I POSSIBILI EFFETTI SOCIALI DELLA GUERRA POST-EROICA E DELLE INGERENZE COGNITIVE

Il palese processo di decentramento della distribuzione del potere e la propagazione dei centri di comando e di influenza geopolitica, è la consecutività alla globalizzazione. La multipolarità è la principale causa dell'erosione allo Stato Sovrano, con la proliferazione di attori non statali assunti al rango di protagonisti delle relazioni internazionali. La ragione di tale mutazione è identificabile nell'accrescimento delle reti informatiche e più in generale, delle comunicazioni. La tecnologia ha agevolato il rafforzamento delle caste politiche a livello globale, dove gestire le transazioni finanziarie e l'implementazione dei sistemi d'arma incarnava la supremazia. La diffusione delle reti elettroniche a basso costo, ha leso questo stato di fatto, agevolando il decentramento geopolitico nello spazio virtuale per l'affermazione di un potere parallelo a quello istituzionale. La costante ricerca del primato sulla rete potrebbe collidere fra gli attori principali, ingenerando un nuovo tipo di scontro combattuto su internet. La politica estera non può prescindere dalla conoscenza degli avversari e tantomeno degli alleati. L'asimmetricità della minaccia potrebbe però instaurare estemporanee comunioni di intenti, soprattutto a causa delle profonde difficoltà di arginare gli attacchi cibernetici. Per tale motivo, è probabile che la cooperazione internazionale potrebbe svolgere un ruolo basilare nel combattere tale fenomeno, in questa materia è già attiva la collaborazione fra NATO ed Unione Europea, dove l'Italia svolge un ruolo predominante che intende perseguire anche nel lungo periodo con investimenti nel settore della Difesa. La ripartizione degli stanziamenti previsti nella Legge di Stabilità, sulla base di quanto riportato nel testo definitivo, possono essere per il momento solo ipotizzabili, gli investimenti effettivi sarà possibile valutarli con precisione solo nella prima parte del 2014, ma alcuni passaggi sono abbastanza interpretabili: fra questi, l'erogazione del denaro per il settore dell'elettronica potrebbe significare lo sviluppo della guerra cibernetica. Questa è l'unione di tutte le attività che anticipano la conduzione delle operazioni militari. Ciò vuol dire la distruzione dell'informazione e dei sistemi di comunicazione avversari con attacchi ai server allo scopo non solo di ascoltare le trasmissioni, ma anche per la sostituzione dei contenuti delle stesse con indicazioni manipolate a svantaggio degli intercettati. La capacità di gestire l'informazione e l'indebita acquisizione di dati potranno costituire nuove gerarchie di potenza con azioni chirurgiche in grado di alterare le fonti del sapere su cui si fondano le società contemporanee. Nel 2007, l'Estonia fu oggetto di un devastante attacco cibernetico che coinvolse indistintamente sia il settore pubblico quanto il privato. Questo principiò un nuovo scenario bellico che doveva essere regolamentato e la NATO invitò un gruppo di esperti a Tallin, in Estonia, i quali realizzarono il cosiddetto Manuale Tallin. Questo definisce principalmente gli algoritmi di azione in previsione di aggressioni: atti mirati all'elusione dei sistemi informatici; operazioni cibernetiche complesse tali da causare non solo distruzione di materiali ma anche ricadute estendibili ad un indebolimento delle forze armate avversarie, ponendo quest'ultime in pericolo di vita; eventi indiscriminati a danno di personale non direttamente coinvolto con le ostilità. Questi passaggi, furono argomentati nell'Assemblea Generale delle Nazioni Unite del 2012, dove si valutarono i rischi connessi agli attacchi cibernetici contro siti come le reti elettriche o gli impianti nucleari, con il conseguente impatto sulla popolazione civile. Per regolare l'uso indistinto della guerra cibernetica, furono identificate regole per lo più legate alla deterrenza, dove lo Stato colpito da una illecita aggressione informatica, il cui effetto sia equiparabile ad un intervento armato, ossia con perdite umane, può esercitare il diritto

