L'Editoriale

Ing. Francesco Marinuzzi Ph.D.

La guerra informativa o infowar

La guerra è stato sempre un elemento caratteristico della storia dell'uomo. I romani erano soliti dire *si vis pacem para bellum* tanto era viva la dialettica fra periodi di pace e di guerra. Nella nostra civiltà, dopo le due guerre mondiali del secolo scorso, l'Europa ha vissuto uno dei più lunghi periodi di pace tant'è che anche molti detrattori dell'Europa riconoscono, comunque questo regime di pace, come concreto risultato.

Invero, nel tempo le guerre ed in generale le conflittualità tendono a spostarsi non solo geograficamente ma anche concettualmente su altri piani di confronto e di scontro fra gli Stati e fra le Comunità. Da questo punto di vista le olimpiadi ed in generale tutte le competizioni sportive internazionali e nazionali sono anche una valida forma di contenimento ed espressione delle diversità pur nella loro limitatezza.

Una nuova dimensione di confronto, a livello europeo, ad esempio, è stata alla fine del secolo scorso, quella economica con la costituzione della moneta unica che ha visto una forte svalutazione della Lira e un sostanziale riconoscimento del valore del marco tedesco. Qualcuno ha addirittura visto in questo progetto della moneta unica e del connesso regime di austerity, l'ennesimo tentativo germanico di supremazia continentale dopo i due fallimentari del '900.

Dipoi, più recentemente, con la rivoluzione digitale, è emersa la nuova dimensione ***cyber*** con presunti attacchi da parte di hacker di alcuni Stati verso le risorse informative e infrastrutturali più preziose degli altri Stati. Questo ha generato, anche recentemente, un grande dibattito nazionale per la costituzione e il finanziamento di specifiche strutture ed organizzazioni dello Stato dedite alla Cybersecurity. Una tematica e una materia propria degli ingegneri soprattutto del settore dell'informazione ma non solo. Infatti, sviluppare programmi, progetti ed architetture informatiche tenendo in debito conto, fin dall'inizio, le esigenze sempre mutevoli di sicurezza informatica, è un compito molto complesso e tipicamente sistemistico ed ingegneristico dove gli approcci più teorici e, permettetemi di dire, filosofici o giuridici, rischiano di esser rischiosi e dannosi. Digitalizzare, infatti, senza considerare debitamente fin dall'inizio la sicurezza, rappresenta un disvalore generale in quanto aiuta il potenziale hacker a sottrarre, in modo invisibile, quantità incredibili di dati in pochissimo tempo e minimo sforzo rispetto allo scenario classico cartaceo. Troppe volte, anche in posizioni apicali di realtà pubbliche nazionali, vediamo laureati in matematica, fisica, architettura o filosofia se non sociologia e psicologia, senza che l'Amministrazione abbia valorizzato adeguatamente il capitale umano già presente afferente al settore ingegneristico.

Ma negli ultimi anni e soprattutto con le recenti elezioni USA è emersa all'attenzione generale una ulteriore dimensione strettamente connessa alla precedente: la dimensione informativa che genera la ***guerra informativa o infowar***. È sempre esistita ma in modo marginale e/o sinergico con le altre dimensioni come quando la decriptazione delle macchine Enigma, da parte di Alan Turing e del suo gruppo, costituì una svolta del conflitto armato della Seconda guerra mondiale.

Attualmente, invece, sta emergendo come dimensione prevalente, se non unica del conflitto. Alcuni suoi tipici obiettivi sono, ad esempio, l'orientamento e l'opinione delle persone al fine del condizionamento dei momenti elettorali delle democrazie occidentali oppure l'induzione di proteste massive popolari in regimi più rigidi oppure delle variazioni improvvise e forti del mercato azionario su cui speculare. Una informazione, un *tweet* emesso da specifici soggetti può colpire decine di milioni di persone istantaneamente in tutto il mondo, alla velocità della luce e, ricorsivamente ed immediatamente, tutte le persone in relazione con questi attraverso i noti meccanismi di condivisione od inoltro della informazione: può destabilizzare il mercato azionario o quello politico immediatamente. Talvolta la velocità e il danno sono così diretti ed immediati che l'eventuale smentita o precisazione successiva risulta inutile. Inoltre, non sempre l'identità della fonte è stata autenticata ed è successo che personalità anche ai vertici si trovino, loro malgrado, a dover smentire tweet o informazioni emesse, non armoniche con il loro ruolo, dal loro account violato. Pertanto, la garanzia della sicurezza informatica e cyber diventa ancora più critica e fondamentale in quanto se violata può potenziare enormemente l'infowar.

Il dibattito attuale nazionale è ancora rimasto alla cyberwar e il problema dell'infowar viene da molti ancora non focalizzato o scambiato per la tematica delle notizie false o fake news. Il successo dell'Osservatorio di Andrea Ceccherini, del blog *Il Disinformatico* di Paolo Attivissimo, che si definisce cacciatore di bufale, sono sintomatici del problema ma non rappresentano, a dire dello scrivente, pur lodevoli, una sufficiente risposta rispetto alla posta in palio. Neanche la rimozione o il blocco immediato del profilo social è una valida soluzione perché pur apparentemente efficace nell'immediato, solleva seri problemi in termini di trasparenza, appellabilità delle decisioni e distribuzione del potere fattuale. Non è un caso che molti parlano dello stato attuale come feudale, digitale, sovranazionale o addirittura *oltre le nazioni* quasi un ritorno agli imperi del Settecento.

Il problema è certo politico ma anche e soprattutto tecnologico ed informatico viste le velocità dei colpi e dei contraccolpi della Infowar. Se gli Stati vogliono sopravvivere e contrastare il potere di influenza degli imperi digitali e soprattutto garantire una vera libertà di opinione e di giudizio devono avviare iniziative strutturate e sinergiche con quelle relative alla cybersecurity dove gli ingegneri possono e devono giocare un ruolo decisivo essendo gli unici, praticamente, in grado di progettare e realizzare complessi sistemi, in tempo reale, di protezione, difesa e/o di preventivo attacco dei soggetti autori o presunti tali della infowar.

Ora, soprattutto qui in occidente siamo ancora troppo inermi ai bombardamenti informativi ai quali possiamo giusto opporre una sana e temporanea indifferenza con un approccio disincantato o di *transurfing*.

Francesco Marinuzzi Ph.D.
Direttore Editoriale