LA GUERRA ONLINE

di GIACOMO CORVI

IL CONFLITTO IN UCRAINA STA MOSTRANDO TUTTE LE POTENZIALITÀ BELLICHE DELLO STRUMENTO INFORMATICO. LA MINACCIA NON RIGUARDA TUTTAVIA SOLTANTO LE PARTI COINVOLTE NELLO SCONTRO: ANCHE LE IMPRESE E LE ISTITUZIONI EUROPEE POSSONO FINIRE NEL MIRINO DEGLI HACKER. SECONDO LUIGI MARTINO DELL'ISPI, SERVE UNA MAGGIORE COMPRENSIONE DEL RISCHIO

Lo scorso 24 febbraio aveva inizio l'invasione russa dell'Ucraina. Lo stesso giorno, quasi alla stessa ora, un attacco informatico metteva momentaneamente fuori uso il sistema satellitare Ka-Sat di **Viasat**, colosso statunitense delle telecomunicazioni che offre servizi di connessione a molti cittadini europei e, come hanno ricostruito varie testate giornalistiche internazionali, anche all'esercito ucraino. Possibile che si sia trattato di una semplice coincidenza? "No, assolutamente no", risponde secco **Luigi Martino**, associate research fellow dell'**Ispi**. "L'attacco informatico – prosegue – è avvenuto poco prima dell'operazione militare, con il chiaro intento di ostacolare i sistemi di difesa ucraini e favorire l'avanzata dell'esercito russo". Insomma, la guerra in Ucraina è anche una guerra informatica.

Recuperando la lezione di **Carl von Clausewitz**, Martino ricorda che la guerra "rassomiglia al camaleonte perché cambia di natura in ogni caso concreto". Quindi anche in base alle tecnologie disponibili. Le capacità informatiche dell'esercito russo sono note da tempo. E anche l'Ucraina si è rapidamente dotata di quello che potrebbe essere definito un piccolo arsenale informatico. "Una settimana prima dell'invasione, il dipartimento della Difesa degli Stati Uniti ha inviato a Kiev il suo *cyber command* per migliorare le capacità informatiche dell'esercito", spiega Martino. "Qualche giorno dopo l'inizio della guerra – aggiunge – è stato invece il ministro della Difesa ucraino a chiamare a raccolta la comunità internazionale di hacker contro la Russia".

IL DOMINIO INFORMATICO

Trent'anni fa, nei giorni di *Desert Storm*, si parlava della "guerra in diretta televisiva". Oggi si può tranquillamente parlare della "guerra online". E non tanto (o non solo) perché gran parte dell'informazione (ma anche delle fake news e della propaganda) ci arriva dal web. Quanto piuttosto perché, come spiega Martino, "il dominio informatico è diventato a tutti gli effetti un nuovo strumento nella cassetta degli attrezzi militari, al pari del potere aereo, marittimo e terrestre". Il caso di Viasat mostra chiaramente le potenzialità di un attacco informatico in uno scenario di guerra.

Non è la prima volta che la Russia ha la possibilità di esprimere il suo cosiddetto *cyber power*. "Nel 2007 – ricorda Martino – un attacco informatico ha colpito una serie di siti web in Estonia, proprio dopo che il governo aveva approvato la rimozione della statua al *Milite Liberatore* dal centro di Tallinn". L'anno succes-

***Luigi Martino**, associate research fellow dell'Ispi*

sivo alcune incursioni informatiche accompagnarono l'invasione russa dell'Ossezia del Sud, in Georgia. E nel 2015, prosegue Martino, "un attacco informatico ha a lungo interrotto la fornitura di energia elettrica a centinaia di migliaia di cittadini in Ucraina".

IL RISCHIO PER IMPRESE E ISTITUZIONI

Il rischio informatico non riguarda tuttavia la sola l'Ucraina. L'Unione Europea e gli Stati Uniti hanno recentemente lanciato un'allerta su possibili attacchi hacker contro istituzioni e imprese come ritorsione per le sanzioni che la comunità internazionale ha irrorato alla Russia. A fine marzo fece molto rumore la notizia di un attacco informatico che aveva messo fuori uso le biglietterie automatiche di **Trenitalia**: le indagini hanno attribuito la responsabilità a un gruppo di criminali comuni, ma è stato inevitabile, almeno all'inizio, pensare a una firma dell'esercito russo.

"La minaccia c'è ed è reale", dice Martino. "Del resto – aggiunge – il rischio informatico non nasce con la guerra in Ucraina, come ben testimoniato dai casi di *NotPetya* e *WannaCry* o anche dall'attacco ransomware che lo scorso anno ha colpito la compagnia di oleodotti **Colonial Pipeline** negli Stati Uniti". C'è di buono che episodi di questo genere, secondo Martino, hanno almeno contribuito ad alimentare in Italia una certa maturità istituzionale. La creazione lo scorso anno dell'**Agenzia per la cybersicurezza nazionale**, in questo senso, è un segnale positivo.

LA MANCANZA DI CULTURA INFORMATICA

Quello che manca è invece un'ampia e diffusa cultura informatica. "Nonostante l'esperienza degli ultimi anni, sono ancora molti gli operatori in Italia, a cominciare dalle piccole imprese e dalla pubblica amministrazione locale, che non hanno ben compreso la portata di questo genere di rischio", afferma Martino. "Tutto ciò – aggiunge – si riflette nella mancanza di finanziamenti adeguati per la sicurezza informatica e nella penuria di risorse umane competenti in questo ambito".

Secondo Martino, servirebbe innanzitutto un'implementazione continua di sempre nuove e sempre più efficaci tecnologie, soluzioni e procedure. E poi anche maggiori investimenti sul capitale umano, visto che, come ricorda l'esperto dell'Ispi, "l'anello debole della sicurezza informatica resta l'individuo: per questo sono, a mio avviso, fondamentali programmi di formazione permanente che possano far prendere coscienza del rischio e stabilire una prima linea di difesa". Anche adeguate coperture assicurative possono risultare utili in questo ambito, ma il mercato italiano per Martino "resta poco maturo, nonostante la forte domanda che si sta venendo a creare negli ultimi tempi".

UNA MINACCIA COSTANTE

A metà aprile la guerra in Ucraina è ancora in pieno svolgimento. Ed è difficile prevedere come potrà evolvere nel prossimo futuro. Per Martino ci sono soltanto due certezze. La prima è che gli effetti del conflitto, qualunque sia il suo esito conclusivo, si faranno sentire ancora a lungo. "La Russia si trova in una situazione di isolamento internazionale che, a mio parere, avrà lunghi strascichi nel panorama internazionale".

La seconda certezza è che con la fine della guerra non si esaurirà il rischio informatico. Anzi, secondo Martino, tenderanno addirittura ad "aumentare nel prossimo futuro con la crescita della connettività: a una maggiore informatizzazione coincide un allargamento del perimetro di rischio e, di conseguenza, una minore sicurezza". L'unica speranza è che gli episodi degli ultimi anni possano favorire la consapevolezza sul tema. E contribuire a istituire presidi che possano prevenire il rischio informatico.