di autodifesa anche con armi convenzionali. Le autorità russe, hanno definito il testo del manuale come un documento che, prevedendo azioni e reazioni, possa legittimare un nuovo tipo di conflitto. Al contrario sarebbe necessario allontanare il pericolo della militarizzazione dello spazio virtuale, ma già dal 2010 gli statunitensi hanno composto il Defence Department's Cyber Command, inquadrato come sottodivisione del Comando Strategico, al fine di implementare le capacità difensive e migliorare le tecniche per lanciare attacchi cibernetici. In cooperazione con i servizi segreti, il Cyber Command ha accesso a 15.000 reti informatiche in 4000 basi militari distribuite in 88 Paesi e prevedrà un organico di mille addetti qualificati alla difesa della Nazione. Anche la Gran Bretagna ha istituito una nuova unità, con il preciso intento di sviluppare una capacità offensiva, a scopo di deterrenza. L'esborso economico è stato rilevante, ma ha già prodotto risultati positivi: infatti, secondo dati ufficiali della Difesa, la Gran Bretagna ha eluso circa 400 mila minacce nel solo 2012, rivolte per il 93% ai più importanti gruppi industriali. L'Estonia si è dichiarata la prima vittima di questa nuova frontiera bellica, indicando come colpevole la Federazione Russa, ma senza riuscire a provarlo, come il Governo statunitense ed israeliano hanno declinato le accuse a loro rivolte per le ingerenze cibernetiche, con i virus Flame e Stuxnet, al diritto iraniano di sviluppare il processo di nuclearizzazione. Il bruco Stuxnet, ha rappresentato un salto generazionale in quanto sembra che sia riuscito ad infettare 45.000 sistemi di controllo industriale della Siemens, agevolando gli incursori alla manipolazione dei processi tecnici degli impianti nucleari. Il mercato per migliorare le risorse informatiche, vale 10 milioni di dollari e tende allo sviluppo di strumenti adatti alla distruzione, interdizione, degradazione ed usurpazione delle reti di mappature, come precisato in un documento dell'USAF. Dunque la guerra cibernetica è definibile come un nuovo livello di scontro, dove l'arma più semplice può essere una chiavetta USB. Nel 2008 con l'ausilio di questo semplice strumento, venne lanciato uno dei più forti attacchi contro i computer militari degli USA. Una spia collegò una penna USB ad un pc portatile in una base statunitense del Vicino Oriente e penetrò tutti i sistemi classificati. Una testa di ponte digitale, da cui migliaia di dati vennero trasferiti sotto il controllo di un'altra Nazione. Un atto che si configura come una capacità d'influenza sull'operato della Nazione bersaglio, e può diventare anche politico e tattico sulla percezione dell'informazione stessa quanto sui progetti tecnologici in essere. È un passaggio dalla guerra di annientamento al nuovo concetto di operazioni diverse dalla guerra classica, il quale potrebbe ingenerare effetti psico-sociali imprevedibili, dove la sicurezza dell'individuo non sarebbe garantita, dunque paragonabile al pericolo di un conflitto nucleare. Una non-guerra combattuta nello spazio virtuale dove la vittoria è più rappresentativa di uno scontro militare, oppure, citando Luttwak, la guerra post-eroica. Quest'ultima, probabilmente non potrà prescindere dal sistema finanziario e dallo sviluppo tecnologico, in particolare quello applicato al commercio ed ai servizi. Di fatto, le armi informatiche potranno essere le capacità e le identità civili. L'obiettivo della disinformazione e della guerra cibernetica si prefissa la non distruzione dello Stato avversario, ma un'azione psicologica contro il nemico nel proprio territorio. Una politica della comunicazione volta a demotivare il competitore, ma a lasciare intatte le sue risorse. Un concetto antico, che risale a Sun Tzu, ignorato nelle guerre convenzionali, ma ripreso nel mondo contemporaneo, dove salvaguardare le risorse tecnologiche e naturali dell'antagonista, per essere tratte dalla parte del vincitore, rappresentano la nuova filosofia della conquista. Ad inizio 2013, nel Meeting sui rischi mondiali presentato dal Forum Economico Mondiale, il conflitto asimmetrico

