

IL FRONTE CYBER

UNO SPECIALE SULLA CYBERWARFARE
TRA GUERRA IN UCRAINA E MEDIO ORIENTE



GUERRE
DI RETE

Gli eBook di Guerre di Rete

IL FRONTE CYBER

Uno speciale sulla cyberwarfare
tra guerra in Ucraina e in Medio Oriente

A cura di Carola Frediani, Sonia Montegiove,
Federico Nejrotti e Rosita Rijtano

Con i contributi di Raffaele Angius, Irene Doda,
Carola Frediani, Rosita Rijtano, Eleonora Zocca



INDICE

Premessa	4
Scelta delle immagini: il <i>Flos Duellatorum</i>	5
Il fronte cyber inizia prima della guerra	7
Introduzione	7
La prima mondiale di un cyber esercito volontario	13
Guerra in Ucraina	13
IT Army of Ukraine, genesi ed evoluzione	14
Tra bug bounty e intelligence	15
Coordinare la decentralizzazione	16
Tra attacchi informatici e propaganda	18
Tante ambiguità, troppi rischi	21
La cyberwarfare promessa tra Israele, Iran e Hamas	25
Medioriente	25
Un conflitto ben poco virtuale	27
La risposta di Tel Aviv	28
Se il feed è un campo minato	34
Social Media	34
I social media come canali di (dis)informazione	35
Strategie a confronto	37
I doppi standard dei social	38
Il rapporto con i governi	40
Master & Commander: la battaglia delle navi fantasma	43
Guerra e Pirati	43
Le vulnerabilità dell'AIS	44
Le modalità di attacco	46
Dal contrabbando di petrolio alle azioni politiche e militari	49
Autori & Curatori	50

PREMESSA

Il fronte cyber è una monografia sulla cyberwarfare, e più nello specifico sulla componente cyber durante le guerre, con riferimento al conflitto in Ucraina e a quello in Medio Oriente. È prodotta da *Guerre di Rete* (guerredirete.it), curata da Carola Frediani, Sonia Montegiove, Federico Nejrotti, Rosita Rijtano, e scritta da Raffaele Angius, Irene Doda, Carola Frediani, Rosita Rijtano, Eleonora Zocca.

Guerre di Rete nasce con l'obiettivo di fornire un'informazione accurata e approfondita che dia conto della rilevanza e della complessità dei temi legati al mondo della cybersicurezza e dei conflitti digitali.

È il frutto dell'impegno di due associazioni culturali: l'omonima *Guerre di Rete*, che da anni pubblica una [newsletter](#) settimanale dedicata alla cybersicurezza; e [Cyber Saiyan](#), una community indipendente di professionisti del settore della cybersicurezza.

Guerre di Rete si sviluppa intorno al modello dello “slow journalism”, non rincorrendo la notizia giornaliera ma cercando di dare senso e completezza alle storie e alle vicende più significative, in maniera trasparente e con toni misurati e distaccati.

Oggi è totalmente supportata:

- da donazioni di lettori, sostenitori, amici e colleghi che credono nella nostra [idea di informazione](#);
- delle associazioni [Guerre di Rete](#) e [Cyber Saiyan](#);
- dal lavoro volontario dello staff di Guerre di Rete: Gerardo Di Giacomo, Carola Frediani, Sonia Montegiove, Giovanni Mellini, Federico Scalco e Patrizio Tufarolo.

SCELTA DELLE IMMAGINI: IL *FLOS DUELLATORUM*

di Federico Nejrotti

Rappresentare visivamente i temi affrontati da prodotti editoriali come *Il Fronte Cyber* e da *Guerre di Rete* non è un capriccioso esercizio manieristico. Invece, è un aspetto fondamentale del processo divulgativo alla base di questi testi.

La scelta delle immagini usate per rappresentare tematiche apparentemente astratte, come quelle vicine al mondo della sicurezza informatica, permette di ampliare la semantica necessaria a discutere argomenti complessi.

Per questa pubblicazione, abbiamo selezionato alcune illustrazioni provenienti da [*Il Fior di Battaglia \(Flos Duellatorum\)*](#) di Fiore dei Liberi disponibili in pubblico dominio grazie all'archivio *Getty*. Si tratta di un manuale di lotta e scherma scritto tra il 1409 e il 1410 a Ferrara.

Il Fior di Battaglia è uno dei primi manuali illustrati di lotta in cui il legame tra testo e immagine è fondamentale, e dall'epoca della pubblicazione la sua diffusione capillare lo rende ancora oggi uno dei manuali fondamentali per discipline come la scherma antica.

Le dinamiche di scontro rappresentate nel manuale permettono al lettore di cogliere la dinamicità dei movimenti descritti, conferendo ai testi un fortissimo potere divulgativo e didattico.

Abbiamo ritenuto opportuno omaggiare *Il Fior di Battaglia* rendendolo una parte centrale della narrazione di questa pubblicazione, nella speranza che possa supportare - come allora - il potere delle parole.



IL FRONTE CYBER INIZIA PRIMA DELLA GUERRA

Non c'è stata una cyber Pearl Harbor, bensì un lavoro continuo e tattico. Ma è prima della guerra che la cyber si dispiega. Ed è in quella fase che va tenuta sotto controllo.

di Carola Frediani

Introduzione

Mentre guardiamo con preoccupazione e angoscia agli sviluppi della guerra in Ucraina e di quella in Medio Oriente, che cosa è emerso finora della loro dimensione cyber?

