I CYBER LEGIONARI
Di Giuliano Marrucci
Collaborazione Eleonora Zocca
Immagini Giovanni De Faveri
Montaggio e grafica Gabriele Di Giulio

GIULIANO MARRUCCI FUORI CAMPO
26 febbraio. Sono passati due giorni dall'inizio dell'invasione russa dell'Ucraina, quando Mikhail Fedorov, il giovane ministro della Trasformazione Digitale nonché vice primo ministro dell'Ucraina, lancia questo appello ai circa 280 mila follower del suo profilo Twitter: "Stiamo creando un'armata informatica. Abbiamo bisogno di talenti digitali. Tutti i compiti operativi saranno impartiti dal canale Telegram "itarmyofukraine". Nel giro di pochi giorni, il canale Telegram supera i 300 mila iscritti. È la più grande armata cibernetica della storia, uno stormo di legionari provenienti da ogni angolo del pianeta che ha dato vita alla prima vera e propria guerra mondiale cibernetica, ed ha già cambiato per sempre il modo in cui pensiamo e ci comportiamo nella dimensione digitale.

FRÉDÉRICK DOUZET – DIRETTRICE GEODE
Chiedere esplicitamente a volontari civili di tutto il mondo di intervenire nelle operazioni di attacco online è sicuramente una novità, e credo sia un'anomalia perché questa richiesta dovrebbe essere una prerogativa degli stati.

CYBER VOLONTARIO – FEARLESS SECURITY
Quando abbiamo visto la propaganda di IT-Army Ukraine su Telegram ci siamo subito adoperati per creare un piccolo team italiano chiamato Fearless Security. Siamo tutti hacker etici, tutti con una laurea o un diploma in informatica ed alcuni di noi hanno già partecipato ad operazioni simili in passato.

GIULIANO MARRUCCI
Vi sentite a tutti gli effetti dei combattenti in una guerra?

CYBER VOLONTARIO – FEARLESS SECURITY
Noi siamo quelli della porta accanto, ma sì, in termini di cyber army ci sentiamo parte di questa guerra e in questo momento il nostro obiettivo è il governante russo.

STÉPHANE DUGUIN – AMMINISTRATORE DELEGATO CYBERPEACE INSTITUTE
Civili che scelgono a livello individuale di prendere parte a un conflitto mettendo a disposizione le loro competenze ci sono sempre stati, ma mai niente di comparabile a quello a cui stiamo assistendo. Questo appello ha scatenato una quantità enorme di attività nella sfera digitale che potrebbero avere conseguenze gigantesche.

STUDIO SIGFRIDO RANUCCI

Cyberspazio è il quarto dominio in una guerra dopo terra, mare e aria, lo ha decretato ufficialmente la NATO. Ora, dall'Iraq in poi diciamo che hanno combattuto delle guerre hacker i reparti specializzati degli eserciti. È successo in Iraq, è successo anche in Estonia, dove sono stati attaccati dei siti istituzionali, è successo anche in Georgia, dove sono stati procurati dei danni alla pipeline che corre tra Baku e Tbilisi. Ora sono stati questi attacchi però sempre svolti da reparti ufficiali cyber dei rispettivi eserciti. Quello che ha di nuovo questa guerra è che invece il governo ucraino, oltre a gestire il proprio di esercito, ha chiesto un aiuto anche a dei volontari civili, a dei legionari virtuali, presenti in tutte le aree del mondo. Siccome hanno risposto in tanti, per gestirli ha utilizzato due start up ucraine che hanno messo a disposizione un loro software per poter sferrare questi attacchi. Solo che la ricaduta potrebbe essere che potremmo cambiare per sempre la nostra idea di internet, del web e si potrebbero verificare delle ricadute inimmaginabili. Il nostro Giuliano Marrucci.

GIULIANO MARRUCCI FUORI CAMPO
Ogni mattina, circa 300 mila persone sparse in tutto il pianeta si collegano a questo canale Telegram in attesa di istruzioni per il prossimo attacco cyber da lanciare contro obiettivi russi di ogni genere. Tra i cyber volontari ci sono anche diversi italiani, che però vogliono rimanere anonimi.