dell'informatica è risultato essere una minaccia tecnologica e geopolitica, la quale potrebbe tendere al fallimento del governo globale, laddove la guerra cibernetica possa tramutarsi in un'arma per la disinformazione attraverso internet od anche a disposizione dei terroristi. Tale scenario è definito come: incendio digitale incontrollato in un mondo iperconnesso. In definitiva, ciò si traduce nel provocare il caos nel mondo reale, nell'uso non corretto di un sistema aperto e di semplice accesso come internet. La guerra dell'informazione si prefissa operazioni sulla psicologia sociale, ossia influenzare emozioni e motivazioni dell'antagonista in modo da poterne controllare e prevenire i comportamenti. Gli attori più agguerriti, però, sono ancora gli Stati, perché lo spionaggio ed il sabotaggio cibernetico necessitano ancora della determinazione e di una logica costi-benefici propri di una Nazione. Una diversa concezione delle relazioni conflittuali tra Stati, una capacità cognitiva che attraverso l'elettronica e l'informazione tende a produrre consensi sia in patria che sugli avversari. Le aggressioni informatiche per la loro natura, potranno verificarsi tra tutte le parti in causa e contro ognuna di esse. Gli stessi soggetti potrebbero divenire da attaccanti ad attaccati, dove gli obiettivi saranno gli Stati e gli sconfinamenti nella privacy dei singoli cittadini e delle imprese. Questo scenario avrà come risultanza una necessaria crescita del controllo della sicurezza interna, andando a rendere sovrapponibile i concetti di sicurezza e difesa. Un conflitto virtuale è stato sofferto dalla Corea del Sud, dove furono presi di mira i bancomat ed i siti web. Inizialmente sembrava un semplice disservizio causato dal sovraffollamento di traffico; solo al perdurare dell'evento apparve l'evidenza di una aggressione dei cosiddetti guerrieri cibernetici. Il primo dato che si evince è il vantaggio temporale di un attacco informatico, in quanto lo Stato bersaglio necessita di un certo lasso di tempo prima di poter accertare la fonte del problema, ciò agevola la distruzione dei dati conservati sui dischi rigidi. La seconda evidenza è la non assoluta letalità di un attacco cibernetico dove, almeno nel caso sud coreano, i sistemi vennero recuperati in pochi giorni. Dunque se queste aggressioni sono relativamente semplici da effettuare, i danni ingenerati sono recuperabili in tempi rapidi, ma è necessario sottolineare che lo Stato bersaglio, anche nel breve periodo di oscuramento informatico, è estremamente vulnerabile in quanto totalmente indifeso. La pirateria cibernetica è anche facile da prevedere: la storia dimostra infatti che a seguito di una disputa politico-militare è sopraggiunto un episodio di indebita intrusione nelle reti informatiche, pertanto questo giustifica la messa a punto di un sistema difensivo. Un esempio è nelle massicce violazioni ai server della Georgia durante la crisi con la Russia, quest'ultimi riuscirono nell'intento di indebolire le capacità di comunicazione dei georgiani. Come manifestato dall'attacco alla Corea del Sud, la guerra cibernetica è estesa anche alle Aziende civili, trasformando di fatto il comparto finanziario e le imprese in un nuovo e più imprevedibile campo di battaglia. Per ottenere dei risultati concreti, al fine di arginare le ingerenze informatiche, è auspicabile che venga istituito un rapporto di collaborazione fra il settore privato ed i Governi, per mettere a punto efficaci strategie di difesa, combinando l'esperienza e l'innovazione tecnologica dei due comparti, allo scopo di prevenire, ma anche di coordinare una reazione comune ad un evento di negazione ai servizi distribuiti in rete. L'acquisizione forzosa di dati sensibili, vuole significare il trasferimento dei segreti di una Nazione, privandola di fatto della sua ricchezza tecnologica a favore di elementi ostili. Un progetto per la regolamentazione della rete è stato presentato nel corso del World Economic Forum, svoltosi a Davos nel gennaio 2014. La Global Commission on Internet Governance, a seguito di quanto argomentato nella città svizzera,