Pur nella diversità radicale dei due scenari di conflitto, un dato era comune in passato: in entrambe le aree si muovevano soggetti aggressivi e sofisticati nelle operazioni digitali e nei cyberattacchi.

L'Ucraina è stata per anni un laboratorio di attacchi informatici (attribuiti ai russi da vari Stati occidentali) con conseguenze fisiche (blackout elettrici, wiper come NotPetya che hanno mandato in tilt le attività di aziende e organizzazioni di tutto il mondo). La Russia era nota da anni per le attività delle sue unità di hacker statali o sponsorizzati dallo Stato, come si dice in gergo, specializzati in hack-and-leak, disinformazione, spionaggio e, come detto sopra, sabotaggio di sistemi industriali.

Israele è una potenza cyber riconosciuta. E nell'area mediorientale il suo antagonista statale (e digitale) è sempre stato l'Iran che, dopo aver subito nel 2010 la prima "cyberarma" (Stuxnet, attribuita a Usa-Israele [con vari aiuti europei](#)), è cresciuto nelle sue capacità informatiche offensive.

Ebbene, malgrado queste premesse, lo scontro cyber è (inevitabilmente, lasciatemi dire) passato in secondo piano con l'esplosione della guerra. Questo perché la componente del cyberspazio è stata sì onnipresente, ma sempre legata alle necessità politiche e militari. O propagandistiche. Quindi resta importante ma non nel modo in cui alcuni potevano immaginarsi, magari mutuando improbabili immaginari cinematografici.

Non c'è stata insomma una cyber Pearl Harbor, ma un lavoro continuo, a volte sotterraneo, a volte volutamente scoperto ed eclatante. La dimensione cyber ha accompagnato attacchi cinetici, così come attività e tecnologie emergenti, ma in modo tattico e mutevole. A volte ha colpito infrastrutture di comunicazione cruciali (reti satellitari come Viasat in Ucraina, fornitori internet, compagnie telefoniche) ma queste sono state danneggiate anche in modo più efficace con tradizionali operazioni militari, o [imponendo](#), come a Gaza, dei [blackout](#) grazie al controllo diretto dell'area da parte di Israele.

Una delle lezioni forse scontate di queste due guerre (ma repetita iuvant) è che all'inizio di un'invasione o di un importante attacco militare dobbiamo sempre aspettarci un'azione distruttiva di qualche tipo alle comunicazioni della regione. E che quindi il controllo e la ridondanza di queste reti (telefonica, satellitare ecc) sono fondamentali.

Ciò detto, "le capacità informatiche militari sono impiegate principalmente per spionaggio, repressione, sovversione e destabilizzazione", come scrive uno [studio](#) 2023 del German Institute for International and Security Affairs (*The Absolute Ideal: Military Cyber Capabilities in War and Society*).

E anche quando si parla di sistemi di intelligenza artificiale (con squarci inquietanti quando applicati nella definizione di obiettivi da colpire) è difficile fare delle valutazioni indipendenti, perché queste tecnologie sono avvolte dalla *fog of war*, la nebbia della guerra (espressione militare da intendere in senso lato), ma anche dalla coltre del marketing aziendale. E qui veniamo al ruolo dei privati in queste guerre. Sia Israele che l'Ucraina avevano, prima del conflitto, un settore tech vivace, e soprattutto nel caso ucraino il ruolo delle aziende private (straniere e nazionali) nella difesa e offesa cyber è conclamato.

Ma la mobilitazione dei privati, soprattutto nella guerra in Ucraina, è stata estesa senza precedenti. L'esempio dell'IT Army ucraino, l'armata di cyber volontari di tutte le nazionalità coinvolti in operazioni offensive, è una prima assoluta ed è oggetto di molte discussioni e riflessioni nel settore per le sue ambiguità e incertezze normative.

Dal suo canto la Russia è accusata di aver trovato una sponda non solo in gruppi di hacktivisti (alcuni dei quali ritenuti infiltrati dall'intelligence), ma addirittura nei suoi gruppi cybercriminali (una recente [ricerca](#) di una società di cybersicurezza analizza come cybercriminali e attori statali russi condividano le stesse botnet di router compromessi che usano per anonimizzarsi).

In questo scenario, da un lato le persone (e gli stessi giornalisti) trovano nei social media una fonte importante e imponente di contenuti e testimonianze, che si mescolano però anche a una grande quantità di resoconti errati, post fuorvianti, misinformazione e disinformazione.

Con la conseguenza che anche i professionisti più qualificati fanno fatica a decifrare quello che vedono scorrere nel feed, e riconosciuti esperti di OSINT (che indica un'attività di analisi e ricerca su fonti aperte in Rete) sono i primi a indicare il proliferare di account che

simulano quelle pratiche investigative senza davvero seguirne i protocolli di accuratezza e verifica (c'è anche un termine per questo, OSHIT, [se ne parla qua](#)).