GIULIANO MARRUCCI
In cosa consiste esattamente la vostra attività?

CYBER VOLONTARIO – FEARLESS SECURITY
Ci sono reparti di noi che si dedicano all'editing video, altri che invece si occupano di veicolare messaggi alla popolazione russa, ad esempio facendo apparire su un sito qualsiasi un messaggio come "fermiamo il massacro in Ucraina" o cose del genere. Poi ci sono quelli che in particolare si dedicano agli attacchi DdoS

GIULIANO MARRUCCI FUORI CAMPO
Che sta per Distributed Denial of Service. In sostanza, si tratta di indirizzare quanto più traffico possibile verso uno specifico server in modo da intasarlo fino a renderlo irraggiungibile. Ogni giorno, il team dell'IT Army posta un elenco di siti web da rendere inaccessibili, e i legionari partono all'attacco. Questo è il sito della famigerata Gazprom. Questo quello di una nota banca russa, e questo il sito dell'amministrazione dell'Oblast di Orel, a 150 km dal confine ucraino.

GIULIANO MARRUCCI
E che idea vi siete fatti delle potenziali conseguenze, anche in termini legali, di queste attività?

CYBER VOLONTARIO – FEARLESS SECURITY
Non ci siamo posti questa domanda, non saprei risponderti. Vogliamo semplicemente la pace e non carnefici dittature.

GIULIANO MARRUCCI
Ginevra, la città che ha dato il suo nome al complesso corpus di convenzioni che dicono cosa è ammesso e cosa no durante una guerra, e che sono probabilmente le leggi più frequentemente disattese dell'intero pianeta. In questo campus futuristico che ospita decine di istituti di ricerca e compagnie attive nel settore biomedicale, c'è la sede del Cyber Peace Institute, una Ong che si occupa di promuovere la pace e la giustizia nella cybersfera, e che conta nel suo consiglio di amministrazione pesi massimi di giganti globali come Microsoft, Mastercard e Telefonica.

STÉPHANE DUGUIN – AMMINISTRATORE DELEGATO CYBERPEACE INSTITUTE
Quando uno decide di essere parte di un conflitto, automaticamente sta rinunciando volontariamente al suo status di civile. E sinceramente dubito che chi oggi sta usando il suo computer per partecipare, ad esempio, a un attacco DDOS contro bersagli russi sia consapevole delle conseguenze.

GIULIANO MARRUCCI FUORI CAMPO
Le conseguenze potrebbero coinvolgere le responsabilità degli Stati. Aubervilliers, area metropolitana di Parigi. Nel più grande campus d'Europa dedicato alle scienze umane e sociali incontriamo Bill Woodcock, autorità indiscussa che ha contribuito concretamente a costruire Internet sin dagli inizi. Woodcock, oggi, è il direttore dell'organizzazione internazionale che offre supporto operativo alle principali infrastrutture di Internet e attualmente è in prima linea nella difesa di quelle ucraine.

BILL WOODCOCK – DIRETTORE ESECUTIVO PACKET CLEARING HOUSE
Entro i confini territoriali ucraini, il governo ovviamente ha piena sovranità: può autorizzare attacchi informatici, non può invece autorizzare chi si trova in altri paesi. E un cittadino straniero che partecipa a un attacco potrebbe coinvolgere nel conflitto il suo paese.

GIULIANO MARRUCCI FUORI CAMPO
A complicare le cose c'è anche il fatto che per gestire le attività dell'IT Army, il governo ucraino ha coinvolto anche due aziende private: la Cyber Unit Tech di Yegor Aushev e, soprattutto, la Hacken di Dyma Budorin, una startup che opera nell'ambito del web3, la terza generazione del web, che grazie all'utilizzo delle blockchain dovrebbe permettere di effettuare transazioni finanziarie senza intermediari. Quindici giorni prima dello scoppio della guerra, il grosso del suo team si è trasferito in Europa. Noi lo abbiamo incontrato a Vienna, dove era venuto per visitare l'ambasciata USA nella speranza di ottenere un visto, senza successo. Il principale contributo di Budorin alla guerra cibernetica ucraina è stato mettere a disposizione il loro software per gli attacchi DDoS, che si chiama disbalancer. Scaricando disbalancer sostanzialmente rendi il tuo computer quello che in gergo si chiama una macchina "zombie", e il team di Hacken la può usare a suo piacimento per lanciare attacchi DDOS ai server che decide lui. Inoltre,

non puoi neanche capire esattamente come funziona, perché il codice non è aperto ma proprietario, quindi segreto.

