Le reazioni geopolitiche all'invasione dell'Ucraina sono poste sotto i riflettori globali ormai da giorni, ma parallelamente alle mobilitazioni di truppe c'è una seconda, innovativa, battaglia che sta sconvolgendo il panorama bellico da dietro le quinte, quello della **guerra cibernetica** ("cyberwarfare"). L'importanza di questa sfera strategica si è dimostrata evidente già nei giorni che hanno preceduto le dichiarazioni indipendiste del Donbass da parte del Cremlino, quando la Computer Emergency Response Team ucraina (CERT-UA) ha segnalato una massiccia manovra di phishing potenzialmente ricollegato a criminali informatici della Bielorussia.

L'assalto non si è fermato però al solo phishing, anzi è presto **evoluto in attacchi ransomware che si sono a loro volta tramutati in ondate di data wiping**, ovvero nella cancellazione coatta dei dati presenti sui server. In un mondo sempre più digitalizzato, l'hacking si sta dimostrato in questi giorni un mezzo comparabile al sabotaggio di ponti e ferrovie, un mezzo essenziale nel rallentare le capacità di coordinamento degli ingranaggi amministrativi che governano l'Ucraina.

Pensare che il cybercrimine sia stato sfruttato unilateralmente sarebbe però ingenuo. I gruppi hacker, mossi da motivazioni etiche o pecuniarie, si stanno frammentando e ridistribuendo tra le due parti, scatenando un ginepraio digitale che rappresenta un'anticipazione di un possibile **futuro fatto di duelli di matrice informatica**: gruppi ransomware passati alla Russia si sono visti a loro volta colpiti da colleghi che ne hanno rivelato i dati sensibili, il celebre collettivo di Anonymous sta sfidando la Russia e i politici occidentali che si sono dimostrati accomodanti con il Presidente Vladimir Putin, il gruppo GhostSec sta assalendo le pagine web dei corpi militari russi e **lo stesso Governo ucraino ha imbastito uno squadrone di hacker**.

Questa "cyber-falange" è stata imbastita in tempi da record da Mykhailo Fedorov, Ministro ucraino della transizione digitale, e coinvolge più di **250mila volontari** con sede in ogni angolo del mondo, i quali si coordinano sommariamente attraverso il gruppo Telegram @itarmyofukraine2022. Il plotone si dichiara responsabile dell'abbattimento della webpage del Ministero degli Esteri russo, della borsa valori e di alcune banche direttamente legate alla politica di Mosca. Persino le pagine internettiane di alcune testate giornalistiche russe si sono trovate vittima di attacchi, con il risultato che sono state tramutate per breve periodo in bacheche ricolme di messaggi critici nei confronti di Putin.

Da una parte e dall'altra si registrano insomma centinaia di migliaia di hacker pronti a saggiare le difese avversarie, uno sciame privo di gerarchia che colpisce orizzontalmente giocando la carta dei grandi numeri, **un'onda cibernetica che probabilmente è destinata a rimanere per sempre anonima**. La guerra in Ucraina sta tuttavia mostrano

anche un’altra faccia della guerra dei tempi digitali: quella satellitare. Molti esperti concordano nel suggerire che gli attacchi hacker attribuiti alla Russia siano stati ben al di sotto delle reali possibilità a disposizione del Cremlino, che le forze attaccanti abbiano contenuto per superbia o per strategia la potenza del proprio intervento, una fiacchezza a cui ora, sospettano le Intelligence statunitensi, si cercherà di porre rimedio preparandosi a **interferenze satellitari**.

Nel caso si tratterebbe della prima dimostrazione concreta dell’esoguerra – ovvero della guerra orbitale – una prospettiva che gli Stati Uniti e gli osservatori terzi stanno temendo. Lo si nota nella scelta di Elon Musk di mettere a disposizione la rete *StarLink* – soggetta a contratti militari con gli USA – al popolo ucraino qualora le telecomunicazioni dovessero crollare, ma anche nei suggerimenti forniti dal leader di *Wikileaks* Julian Assange, il quale raccomanda a tutte le persone dell’area di scaricarsi l’app di messaggistica **Briar**, applicazione che è particolarmente attenta alla privacy e che funziona anche in assenza di wifi grazie a un sistema peer-to-peer in chiave Bluetooth.

Le incertezze in campo sono ancora molte, ma questa sfida globale sta mettendo in scena degli approcci informatici la cui portata era stata fino a ora solamente teorizzata. Considerando l’ampia lista di **armi “futuristiche”** che ambo le parti hanno raccolto nei reciproci arsenali, non resta che sperare che la situazione non degeneri ulteriormente.

[di Walter Ferri]