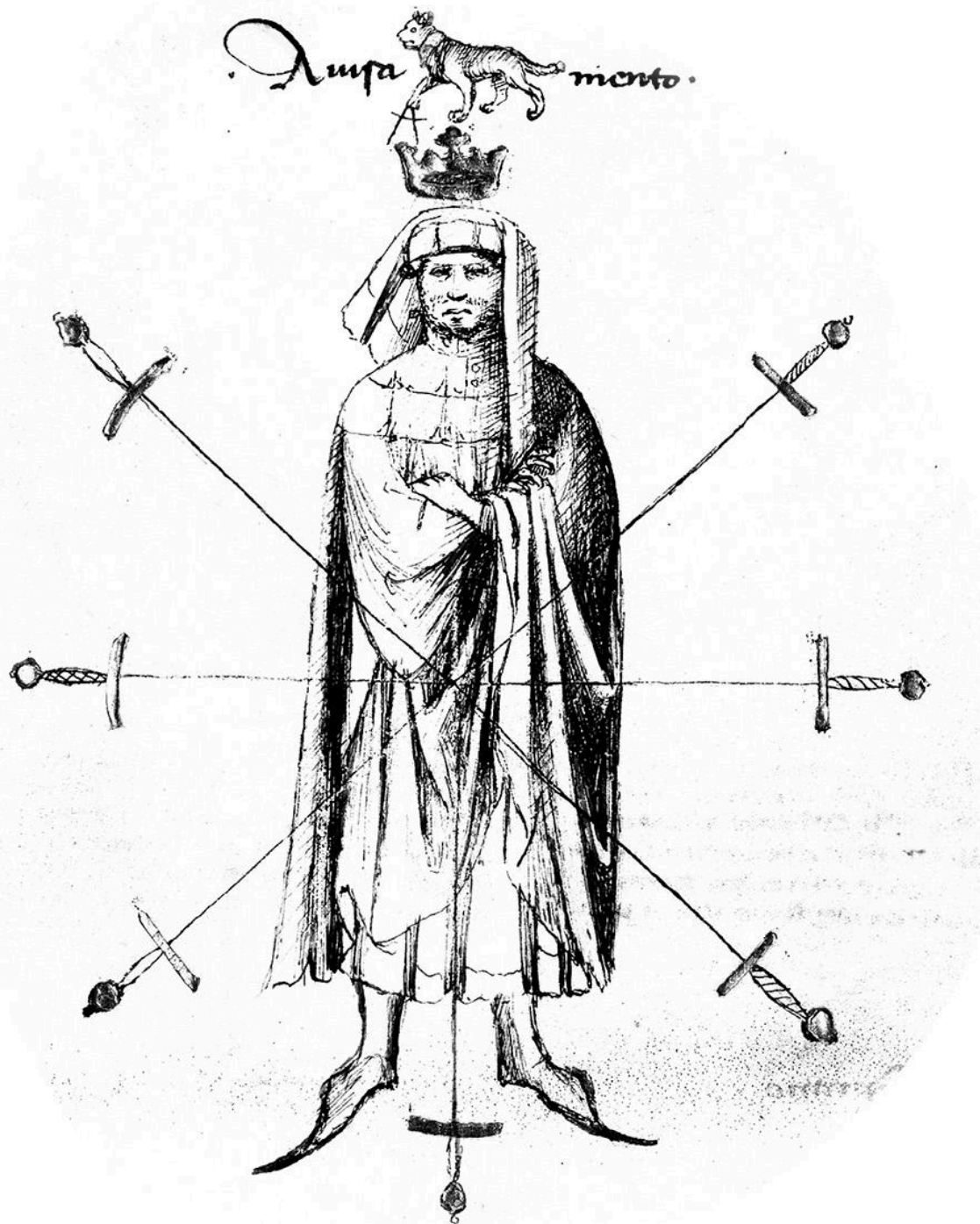
Per ora dunque l'esperienza di queste due guerre mostra come la dimensione cyber durante un conflitto militare sia soprattutto uno strumento tattico, di disturbo a bassa intensità e di sovversione, come scrive un recente [report](#) del Geneva Centre for Security Policy.

“Un aumento dello spionaggio e degli attacchi distruttivi dovrebbe metterci in guardia dal rischio di guerra, così come le concentrazioni di truppe, le esercitazioni offensive ravvicinate e le frequenti violazioni dello spazio aereo”, scrive ancora il report del German Institute for International and Security Affairs, aggiungendo che proprio in questa fase sia necessario un controllo pubblico.

Per quanto sia allettante ed efficace condurre in tempo di pace operazioni di spionaggio di rete, furto e distruzione di dati, continua il report, i parlamenti, i cittadini e la stampa dovrebbero interrogarsi criticamente sulle motivazioni nazionali e governative nello sviluppo di capacità informatiche nazionali o militari. “Uno strumento inadatto alla guerra può farla attraverso operazioni in tempo di pace”.

Senza dimenticare che in alcuni Paesi, i comandi informatici e altre unità cyber possono essere sviluppati anche per scopi politici interni. E le partnership pubblico-privato non aiutano la trasparenza. Per questo “i parlamenti, i cittadini e la stampa dovrebbero chiedere una più chiara separazione dei poteri e dei mandati. Per farlo occorre separare deliberatamente, anziché centralizzare, i poteri statali in campo cyber: ovvero la gestione degli incidenti a livello nazionale, l'applicazione della legge, l'intelligence, la difesa militare cyber e la diplomazia”, conclude il report.

Controllare i controllori è qualcosa di molto difficile da fare in tempi di guerra. Per questo è imperativo iniziare a farlo durante la pace.