DYMA BUDORIN – COFONDATORE E CEO HACKEN
La responsabilità è tutta a carico nostro, ma non siamo politici, siamo imprenditori. Ed è nostro interesse farci una reputazione lavorando sodo e bene.

GIULIANO MARRUCCI
Cosa ne pensi di questo progetto?

BILL WOODCOCK – PACKET CLEARING HOUSE
Intanto chiariamo che questo è per definizione illegale. Scaricare codice da dei criminali che non sai esattamente cosa fa e permettergli di usare la tua macchina per portare a termine altre attività illegali, a me pare una pessima idea.

GIULIANO MARRUCCI FUORI CAMPO
Ciononostante, a fidarsi sembra siano in parecchi. Disbalancer è stato già scaricato 80 mila volte, e per Hacken è anche una grande opportunità di farsi pubblicità e incassare soldi. Il software, infatti, è collegato a una criptovaluta che si chiama appunto DDOS, e che prima della guerra conoscevano in pochi.

DYMA BUDORIN – COFONDATORE E CEO HACKEN
Il giorno che abbiamo annunciato che Hacken avrebbe partecipato alla guerra cibernetica, molti russi e altre persone non hanno voluto mischiare affari con politica, e hanno venduto. E il valore della valuta è crollato. Ma poi abbiamo ricominciato a crescere, e ora siamo a circa il doppio del prezzo iniziale.

GIULIANO MARRUCCI FUORI CAMPO
Ed è solo l'inizio. Da qualche giorno Hacken ha annunciato il suo prossimo obiettivo: 100 mila utenti attivi che usano contemporaneamente disbalancer h24 sulle loro macchine. E nelle chat s'è scatenato l'entusiasmo. Secondo questo utente, una volta finita la guerra tutti conosceranno disbalancer, e DDOS diventerà un asset di grande valore. Secondo quest'altro invece investire in disbalancer oggi significa garantirsi ricchezza e una bella pensione anticipata.

DYMA BUDORIN – COFONDATORE E CEO HACKEN
Questo obiettivo di centomila utenti deriva da un calcolo che abbiamo fatto: il nostro obiettivo è lanciare un attacco DDoS così grande da mandare in tilt tutte le porte di accesso all'internet russo contemporaneamente. A quel punto la Russia non avrà altra opzione che isolare il suo internet dal resto del mondo. Una volta che hai dimostrato che con dei software è possibile isolare completamente un paese, i paesi si organizzeranno a blocchi, e limiteranno il loro internet solo all'interno.

GIULIANO MARRUCCI FUORI CAMPO
Sempre negli edifici del campus Condorcet di Parigi abbiamo incontrato anche Frédérick Douzet, la direttrice del gruppo di ricerca GEODE, che sta per Geopolitica della Datasfera.

GIULIANO MARRUCCI
Siamo alla fine dell'internet come piattaforma globale senza frontiere?

FRÉDÉRICK DOUZET – DIRETTRICE GEODE
In realtà, a causa di tutte le tensioni geopolitiche che stiamo vivendo, il processo di balcanizzazione del cyberspazio è già in corso. La domanda allora è se noi vogliamo incoraggiare ulteriormente questo processo. Io credo che avrebbe un effetto molto negativo sulla popolazione civile russa, li renderebbe ancora più impermeabili a qualsiasi informazione diversa dalla propaganda di stato.

