# Prove di guerra digitale

**Autore:** Giulio Meazzini
**Fonte:** Città Nuova

**L’arresto di Assange, fondatore di Wikileaks. La vulnerabilità della Rete. La militarizzazione del cyberspazio. Lo scontro tra governi ed hacker.**

**Senza Internet** gli stati si fermerebbero. Le grandi infrastrutture che controllano la vita delle nostre complesse società sono tutte basate su reti di computer più o meno protette, più o meno interconnesse tra di loro. Quindi sono tutte, più o meno, vulnerabili ad attacchi che arrivano attraverso la rete delle reti, cioè Internet.

**I recenti attacchi** a vari siti, tra cui quelli del governo svedese e delle carte di credito (Paypal, Mastercard, Visa) ad opera dei sostenitori di Julian Assange, il fondatore di Wikileaks arrestato a Londra, sono solo noccioline. Un piccolo assaggio di quello che potrebbe succedere domani con le cosiddette *cyberwar* e *cyberwarfare*. Con questi termini si intendono le guerre condotte senza l’uso di cannoni e invasione di territori nemici, ma semplicemente tramite computer che colpiscono ed interrompono, da lontano, le comunicazioni e le infrastrutture informative del nemico, alterandone la normale vita sociale.

**Per avere un’idea del livello di collasso** civile a cui può portare una guerra di questo tipo, basta considerare la lista sotto riportata. Sono alcuni processi vitali per una società, basati su infrastrutture informative, elencati in ordine di importanza. Un ordine particolare, però, perché non considera solo l’impatto che avrebbe l’interruzione di ogni singolo servizio, ma anche il numero di altri processi critici che sarebbero a cascata condizionati negativamente:

1. produzione e distribuzione di elettricità
2. servizi di telecomunicazione
3. fornitura carburanti
4. servizi autostradali
5. fornitura acqua potabile e per uso industriale
6. sistemi di pagamento e finanza
7. servizi antincendio e di protezione civile
8. previsioni del tempo
9. gestione fognature
10. trasporto persone e merci via treno
11. fornitura servizi sanitari
12. informazione via tv e radio

Per ognuno di questi processi sono state previste modalità di funzionamento tali da assicurare almeno una minima continuità del servizio anche in caso di emergenza. Ma il vero spauracchio è l'effetto a catena che disservizi multipli potrebbero portare. In pratica la normale vita civile e sociale si fermerebbe. Semplicemente.

**I governi si stanno attrezzando** per difendersi da attacchi (e ricatti) alle infrastrutture di questo tipo, che possono provenire da gruppi terroristici di pirati informatici o da altri governi ostili. «Lo spazio cibernetico è un nuovo fondamentale campo di battaglia e di competizione geopolitica del XXI secolo» così il Comitato parlamentare italiano per la sicurezza nel luglio 2010. Il Pentagono americano ha istituito lo *Strategic Cyber Command*. La Nato ha il Centro per la ciberdifesa a Tallin in Estonia. All'Onu qualcuno comincia a chiedere un trattato per la pace nel ciberspazio. Altri stati, invece, per difendersi da attacchi di questo tipo stanno tentando di isolare le proprie reti nazionali di computer, staccandole da Internet e imbavagliando, di conseguenza, il libero scambio di informazioni e di idee.

**Ma un fatto nuovo** si è verificato con l'arresto di Assange, un fatto che i governi forse non avevano previsto. Per la prima volta, infatti, assistiamo ad un confronto aspro, diretto, globale tra i governi, messi alla berlina in Rete, e la comunità di quelli (molti) che credono nella natura libera e trasparente di Internet e sono disposti a tutto per difenderla, primi tra tutti gli *hacker*, i samurai della rete. Come tutte le novità, è difficile prevedere come andrà a finire.