LA PRIMA MONDIALE DI UN CYBER ESERCITO UOLONTARIO

Il governo ucraino ha lanciato un appello su vasta scala per sostenere i propri attacchi informatici contro Mosca, creando un ibrido né civile né militare. Un precedente da guardare con attenzione, senza sottovalutarne i rischi.

di Rosita Rijtano

Guerra in Ucraina

Su Telegram l'hanno definita la loro cyber-Chornobaivka, la città del sud Ucraina occupata dalle truppe russe nei primi giorni di guerra, e poi liberata dalle forze di Kyiv. Si tratta di Mosnet, un fornitore di servizi Internet con base a Mosca finito offline il 16 aprile scorso dopo un attacco sferrato dalla IT Army: una sorta di esercito digitale volontario che il Governo ucraino ha creato subito dopo l'invasione ordinata da Vladimir Putin, con lo scopo di consentire a chiunque, da qualsiasi parte del mondo, e anche senza particolari competenze informatiche, di sostenere la sua resistenza cyber.

“Che giornata”, scrivono gli amministratori della chat per celebrare il colpo, al 28 aprile 2024 uno degli ultimi successi. Oggi il canale IT ARMY of Ukraine conta 146.445 seguaci. Una cifra quasi dimezzata rispetto ai primi giorni del conflitto ([raccontati](#) nella newsletter Guerre di Rete), quando il numero di iscritti ha raggiunto la quota record di 300mila per poi assestarsi a lungo sopra i 200mila. Ma il calo non preoccupa il ministero della trasformazione digitale di Kyiv, che ha dato vita al cyber battaglione: “È vero che i nostri follower su Telegram sono diminuiti”, ammettono dal ministero rispondendo alle domande di Guerre di Rete. Ma – precisano – “il parametro non rappresenta

l'efficacia e la forza dell'IT Army. Anzi. In questi anni, le nostre capacità operative sono aumentate in maniera costante, con una crescita mensile del 10-25 per cento del traffico generato e dei membri attivi coinvolti (la stima, secondo altre fonti interne all'armata, è di circa 10-15mila persone, ndr). Questo incremento sottolinea la dedizione duratura e le competenze sempre più evolute all'interno dei nostri ranghi”.

IT Army of Ukraine, genesi ed evoluzione

Ted, nome di fantasia, fa parte dei volontari dell'esercito digitale ucraino fin dalla prima ora. Non era del tutto estraneo all'ambiente informatico: è proprietario di una compagnia hi-tech, di cui non vuole rivelare i dettagli. Ma non si era mai occupato di cybersecurity.

“Quando sono fuggito da Kyiv, trasferendomi con la mia famiglia nella parte occidentale dell'Ucraina, mi sono subito chiesto cosa potessi fare per il mio Paese”, racconta a Guerre di Rete. L'esercito digitale gli è sembrato lo sbocco naturale, “al fronte sarei stato inutile”. Ted definisce la nascita dell'IT Army una “fortunata coincidenza”.

“I primi giorni nessuno sapeva con chiarezza cosa fare e in che modo potessimo contribuire alla guerra – prosegue -. Le decisioni sono state più dettate dal fiuto che da una precisa strategia. Abbiamo inventato tutto strada facendo. È noto che l'Ucraina sia patria di talentuosi esperti di cybersecurity. Ma è stato subito chiaro che non potevamo più continuare a contare solo su di loro per lanciare offensive contro la Russia. L'intuizione geniale è stata trovare il modo di coinvolgere il più ampio numero di persone possibile, a prescindere dalle loro competenze. L'interesse globale ci ha sorpreso”.

Analizzandola, però, la storia della IT Army è meno naif di come la presenta Ted. In un [report](#) pubblicato nel giugno del 2022 dal Center for security studies del politecnico federale di Zurigo (ETH Zurich), il ricercatore Stefan Soesanto ne collega la genesi a Yegor Aushev, un

imprenditore hi-tech molto conosciuto, nonché collaboratore del Governo e fondatore di tre aziende diventate sempre più rilevanti negli ultimi otto anni, cioè dall'invasione della Crimea in poi: Cyber Unit Tech, Cyber School e Hacken.io.

Secondo la ricostruzione di Soesanto, sarebbe stato lui a suggerire l'idea al ministro della trasformazione digitale Mykhailo Fedorov, all'epoca trentunenne. Mentre, in parallelo, Aushev si occupava di reclutare come volontari dei professionisti del settore, rispondendo alla richiesta di un non meglio precisato ufficiale del ministero della difesa.

“Cyber-comunità ucraina! È ora di partecipare alla protezione informatica del nostro Paese”, scriveva in un post pubblicato su vari forum il 24 febbraio 2022, di cui [ha dato notizia l'agenzia Reuters](#).

Due giorni dopo, il 26 febbraio, è stato Fedorov a rilanciare la palla, alzando la posta con un [annuncio](#) diffuso su Telegram, Facebook e X (ex Twitter). Messaggi leggermente diversi tra loro – più diretto a un pubblico globale quello scritto su X, e più orientati ai cittadini ucraini gli altri due – ma con un comune denominatore: l'invito a supportare la lotta online di Kyiv. Questo il testo pubblicato sia su Telegram sia su Facebook: “In Ucraina abbiamo un sacco di talenti nella sfera digitale: sviluppatori, designer, copywriter e così via. Stiamo creando una IT Army. Tutti i compiti operativi verranno presentati in un canale Telegram: t.me/itarmyofukraine. Ci saranno compiti per tutti”.