GIULIANO MARRUCCI FUORI CAMPO
Dyma Budorin ha lavorato per tre anni nelle forze armate ucraine alla costruzione di un sistema di difesa cibernetica adeguato con il presunto sostegno anche delle forze Cyber della NATO.

GIULIANO MARRUCCI
Questo sostegno da parte delle forze Cyber della NATO è stato davvero di aiuto?

DYMA BUDORIN – COFONDATORE E CEO HACKEN
Onestamente direi decisamente di no. Hanno mandato alcuni esperti, ma il loro interesse più che a creare un sistema di difesa sembrava finalizzato a venderci alcune vecchie tecnologie e anche a spiare. Ma anche il governo ucraino non ha mostrato volontà e competenze per costruire qualcosa di significativo per difenderci.

GIULIANO MARRUCCI FUORI CAMPO
E così quando alla fine è scoppiato il conflitto, il popolo ucraino si è ritrovato in balia degli attacchi russi. In Russia sarebbe in vigore, secondo gli analisti, un patto occulto di non belligeranza tra agenzie governative e gruppi criminali, che non vengono perseguiti ma quando serve devono essere pronti a prestare una mano per realizzare gli obiettivi strategici del governo. Ce lo aveva confidato nei minimi dettagli, cinque anni fa, Anton Nossik, considerato dai dissidenti il padre dell'Internet Russo. Report è stata l'ultima testata straniera a intervistarlo prima che nel 2017 scomparisse a causa di un infarto.

ANTON NOSSIK – GIORNALISTA E ATTIVISTA
Se c'è un nemico della Russia, ad esempio quando è scoppiato il caos in Estonia, gli hacker russi hanno lanciato i loro attacchi contro i siti governativi. L'anno dopo è scoppiata la guerra in Georgia e gli hacker russi hanno attaccato il governo georgiano. Quando l'agenzia mondiale antidoping propone al CIO di escludere gli atleti russi dalle olimpiadi di Rio nel 2016, il giorno dopo i suoi

server vengono hackerati. Si tratta in realtà sempre di singoli hacker che vengono assoldati da qualche colonnello o generale delle forze di sicurezza. Rubano informazioni commerciali sensibili, intercettano comunicazioni tra privati, vengono utilizzati per regolare i conti con i nemici di Putin. Come è successo quando sono state pubblicate comunicazioni riservate tra membri del governo, compreso il primo ministro, è emerso poi che figure apicali del dipartimento cyber security avevano pilotato gli hacker da quattro anni.

GIULIANO MARRUCCI
E anche dopo l'invasione dell'Ucraina è andato in scena lo stesso identico copione.

BILL WOODCOCK – DIRETTORE ESECUTIVO PACKET CLEARING HOUSE
Il giorno stesso dell'invasione russa c'è stato un attacco molto significativo contro un satellite di Viasat, che ha comportato problemi enormi in mezza Europa, compresi alcuni parchi eolici in Germania. Questo tipo di attacchi però richiedono che al momento dell'attacco le condizioni siano identiche a quando è stato preparato. Ma quando c'è una guerra tutto cambia velocemente, e quindi i russi hanno ripiegato verso attacchi più semplici, e così abbiamo assistito a un aumento di attacchi, il classico fishing per introdurre malware nei dispositivi dei cittadini comuni. E questo poi ha sconfinato verso la Polonia, dove ci sono tantissimi profughi.

STUDIO SIGFRIDO RANUCCI
Sarebbe la fine di internet come piattaforma globale. La diffusione di questi software che rendono i computer degli zombie dai quali sferrare attacchi senza controllo indebolirebbe ulteriormente la rete, la renderebbe ancora più insicura e questo accelererebbe la balcanizzazione del web. Cioè proprio per motivi di sicurezza, ogni paese potrebbe propendere per un internet chiuso, questo a discapito della libertà, a discapito della democrazia e anche della libertà di stampa, quando il web non viene utilizzato per disinformare. Insomma, questa è una delle ricadute di questa orribile guerra, insieme a quella di aver generato circa quattro milioni di profughi. Cento mila sono arrivati nel nostro paese e si è posto anche il problema della loro ospitalità.