Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 91 (2019)
Heft: 5

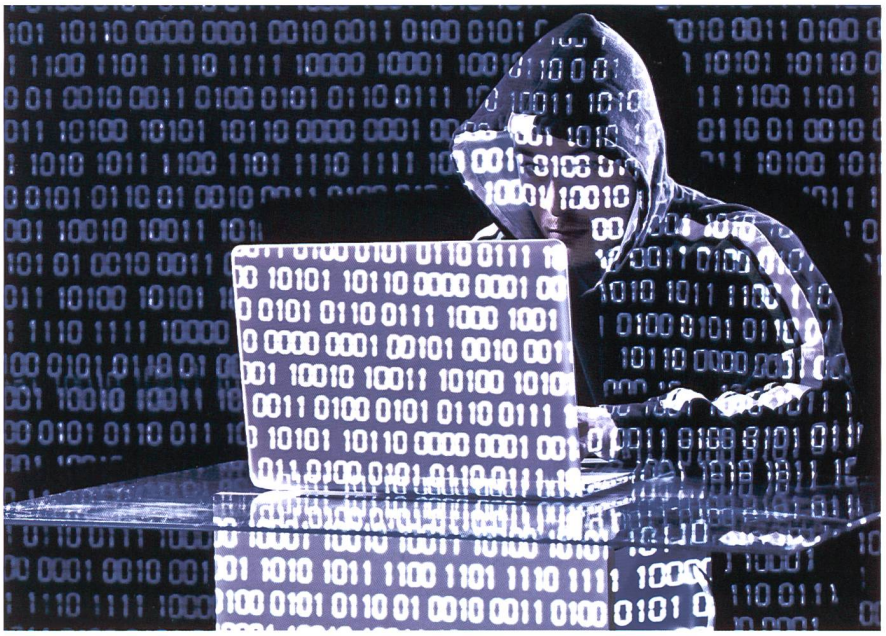
Artikel: Cyberwar fra mito e realtà
Autor: Dillena, Giancarlo
DOI: https://doi.org/10.5169/seals-867891

Cyberwar fra mito e realtà

Nell'immaginario collettivo è il campo di battaglia privilegiato del futuro. Perché oramai tutto si passa per la via digitale. Colpendo la reti informatiche si può quindi accecare, paralizzare, precipitare l'avversario nel caos.

uff spec
Giancarlo Dillena

ufficiale specialista Giancarlo Dillena
Capocomunicazione STU



Uno scenario agghiacciante per gli attaccati, che la fiction ripropone continuamente, con abbondanza di effetti speciali. E di fantasia. La realtà è, come sempre, più complessa e sfumata. E come tale va affrontata.
La tesi è stata più volte ripresa negli argomentari degli avversari irriducibili dell'esercito. Ancora nel corso dell'ultima, sfortunata votazione sugli aerei da combattimento, la sinistra ha proclamato che "dotarci di nuovi armamenti convenzionali non ha senso perché il nuovo orizzonte della guerra è oggi il cyberspazio". Una posizione evidentemente funzionale allo scopo di indebolire e possibilmente eliminare l'esercito, ma che di per sé merita qualche riflessione ulteriore. Anche perché alimentata dalla crescente e invasiva presenza del digitale nella vita quotidiana, che ognuno di noi avverte e che porta con sé un corollario di scenari apocalittici. Se i computer si bloccano, se la rete va in panne, siamo tutti perduti: niente più informazioni; niente più comunicazioni; ma anche niente più energia, niente luce, niente acqua potabile. Basta un gruppo di hacker agguerriti e tutto "va in tilt". Figuriamoci se a condurre operazioni di questo tipo sono gli stati (o gruppi terroristici importanti), nel quadro di una guerra!

