

Wargame 2022

scritto da Gilberto Pierazzuoli

La rete è oggi il sistema nervoso del corpo esteso della specie umana nel suo sviluppo occidentale, questo perché la tecnica e la cultura sono in qualche modo *embedded* nei corpi degli animali umani ([Fadini](#)). È una infrastruttura ormai fondamentale per lo svolgimento di tantissime attività anche vitali del sistema. Ma la rete non è pubblica. Questi sono gli **organismi privati che hanno funzioni fondamentali** per il suo funzionamento (dal sito del [Ministero per lo Sviluppo Economico](#)):



IANA: Internet Assigned Numbers Authority (Marina del Rey, CA, USA).

La [IANA](#) è l'autorità originariamente responsabile della supervisione sull'assegnazione degli indirizzi IP, del coordinamento dell'assegnazione dei parametri di protocollo previsti dagli standard tecnici di Internet, dell'amministrazione del DNS, ivi compresa la delegazione dei domini di primo livello, ed anche la supervisione sul sistema dei "root name server". Sotto il controllo di ICANN, la IANA continua a distribuire gli indirizzi ai RIR, a coordinarsi con IETF ed altri per assegnare i parametri di protocollo e a sorvegliare sull'operatività del DNS.

ICANN: Internet Corporation for Assigned Names and Numbers (Marina del Rey, CA, USA)

L'[ICANN](#) è un ente no-profit, organizzato con modalità internazionale, che ha la responsabilità di assegnare gli indirizzi IP (Internet Protocol) e gli identificatori

di protocollo e di gestire il sistema dei nomi a dominio di primo livello (Top-Level Domain) generico (gTLD) e del codice internazionale (ccTLD) nonché il sistema dei root server.

NRO: Number Resources Organization

Creata dai RIRs (Regional Internet Registries) per formalizzare i loro sforzi cooperativi, l'[NRO](#) è nata per gestire l'insieme delle risorse IP non ancora assegnate del "Number Resource pool", per promuovere il processo bottom-up dello sviluppo delle policy e per fungere da punto di raccolta per i suggerimenti della comunità Internet, all'interno del sistema dei RIRs. NRO opera anche come Address Supporting Organization di ICANN.

RIRs: Regional Internet-address Registries

I [RIR](#) sono responsabili della distribuzione degli Internet Number, inclusi quelli degli Autonomous System, gli indirizzi IPv4 ed IPv6.

CENTR: Council of European National Top-Level Domain Registries (Bruxelles, Belgio)

Il [CENTR](#) è la più grande associazione esistente nel campo dei nomi a dominio e rappresenta oltre 40 Registry (registri) ed il 95% dei nomi a dominio registrati a livello mondiale.

CORE: Internet Council of Registrars (Ginevra, Svizzera)

Il [CORE](#) è un'associazione senza fini di lucro tra Registrar di nomi a dominio. Uno degli scopi principali dell'associazione è quello di offrire ai CORE members l'accesso ad un sistema di registrazione dei nomi a dominio Internet condiviso (Shared Registry System - SRS). Il CORE è nato nel 1997 a fronte del "Generic Top-Level Domains Memorandum of Understanding" (gTLD MoU) con il proposito di attivare nuove estensioni dei nomi a dominio.

CRADA: Cooperative Research and Development Agreement

[CRADA](#) è la sigla dell'accordo siglato fra il Department of Commerce americano - rappresentato dal National Institute of Standards and Technology (NIST) e dal National Telecommunications and Information Administration (NTIA) - ed ICANN (Internet Corporation for Assigned Names and Numbers). L'accordo stabilisce come le parti coinvolte nello studio e nella gestione del "Internet (DNS) root server system" si debbano adoperare per rendere il sistema sempre più robusto e sicuro.

ICC: International Chamber of Commerce

L'[ICC](#) è stato fondato nel 1919 con una finalità che è rimasta sostanzialmente immutata: essere al servizio degli affari nel mondo, promuovere il commercio e gli investimenti, l'apertura dei mercati per beni e servizi ed il libero flusso dei

capitali. Le attività svolte oggi coprono un ampio spettro che va dall'arbitrato e risoluzione delle dispute, alla promozione del libero mercato, all'autoregolamentazione del mondo degli affari ed al contrasto alla corruzione ed ai reati nel commercio. L'ICC è leader nell'autoregolamentazione del mondo degli affari e nel commercio elettronico; i codici predisposti per la pubblicità e per il marketing sono stati replicati, in molti casi, sia nelle regolamentazioni nazionali che nei codici delle associazioni professionali. L'ICC è più volte intervenuto nelle discussioni sulla Internet Governance in ambito ITU e WSIS/WGIG.

IETF: Internet Engineering Task Force / IAB: Internet Architecture Board

[IAB](#) (Internet Architecture Board), [IESG](#) (Internet Engineering Steering Group), [IETF](#) (Internet Engineering Task Force), [IRTF](#) (Internet Research Task Force), [IRSG](#) (Internet Research Steering Group) progettano gli standard ed i protocolli Internet necessari al funzionamento, alla manutenzione, alla distribuzione ed allo sviluppo della Rete. Tutti questi organismi sono ospitati funzionalmente dall'[ISOC](#) (Internet Society).