Tra bug bounty e intelligence

Un'iniziativa ufficiale che non ha fermato il coinvolgimento di Aushev nell'operazione, a cui l'imprenditore ha dato un'ulteriore forte spinta il 3 marzo 2022 con un programma di bug bounty, cioè quei premi in denaro che le società hi-tech offrono ai ricercatori di sicurezza informatica in grado di trovare delle vulnerabilità, potenzialmente sfruttabili dai criminali cyber, nei propri sistemi. Il nome della

competizione lanciata dall'imprenditore di Kyiv era tutto un programma: "HACK RUSSIA". La sfida consisteva nel trovare delle falle per attaccare obiettivi russi, da riportare a un indirizzo Gmail, per una golosa posta in palio: ben 100mila dollari in criptovalute.

Il coinvolgimento di Aushev, i suoi legami con il ministero della difesa, e la considerazione che per i servizi di intelligence del Paese, lasciare che l'IT Army "conduca le proprie operazioni in modo libero e indipendente, soprattutto in tempo di guerra, sembra non solo essere una forzatura analitica ma potrebbe anche determinare una confusione strategica e a delle interferenze tattiche in campo militare", hanno portato Soesanto a ipotizzare un legame tra le diverse entità. "Sul fronte pubblico – sostiene il ricercatore –, l'IT Army serve da contenitore per sfruttare volontari da ogni parte del mondo nelle persistenti attività informatiche contro il Governo e le compagnie russe. (...) Sul fronte privato, invece, il nucleo centrale di questo esercito mantiene dei profondi legami con (o è composto in prevalenza da) membri dei servizi di intelligence e difesa di Kyiv".

Coordinare la decentralizzazione

Tesi plausibile, ma non facile da provare, dati i molti omissis che riguardano l'operazione: primo fra tutti il numero di individui effettivamente coinvolto, che rimane ignoto persino agli stessi vertici ucraini. Di certo, l'organizzazione della cyber armata sembra essersi evoluta nel tempo. Così come sono cambiate le modalità di partecipazione. Mentre a rimanere immutato è stato il tipo di attacco informatico preferito, cioè i Distributed Denial of Service (DDoS): traducibile in italiano come Negazione distribuita del servizio, consiste nel tempestare di richieste un sito fino a metterlo ko e renderlo irraggiungibile. Come ricostruisce la ricerca del politecnico di Zurigo, appena nata la IT Army si componeva di un nucleo centrale di coordinamento, mantenendo una struttura organizzativa decentrata e

diffusa. Una impostazione che preserva tutt'ora, anche se – a differenza della base volontaria – il vertice è man mano diventato più importante e articolato. “Possiamo individuare tre livelli”, spiega Ted a Guerre di Rete: “Un team che si occupa di pianificare le attività, individuando gli obiettivi da attaccare. Un altro che sviluppa i software necessari all'operazione e, infine, c'è chi si occupa della comunicazione: per un'organizzazione di questo tipo è fondamentale motivare il proprio pubblico e informarlo delle missioni che sta portando avanti”.

Anche perché oggi arruolarsi è davvero alla portata di tutti. In prima battuta funzionava così: i target venivano condivisi su Telegram e gli utenti erano incoraggiati a “utilizzare ogni vettore di attacco cyber e DDoS contro queste risorse”. Chi voleva partecipare, pur non avendo alcuna competenza informatica, poteva collegarsi a delle pagine web che avrebbero dirottato il traffico verso dei portali moscoviti. C'erano poi gli account Instagram degli oligarchi, e delle loro famiglie, da prendere di mira. I video e i canali YouTube da segnalare. Viceversa, i più esperti erano attratti con alcune sfide, come far comparire dei video negli schermi della metropolitana di Mosca, e potevano seguire passo dopo passo dei manuali caricati su GitHub (la piattaforma su cui gli sviluppatori di tutto il mondo condividono i propri codici sorgenti) per installare strumenti più potenti utili alle offensive. Adesso chi ha le capacità può ancora cimentarsi in attacchi di diversa complessità, ma a tutti gli altri è sufficiente un click per trasformare il proprio computer in un'arma cibernetica. Basta scaricare un software per diventare un cyber soldato a servizio di Kyiv. Si chiama IT Army Kit e l'identità dei suoi programmatori rimane celata dietro una sigla e un hashtag che ha accompagnato l'esercito informatico ucraino sin dalle origini, l'#Uacybershield: “un'organizzazione operativa fin dal 24 febbraio 2022, il secondo giorno dell'invasione su vasta scala dell'Ucraina da parte di Mosca”, recita la sua auto-descrizione. Eppure nulla è lasciato al caso. Carica di simbolismo è pure l'immagine di sfondo del suo sito

riferimento, cyberarmy.com.ua: la maschera di Guy Fawkes, il più noto tra i cospiratori inglesi che volevano far esplodere la camera dei lord a Londra nel 1605, diventata icona anche del collettivo hacker

Anonymous. Sotto la scritta: “Gloria all’Ucraina. Nave militare russa vai all’inferno”.

Di contro, la chat fondata da Pavel Durov ha via via perso quasi del tutto la propria connotazione operativa, diventando sempre di più – se non quasi esclusivamente – uno strumento di propaganda. Ci sono messaggi che celebrano il successo di alcune operazioni, altri ancora che elogiano i posti di lavoro creati nel settore digitale, e persino alcuni che diffondono la cultura cyber. Come un post che racconta la storia di Kevin Poulsen, conosciuto con lo pseudonimo di “Dark Dante” (il Dante oscuro): un hacker statunitense arrestato dall’Fbi negli anni Novanta per, tra le altre cose, aver violato dei database federali, che è diventato un “rispettato giornalista esperto di cybersicurezza” dopo la prigione.