studierà soluzioni in materia di censura e sorveglianza, promuovendo in contemporanea una piattaforma di consultazione attraverso canali istituzionali ed accademici per identificare le necessarie strategie future allo scopo di agevolare gli Stati che intendono lo spazio virtuale come un'occasione di crescita e di scambi mediatici liberi ed aperti. Già dalla scorsa legislazione, il Governo italiano ha autorizzato la formazione di una sezione dedicata alla difesa dello spazio virtuale. Il nucleo per la sicurezza cibernetica è presieduto dal Consigliere Militare del Presidente del Consiglio. L'impatto di internet sull'economia e sulla società è possibile esplicitarlo sulle ricadute seguite alla decisione del Governo egiziano di oscurare la rete durante la rivolta sociale del Febbraio 2011: l'OECD, ha stimato una perdita sugli scambi commerciali pari al 3-4%, con un valore di circa 90 milioni di dollari. La centralità di internet e le implicazioni che potrebbero ingenerarsi dalla sua interruzione, dunque prevarrebbero sulla finanza sino ad invadere la geopolitica. La governance della rete è principalmente dell'ICANN, Internet Corporation for Assigned Names and Numers, la quale suddivide internet in spazi da assegnare ad autorità locali che a loro volta, distribuiscono gli indirizzi IP ai vari Provider. Pertanto, il processo di rinnovamento probabilmente avrà come obiettivo iniziale l'ICANN attraverso il controllo dell'attività stessa e del consiglio di amministrazione sul quale è necessaria una supervisione statale, perché è una società privata no profit e l'orientamento generale sembra quello di mantenerla tale. Nella conferenza dell'ITU svoltasi a Dubai, i paesi membri si sono frammentati in aree geopolitiche ben delineate, in particolare gli USA ed alcuni Paesi occidentali si sono discostati nella proposta di un intervento diretto dello stesso ITU nella governance di internet, palesando una contrapposizione ideologica con Russia, Cina, Paesi arabi ed africani, non solo sui contenuti della conferenza ma sulle metodologie di controllo della rete. Il trattato di Dubai entrerà in vigore nel 2015, pertanto è plausibile supporre che si possa verificare un avvicinamento fra i contendenti ed apportare le riforme decise a Dubai: correzioni alla politica dell'ICANN; implementare le regole internazionali per le telecomunicazioni atte a garantire il rispetto dei diritti umani; disciplinare l'accesso ai servizi della rete. Quest'ultima è l'arma attraverso la quale si possono scatenare attacchi cibernetici e gestire l'informazione, la regolamentazione di internet non negherà l'accesso ai pirati dello spazio virtuale, ma limiterà le conseguenze che potranno scaturire da convincimenti pilotati la cui coercizione è sovrapponibile all'uso delle armi. L'obiettivo del controllo dell'informazione è ledere il sistema cognitivo, dunque non più il corpo ma la mente, ossia instaurare una percezione dell'identità alterata di una persona o di una organizzazione. La risultanza sulla distribuzione di immagini, simboli od informazioni, rappresenta una forte incognita; infatti è prevedibile, ma non certa, la decodifica che i ricettori assegneranno ai singoli eventi: in base al retaggio culturale, alle credenze religiose, al ceto sociale di appartenenza, alla condizione economica personale ed alla società in cui vive, ogni singolo soggetto avrebbe una diversa percezione della falsa realtà mediatica che si desidera imporgli, dunque le reazioni potrebbero non essere quelle pianificate e le implicazioni sarebbero imperscrutabili. Di fatto, gli effetti alle azioni di manipolazione cognitiva occasionerebbero risvolti molteplici e non determinabili. Una minaccia che si estenderebbe a tutte le Nazioni, anche a quelle dalle risorse economiche e tecnologiche non sviluppate. Pericolo che aumenta esponenzialmente in quei Paesi dalla scarsa omogeneità nazionale o fortemente divisi fra etnie culturali e religiose. Gli attori principali dello scenario internazionale, con l'ausilio della guerra cognitiva e cibernetica tendono a rallentare lo sviluppo di una Nazione evoluta

distruggendo le sue tecnologie, un vantaggio competitivo di peso specifico importante nel contesto della guerra post-eroica. Per bilanciare gli squilibri regionali e globali, è stata ipotizzata anche la deterrenza nucleare: ossia creare una compensazione fra Stati basata sulle armi di distruzione di massa che possa trasmutarsi in un equilibrio cognitivo. La parificazione nucleare non escluderebbe in ogni caso le ingerenze cibernetiche, ma si annullerebbe nelle micro conflittualità regionali, le cui cause a volte sembrano distanti dalle logiche dominanti dei Paesi tecnologicamente ed economicamente avanzati. La proliferazione nucleare di un singolo Stato, avrebbe un forte impatto sulla società della Nazione stessa, con il rischio della nascita di gruppi dalla forte identità, pervasi da un super-io tale da indurli ad accettare la distruzione totale e dunque di loro stessi, come strumento razionale per raggiungere il fine prefissato.

Giovanni Caprara

Bibliografia

Roberto Di Nunzio: conseguenze sulla sicurezza interna della guerra dell'informazione, Gnosis.

Lorenzo Maria Pupillo: notiziario tecnico Telecom Italia.

Stefano Epifani: Sicurezza: nasce la Commissione Mondiale sulla Governance di Internet, Tech Economy.

Luca Bellocchio: relazioni internazionali e politica globale.