W3C: World Wide Web Consortium (Cambridge, MA, USA)

Il [W3C](#) nasce nell'ottobre 1994 per portare il Web al suo massimo potenziale, mediante lo sviluppo di tecnologie (specifiche, linee guida, software e strumenti di verifica) al fine di creare un forum per informazioni, commercio, ispirazioni, pensiero indipendente e comprensione collettiva.

Tutto questo senza parlare dell'infrastruttura della rete stessa che acuminerebbe il fenomeno. Quello che comunque viene fuori è il fatto di come la rete sia fortemente sbilanciata in favore della parte nord atlantica del mondo. Se poi andiamo a vedere la proprietà dei siti e delle piattaforme più frequentate ed usate, lo sbilanciamento verso gli USA diventerà ancora più evidente. Per questo Cina e Russia stanno tentando di creare strutture indipendenti e di favorire lo sviluppo di piattaforme alternative a quelle "occidentali". In questo caso la Russia - cosciente del valore attuale della struttura di rete e in vista di possibili sanzioni in risposta a una sua eventuale mossa, volta ad alleggerire la pressione geopolitica della Nato ai suoi confini occidentali - ha preso delle misure che le possano permettere una forma di autarchia digitale, rafforzando nello stesso tempo gli strumenti di sorveglianza e controllo dei sudditi e della informazione. Il primo maggio 2021 Putin ha firmato una nuova legge che porterà alla censura su

ampie parti di Internet e, tra le altre cose, richiederà ai fornitori di Internet di installare apparecchiature per instradare il traffico web russo attraverso i server nel paese, riuscendo così anche ad impedire una mossa degli Stati Uniti volta a isolare la Russia da Internet globale. Questo permetterà al regolatore russo dei media, Roskomnadzor, di prendere il controllo della rete interna così come di metterlo in grado di filtrare tutto il traffico della stessa. Si sta anche, nello stesso tempo, mettendo mano allo sviluppo di una versione nazionale del sistema di nomi di dominio di Internet, per consentire alla rete russa di funzionare anche nel caso di disconnessioni dal resto del mondo.

Il potere bellico dell'universo digitale è fatto di molte cose, si va infatti dallo spionaggio informatico, agli attacchi cibernetici alle reti avversarie, sino ai droni assassini che fanno la guerra automatica. La guerra digitale non sostituisce però la guerra tradizionale, è invece spesso uno strumento che affina le tecniche belliche precedenti. La guerra ha sempre avuto un'influenza pesante sull'informazione, sia impedendola, sia contaminandola con false notizie. Internet, e l'attuale implementazione delle piattaforme social, sono infatti generatori e moltiplicatori naturali di *fake news*. La guerra è dunque, oggi più di ieri, guerra di informazione. È di nuovo, come non mai prima, manipolazione del consenso e generatrice di opinioni che, sotto la minaccia del pericolo per la sicurezza nazionale, non tollerano nessuna forma di dissenso. Di nuovo si ha principalmente il fatto che la guerra dell'informazione ha oggi espanso il suo raggio d'azione. La guerra informatica ha già coinvolto tutto il resto del mondo, un mondo connesso e globalizzato che è in qualche modo cointeressato ad ogni conflitto e principalmente a quelli che non avvengono alla periferia del mondo. Conflitti, quest'ultimi fatti per interposta persona e cioè per interposta nazione, che non hanno mai smesso di infiammare il mondo.

✘ Il cyberspazio è informazione, ma l'informazione digitale ormai permea di sé ampi aspetti della vita umana. I padroni di Internet sono i padroni del mondo, per questo Russia e Cina tentano di colmare il divario con gli Stati Uniti. La guerra Russia e Ucraina si innesta infatti dentro quella riedizione della guerra fredda che vede contrapporsi Cina e Stati Uniti sul terreno delle tecnologie digitali, con Russia e Europa che devono trovare una loro identità se non vogliono trovarsi completamente sottomesse ai due colossi tecnologici. In un sistema globalizzato e interconnesso, dove domina una forma di logistica basata sulla riduzione al minimo delle pause e di tempi morti, modello fortemente dipendente

dalle tecnologie informatiche, gli strumenti costituiti dalle sanzioni economiche hanno un'efficacia mai vista in precedenza. Per questo oggi è diventata indispensabile ogni forma di autosufficienza energetica e tecnologica. Autosufficienza per sé o per il gruppo di alleati ai quali si fa riferimento.