Nella realtà si osserva che l'uso delle *cyberweapons* nei conflitti è stato fin qui improntato piuttosto alla prudenza. In chiave di strumento di disturbo, più che di attacco frontale. E sovente con l'intento di *destabilizzare e danneggiare, piuttosto che distruggere*, gli apparati avversari. È questa, non a caso, la dottrina ufficiale di impiego delle armi informatiche condivisa da Cina e Russia, che inseriscono l'uso dei nuovi mezzi nel *contesto più ampio della "guerra dell'informazione"*, da tempo sviluppata con particolare cura nella tradizione strategica delle potenze comuniste. In sostanza si tratta prima di tutto di ingannare, confondere e disorientare l'avversario, inteso innanzitutto come "opinione pubblica". La rete offre, da questo punto di vista, un rinnovato campo d'applicazione, formidabile ed inesauribile, per la propaganda e la "dezinformatzija". Nello stesso ordine di idee gli attacchi informatici attraverso *malware* e altre forme di hackeraggio sono stati utilizzati per colpire obiettivi specifici (come nel 2010 contro le centrifughe iraniane per l'arricchimento dell'uranio; o nel 2012 contro la rete informatica della compagnia petrolifera saudita Aramco), con intenti disabilitanti, ma limitati.

L'impressione è che l'arma informatica, nelle sue diverse applicazioni, sia oggi considerata soprattutto utile in una *fase di tensione – o di guerra di bassa intensità* – per interferire, bloccare specifici progetti avversari, "mostrare" una elevata capacità di infiltrazione come ammonimento all'avversario. Può rivelarsi anche utile in *una fase di pre-attacco*, come misura preparatoria nel quadro di un piano più vasto che implichi una *escalation* programmata. Nel momento in cui il livello del confronto si alza e si passa alla

guerra guerreggiata, il ricorso alle armi convenzionali permette comunque di ottenere risultati più sicuri e visibili, di maggiore utilità sia in termini dimostrativi che di efficacia pratica. In altre parole un missile lanciato su una centrale elettrica piuttosto che su un centro di comando presenta un ben maggiore potenziale distruttivo, il cui risultato può essere facilmente verificato, è ben visibile a tutti (amici e nemici) e ha conseguenze pratiche certe.

Questo fino ad oggi. Non attendersi nel prossimo futuro ulteriori sviluppi tecnici, in grado di dare alle *cyberweapons un'efficacia selettiva (ma anche complessiva)* che oggi non sembrano ancora avere, sarebbe assurdo. La vertiginosa espansione del digitale "civile" intorno a noi, sia in termini qualitativi che quantitativi, lascia facilmente supporre che quello militare (da cui derivano già oggi applicazioni oramai largamente diffuse, a cominciare dal GPS) non conosca un trend analogo, per non dire ancora più rilevante. Ma questo non significa ancora che la *cyberwar* sia destinata a spazzare via situazioni, dottrine e armamenti convenzionali. Una certa cautela nel fare previsioni è imposta da due ragioni fondamentali.

La prima è la vecchia storia della lancia e dello scudo, che accompagna la guerra fin dai primordi. I nuovi mezzi offensivi possono sfruttare *il gap iniziale* che li caratterizza al loro apparire. Ma prima o poi devono fare i conti con mezzi difensivi in grado di annullarne, o comunque ridurne notevolmente l'impatto. Non c'è alcuna ragione di pensare che non debba essere così anche per le lance e gli scudi dell'era digitale.

La seconda è legata a un'altra vecchia storia. Chi è dipendente da strutture tecnologiche più importanti e sofisticate è anche *maggiormente vulnerabile* quando deve affrontare un avversario che ha modi di vita più semplici e armi più "primitive", ma brutalmente efficaci. In termini moderni la ricchezza tecnologica di una società aumenta la sua fragilità, rispetto ad avversari pronti a tutto e senza vincoli (politici o d'altra natura). Il che vuol dire, in parole povere: prepara al meglio la *cyberdifesa;* ma accanto al computer tieni sempre il fucile carico e non dimenticare mai come si fa a usarlo! ◆