che la maggioranza dei cyber-attacchi ha origine in Cina, scatenati dalla supertecnologica Unità 61398. Nell'ottica di una cyber-guerra permanente in funzione offensiva e difensiva, sull'assioma «*no satellites, no fight*», Pechino ha in costruzione una stazione spaziale auto-prodotta e completata entro il 2022, che potrebbe eludere/ridurre la conseguenza del "cyber first strike".

La competizione geopolitica per la «*governance/sovereignty over cyberspace*» è il ritorno ad una Cold War, una Cold Hybrid War latente, insidiosa, senza confini e pluri/apolare, dove è ancora presente il "blocco sovietico" tradizionalmente incapace di soft power, cui si sono aggiunti altri "blocchi-Stato/non-Stato", gruppi terroristici di difficile identificazione e hackers trasversali deideologizzati, tutti moltiplicatori di forze in grado di portare operazioni offensive multiple da qualsiasi angolo del cyber-spazio. L'avvento delle nuove tecnologie offre potenzialità uniche, ma anche vulnerabilità uniche per una società civile che vive in un "ambiente strategico asimmetrico" con confini tra avversari ed alleati sempre più fluttuanti, la cui difesa è ancora "work in progress".

dott. **Tomaso Vialardi di Sandigliano**
(*Presidente Federazione Biella e Vercelli*)

NOTE

1 - L'Italia fu la quarta Nazione europea a connettersi in rete (30 aprile 1986) con un finanziamento del Dipartimento della Difesa statunitense che voleva collegare i Comandi militari considerati strategici in Europa (Norvegia, Regno Unito, Germania, Italia).

2 - Tralasciando le fisime filosofiche su una definizione univoca, cyberspace esprime lo spazio virtuale dove interagiscono computers connessi ad una rete (Internet), diventando la *"quinta dimensione della conflittualità dopo terra, mare, aria e spazio"* (global commons) riconosciuta dalla NATO il 14 giugno 2016. Come conseguenza, si dovrà integrare il cyberspace nella *"clausola di difesa collettiva"* dell'articolo V (recepita ambiguamente nella Sez. 2, art. 42, par. 7 del Trattato UE di Lisbona).

3 - Software specialistico che può eseguire autonomamente azioni di tweeting, re-tweeting, liking, following, unfollowing e direct messaging con altri accounts. In scala minore, un esempio in Italia si è avuto nella narrazione giornalistica della "Bestia" gestita da Luca Morisi che avrebbe aiutato la crescita dei consensi di Matteo Salvini.

4 - DDoS-attack (Distributed Denial-of-Service) è un attacco informatico multiplo in cui si fanno esaurire le risorse di un sistema che fornisce un servizio (ad esempio una rete Internet), attraverso una rete (botnet, short per robot network) di computers "ignari" (zombie) creata da uno o più hackers, infettati in precedenza e attivati da remoto (botmaster). SQL injection è un attacco paragonabile al DDoS, più sofisticato perché necessita di una botnet più ristretta, consentendo un'azione più diretta ed immediata.

5 - Advanced Persistent Threat 33 è l'unità di cyber spionaggio iraniana attiva almeno fin dal 2013.

6 - Software che controlla e registra la sequenza dei tasti digitati sulla tastiera di un computer.

7 - Tallinn chiese l'applicazione dell'Articolo V del Trattato NATO, parificando per la prima volta un attacco cyber a un attacco armato. La NATO "rifletté", in attesa di una *«formazione del consenso della definizione comune sulle strategie e gli strumenti per affrontare le nuove minacce»* [sic!]. Come consolazione, la NATO diede a Tallinn la sede del CCDCOE (2008).

8 - IoT: processo di interconnessione a Internet di oggetti di utilizzo quotidiano ("things", "cose"), da quelli usati in casa (domotica), alle risorse in ambito medico (IoMT, Internet of Medical Things), e ai dispositivi "indossabili" come smartphones e tablets.

9 - IoB: tecnologia che prevede l'introduzione nel corpo di dispositivi (body melded) che utilizzano i segnali elettrici che si trasmettono attraverso il tessuto corporeo, creando un network tra esseri umani connesso a Internet.

10 - Mentre la maggior parte delle tecnologie di attacco a un sistema "air gapped" consente solo una comunicazione unidirezionale, l'infiltrazione o l'esfiltrazione di dati, LaserShark impiega come ricevitori i LED integrati su qualsiasi dispositivo, permettendo un attacco con una comunicazione bidirezionale.

11 - Cfr. T. Vialardi di Sandigliano, *"Il dilemma dell'autoritarismo digitale"*, in "Il Nastro Azzurro" n. 1, 2021.

12 - Direttiva NISUE 2016/1148 recante *«misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»* adottata il 18 maggio 2018.

13 - *«L'impatto economico [degli attacchi cibernetici] supera il 6% del PIL mondiale e la cifra potrebbe essere sottostimata»*, Clusit, Rapporto 2021.

14 - Nel NCW più avanzato il networking (sistema di collegamento in rete di più elaboratori, comprendente piattaforme, sistemi operativi, protocolli e architetture di rete) è primario sui networks (reti di collegamento), perché permette la gestione coordinata di più Comandi geograficamente lontani nelle operazioni «in and through cyberspace», con una propagazione dello spettro militare globale e istantaneo (full-spectrum dominance), dove ogni soldato è un «Individual Combat System» integrato del networking. In questa modellazione lo spazio operativo cyber viene suddiviso in tre livelli (layers), distinti ma interrelazionati: physical network, logical network, cyber-persona.