La Russia è oggi forte sul piano del *know how* software, ma terribilmente indietro nel comparto hardware e delle infrastrutture di rete. Per quanto riguarda, per esempio, la diffusione delle tecnologie 5g indispensabili per competere all'interno dell'attuale modello di sviluppo, essa è fortemente dipendente dall'occidente (Cisco, Ericson, Nokia) con l'unica alternativa della cinese Huawei. È questa la triangolazione decisiva che geopoliticamente domina il momento attuale, con l'Europa incapace e impotente, di fronte alle dipendenze energetiche che ha verso est e per quelle tecnologiche che ha verso ovest. Per questo La Russia ha osato iniziare il conflitto con l'Ucraina sapendo che l'Europa le è dipendente dal punto di vista energetico, visto poi che l'alternativa al gas russo sarebbe quello americano, che ha però bisogno di essere rigassificato e che costa di più.

La Russia mira perciò “anche a rafforzare le proprie strutture tecnologiche per potenziare, sulla falsariga di quanto sta avvenendo militarmente, anche il proprio ambiente online contro i percepiti avversari “occidentali”. Questi ultimi sono ritenuti – anche indirettamente – responsabili di **destabilizzare le dinamiche politiche interne**, dando voce, attraverso l'uso massivo di piattaforme social, agli oppositori antisistema (emblematico, ad esempio, l'effetto “virale” di [uno degli ultimi video](#) di **Alexei Navalny**, il principale nemico interno di Putin, visualizzato 120 milioni di volte e condiviso proprio grazie a YouTube, gestito da Google, di provenienza americana)” ([qui](#)).

Le cose, dal punto di vista generale, sono complicate ma lo scacchiere e le contrapposizioni sono queste, difficile perciò, almeno per me, capire le prossime mosse, quello che posso invece fare è raccontare quali aspetti delle tecnologie digitali possono essere usati come armi di guerra. Quello che sappiamo è che l'universo digitale fornisce strumenti inediti ad uso conflittuale. Alle mosse di Biden per isolare le banche russe, Putin risponde con le criptovalute, un rublo digitale per commerciare con altri paesi, in sostituzione dei dollari senza vietarsi, nello stesso tempo, di usare quegli strumenti di hacking per i quali la Russia è diventata famosa, come le tecniche di [ransomware](#) per recuperare valuta e compensare i sequestri. Ma non si tratta semplicemente di una sostituzione, quegli stessi strumenti di hacking possono intervenire sulla [blockchain](#)

mascherando le origini delle transazioni, aggirando così le sanzioni. Niente poi di così nuovo: secondo un rapporto delle Nazioni Unite, la Corea del Nord ha usato ransomware per rubare criptovalute al fine di finanziare il suo programma nucleare. Commerciale in criptovalute fa di nuovo emergere una alleanza con la Cina che ha già lanciato la propria valuta digitale tramite la propria banca centrale, cosa peraltro di non poco conto visto che in occidente le criptovalute sono di origine privata e non statale. La differenza ha infatti caratteri fondamentali. La garanzia del valore in un caso la dà lo stato, nell'altra soltanto la catena di autenticazione (blockchain) sparsa nella rete. Potere giocare su entrambe le possibilità raddoppia il potere, svincola dalla dipendenza e dal confronto con l'occidente capitalistico.

Dal punto di vista del cyberspazio la Russia si muove sia sul fronte esterno che su quello interno imponendo dispoticamente forme di controllo che in Cina sono invece accettate dalla popolazione ([Byung-chul Han](#) e [Yuk Hui](#)). Ecco che “contestualmente alla



predisposizione della legge sull'Internet sovrana, il Parlamento russo [ha approvato il divieto](#) di vendita di smartphone, computer e TV prive di alcune **app russe preinstallate** ([qui](#)), applicazioni che possono “[sorvegliare o censurare](#), come evidente strategia di convergenza tecnologica che mira alla realizzazione di un sistema operativo autonomo e indipendente di servizi hardware e software in grado di monitorare il flusso di informazioni online” (ibidem).

La guerra nella Grecia antica ha avuto anche una componente ludico-agonistica, dice [Jean Pierre Vernant](#) ripreso da [Agamben](#), un tentativo per rendere la guerra meno cruenta e per limitarne gli effetti nefasti, ma il wargame digitale attuale gioca sul bordo di un abisso che potrebbe portare a conseguenze “finali”, da fine del mondo, appunto, come la terza e ultima guerra mondiale. Armare o tifare oggi per uno dei contendenti, invece di adoperarsi in tutti i modi per la pace è da folli. Se sopravvivevamo all'abominio, ci si domanderà inebetiti del perché di questa follia, cercando con difficoltà le voci dissenzianti che l'apparato massmediatico,

digitale e non, hanno messo a tacere sovrastandone la loro flebile sparuta presenza. Non si tratta qui di una guerra tra umani ma di una guerra agli umani con tutte le altre specie a seguire. Il digitale eterodiretto dal capitalismo è questo apparato di controllo e di condizionamento che lavora sul virtuale con effetti reali. Sarebbe l'ora che di immateriale e di gamificato ci fosse la guerra e non la produzione di questa nefasta opinione: la doxa guerrafondaia del pensiero unico ormai pervasivo.