Tra attacchi informatici e propaganda

“Se riusciamo a bloccare le ferrovie, anche solo per un paio di ore, è una grande soddisfazione”. Ted non ha dubbi sul fatto che l’IT Army stia dando un importante contributo al conflitto, anche se in concreto la cyber-guerriglia è molto lontana dalla stereotipizzazione costruita dai media. “Il nostro ruolo è, prima di tutto, quello di contribuire a esaurire le risorse finanziarie del nemico, soprattutto nei settori in cui le sanzioni internazionali imposte a Mosca sono meno efficaci”, dice, aggiungendo: “Ormai è chiaro che la guerra non finirà finché Putin potrà finanziariamente sostenerla, ecco perché glielo stiamo rendendo sempre più difficile”. La sua più grande soddisfazione è stato un attacco condotto il 31 dicembre scorso contro Evotor, uno dei più grandi fornitori russi di software per i terminali di pagamento nei negozi. “Abbiamo bloccato oltre un milione di esercizi commerciali in tutto il Paese per più di un giorno”, sostiene Ted. Secondo il giornale online

ucraino [Ukraïns'ka pravda](#), per i russi la prima sera di Capodanno sarebbe stata un “vero e proprio collasso: i cittadini non sono stati in grado di pagare con la carta in negozi, caffè, parrucchieri o qualsiasi altra attività”. Un danno che Ted quantifica in centinaia di migliaia di dollari.

Non a caso, uno dei bersagli sin dall’inizio ricorrenti è stata Sberbank, una delle maggiori banche russe. I dati ufficiali, però, non ci sono e – anche in questo caso – stabilire in maniera oggettiva l’operatività, e l’efficacia, della cyber armata è difficile. Ci ha provato [una ricerca indipendente dell’università della Florida](#) pubblicata dal Journal of Strategic Security, che ha sfruttato un dataset realizzato dal Center for International and Security Studies del Maryland (CISSM). Ma lo stesso autore dello studio, William Done, mette in evidenza le lacune di questa banca dati: basandosi su fonti di intelligence open source, potrebbe non essere aggiornata sulle effettive operazioni realizzate; è impossibile verificare alcune delle informazioni visto che le autorità russe potrebbero non avere ammesso alcuni disservizi; e, infine, è ancorata a una prospettiva occidentale, con tutti i preconcetti che ne conseguono. “Nonostante i limiti – precisa Done – si tratta del database più completo e affidabile per stabilire il numero, le caratteristiche e gli obiettivi delle operazioni ucraine cyber offensive”. L’analisi prende in considerazione un lasso di tempo che va dal 26 febbraio 2022, data che coincide con la creazione formale dell’IT Army, al 31 gennaio 2023, individuando 151 attacchi documentati e verificati, di cui 58 direttamente o indirettamente coordinati, o controllati, dall’esercito digitale di Kyiv. Un contributo definito “critico” è stato dato dal collettivo Anonymous che avrebbe condotto il 52.9 per cento di tutte le operazioni dirette contro le entità della federazione russa, di cui il 20 per cento sotto la direzione dell’esercito digitale ucraino, contribuendo così al successo dei suoi attacchi cyber per circa un terzo.

L'obiettivo principale è stata la pubblica amministrazione centrale del Cremlino: uffici governativi, militari, e intelligence ma anche corpi legislativi e aziende controllate dallo Stato, come l'agenzia aerospaziale Roscosmos e il colosso del gas Gazprom. In seconda posizione troviamo l'industria dell'informazione. A differenza degli altri target, tempestati di attacchi DDoS, questo settore ha subito per lo più la manipolazione dei messaggi da remoto. Alcuni dei media finiti nel mirino sono nelle dirette mani dello Stato, per esempio l'agenzia di stampa TASS; e altri – invece – sono formalmente indipendenti, anche se di fatto pro-Putin (come Kommersant). “Questa attenzione agli organi di informazione riflette l'enfasi posta nel proteggere il morale e l'interesse ucraino dall'influenza esercitata da Mosca”, sottolinea il report. Terzo, e ultimo, comparto rilevante è quello finanziario, obiettivo del 13,8 per cento degli attacchi, di cui il 50 per cento diretto proprio contro Sberbank: “organizzazioni che – scrive Done – potrebbero indirettamente supportare il conflitto in corso, date le grandi risorse finanziarie a loro disposizione e le loro sostanziali responsabilità nel sostenere lo Stato russo”.

Ma, al di là dell'utilità operativa, è sul piano comunicativo che l'IT Army si gioca la partita principale. “È sbagliato aspettarsi che questa cyber armata sia cruciale per vincere la guerra, o possa avere un significativo impatto sul campo”, spiega a Guerre di Rete Vasileios Karagiannopoulos, professore associato in cybercrime e cybersecurity dell'università di Portsmouth. “Certo, può essere utile a danneggiare l'economia, ostacolare le truppe di Putin rallentando le comunicazioni, e a influenzare l'opinione pubblica russa diffondendo messaggi che bypassano la censura del Cremlino. Ma il suo contributo al conflitto sta più nel creare una pressione politica che nell'avere un effetto diretto”.

Tante ambiguità, troppi rischi

Karagiannopoulos definisce l'IT Army un "world first", una prima mondiale, di cui in Ucraina si discuteva già da tempo prendendo a modello l'Estonian Defense League's Cyber Unit: un'organizzazione simile nata in Estonia e guidata da un informatico, che coinvolge membri dell'esercito e soprattutto volontari con l'intento di proteggere le telecomunicazioni del Paese dalle minacce cyber.

Ma l'aperto reclutamento di così tante persone con lo scopo di condurre attacchi informatici sponsorizzati da uno Stato non ha precedenti.

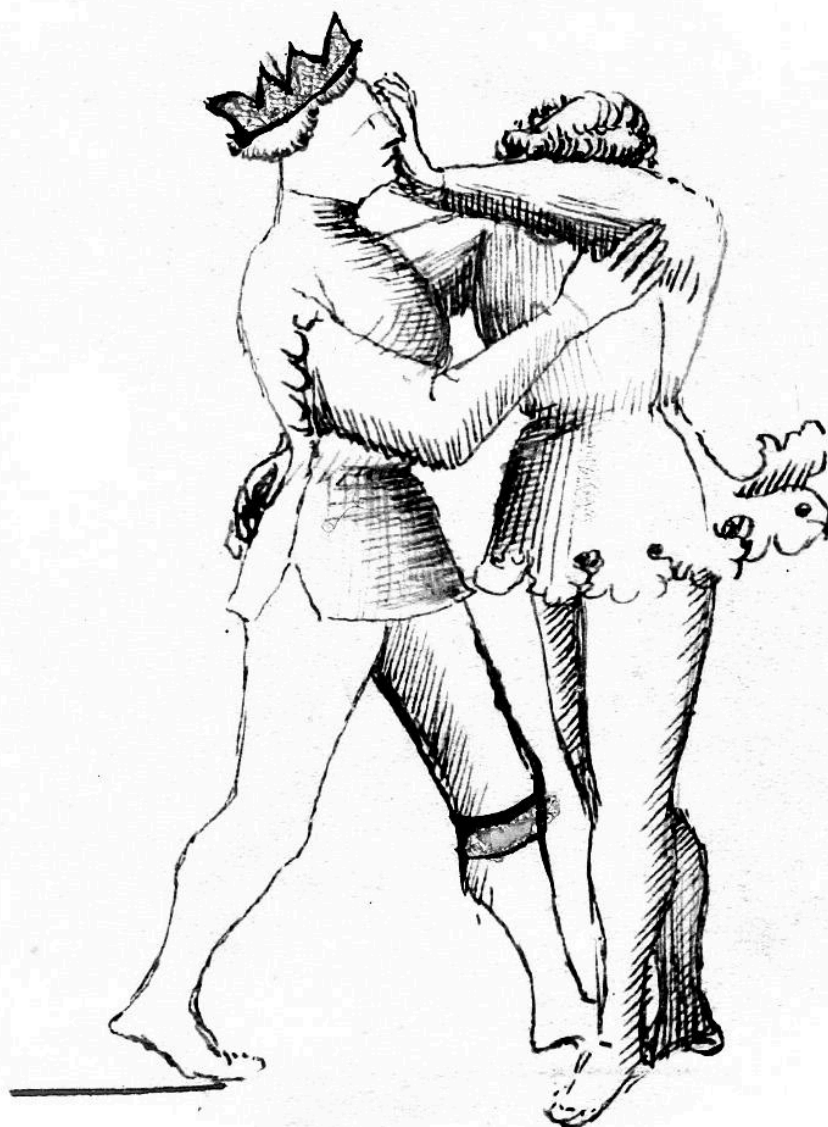
“Nessun governo prima – prosegue il ricercatore – aveva mai lanciato un appello agli hacker, e non solo, di tutto il mondo chiedendo di supportare i propri sforzi bellici, diventando parte integrante delle proprie operazioni militari ibride”. Una caratteristica che distingue le cyber-reclute pro Kyiv dai classici hacktivisti, da tempo impegnati politicamente nelle questioni internazionali, compresi gli scenari di guerra. Solo come ultimo esempio, li abbiamo visti (virtualmente) scagliarsi contro Israele per i bombardamenti in Palestina. Ed è così che, per Karagiannopoulos, l'hacktivismo si manifesta nella sua forma più pura: “Cyber-azioni di protesta, o di supporto a una delle parti in causa, che promuovono la difesa dei diritti umani. Anche in Ucraina la Russia sta violando i diritti, la differenza è che dietro la costituzione dell'IT Army c'è il Governo di Kyiv”. Questo conferisce ai suoi combattenti uno status speciale: “Non hanno alcun legame formale con le istituzioni ucraine, eppure partecipano alle sue operazioni, trovandosi a metà strada tra l'essere parte dell'esercito ucraino e dei semplici attivisti”, conclude il docente.

Un ibrido – né civile né militare, né legale né illegale, né pubblico né privato – che espone chiunque prenda parte al battaglione anche a seri rischi, e costituisce un precedente a livello internazionale da guardare

con attenzione. Anche perché l'IT Army ha dato vita a un intero ecosistema che si compone di compagnie informatiche ucraine, o fondate da ucraini, e da ucraini che lavorano per aziende tecnologiche occidentali. Non solo: più in generale, dall'inizio dell'invasione, il Paese ha potuto contare sul supporto di molti giganti hi-tech che hanno fornito risorse e competenze, creando in certi casi anche nuovi strumenti e nuove conoscenze. Solo qualche esempio: Amazon Web Services ha fornito degli strumenti per il backup; mentre Cloudflare e Google hanno messo a disposizione dei servizi di cybersecurity, mentre Starlink ha fornito i propri satelliti per la connessione internet. Fin da subito il ministero degli affari esteri russo [ha condannato](#) “la continua aggressione informatica da parte dell'Occidente collettivo”, minacciando possibili “drammatiche conseguenze” per le persone coinvolte. Pure il comitato centrale della Croce rossa [si è detto preoccupato](#) per “la pratica di reclutare civili nelle attività informatiche militari”, mettendo in guardia: “Anche se non tutte le modalità di coinvolgimento dei civili sul campo di battaglia digitale si qualificano come partecipazione diretta (al conflitto, ndr), il pericolo è che possano essere considerati come dei nemici, esponendoli al rischio di gravi danni”.

L'Ucraina sta lavorando a una legge che punta a mettere fine a ogni incertezza incorporando i membri dell'armata nella componente di riserva delle proprie forze armate, sul modello di estone. Ma al momento la questione rimane aperta. Un'altra ambiguità la sollevava la ricerca del politecnico federale di Zurigo, mettendo in evidenza che non è ancora chiaro se il ministero della trasformazione digitale ucraino abbia avuto, o meno, l'autorità legale per creare un organismo del genere. Anche se sono passati due anni dalla pubblicazione, la conclusione di Soesanto offre ancora oggi spunti che fanno riflettere: “Gli osservatori e i governi occidentali – scriveva – credono che l'IT Army si componga di un insieme casuale di volontari che portano

avanti attacchi DDoS senza senso contro siti web russi. Fino ad ora hanno fallito nel riconoscerne la struttura organizzativa sottostante, la condotta operativa e l'ecosistema più ampio che è alla base dell'armata, così come della lotta dell'Ucraina per il dominio cibernetico e dell'informazione. Nel bene e nel male, continuare a ignorare l'essenza dell'esercito digitale di Kyiv costituirà un fattore di caos per la futura stabilità del cyberspazio, e quindi della sicurezza europea, ma non solo”



LA CYBERWARFARE PROMESSA TRA ISRAELE, IRAN E HAMAS

Per anni l'Occidente pacificato ha fantasticato sulle guerre del futuro, tra suggestioni in stile *War Games* e ispirazioni cyberpunk. In realtà finora la dimensione cyber del conflitto è rimasta marginale, sostenendo le operazioni cinetiche. Il valore strategico delle operazioni informatiche si colloca prima del conflitto, e poi lo accompagna sul piano della propaganda.

di Raffaele Anglus

Medioriente

Sono appena passate le tre del mattino del 27 giugno 2022 quando in un'industria siderurgica di Khuzestan, sulla costa occidentale dell'Iran, un crogiolo pieno di acciaio fuso si rovescia spargendo il suo contenuto per tutta la fabbrica. L'incidente non è però riconducibile a un problema tecnico o a una disattenzione: appena poche ore dopo, un gruppo di criminali informatici che si fa chiamare Gonjeshke Darande ("Passero Predatore" in farsi) ha rivendicato un'azione offensiva ai danni dell'azienda iraniana, sostenendo di aver causato lo sversamento di proposito. A corredo dell'annuncio, ci sono le riprese di due diverse telecamere a circuito chiuso dalle quali è possibile vedere il momento in cui la cisterna ha preso fuoco inondando la fabbrica.

Le immagini, divulgate sui social e poi riprese dalla stampa mondiale, mostrano due operai uscire dal campo della telecamera undici minuti prima dell'incidente; in sovrimpressione un messaggio rivolto al pubblico: "Come potete vedere questo attacco informatico è stato condotto prestando attenzione a proteggere individui innocenti".

Sebbene Predatory Sparrow operi nell'anonimato, modalità e frequenza delle operazioni rivendicate lasciano pensare a un APT - Advanced Persistent Threat - ovvero a un'organizzazione statale o parastatale che dispone di risorse, mezzi e di un bersaglio privilegiato e costante nel tempo: l'Iran. Rafforza questa convinzione persino il nome scelto dal gruppo, in cui sembra nascondersi un riferimento a un'altra gang responsabile di cyber attacchi, in questo caso di riconosciuta origine iraniana: l'APT Charming Kitten, ovvero gattino fascinoso.

Per Teheran non sembrano esserci dubbi sul fatto che dietro Predatory Sparrow si nasconda in realtà il Governo israeliano, così come Charming Kitten è ritenuto essere da molte aziende di sicurezza (tra cui [Google](#), [Recorded Future](#), Proofpoint) il braccio armato digitale dell'Iran. Quest'ultimo è ritenuto responsabile di una serie di attacchi che perdurano da anni e che hanno avuto come principale obiettivo l'infiltrazione all'interno di organizzazioni statali statunitensi e israeliane, l'acquisizione di informazioni di intelligence e lo spionaggio di dissidenti iraniani residenti in Europa, come rivelato anche da un recente [report](#) dei servizi segreti tedeschi.

In un'immaginaria serie di scaramucce tra i due gruppi (non è possibile affermare che agiscano l'uno in risposta all'altro), la mossa più recente - nonché la più scenografica - è quella di Predatory Sparrow, che a dicembre del 2023 ha messo fuori servizio il 70% dei distributori di benzina iraniani, mandando nel caos il Paese. Il messaggio che accompagnava la rivendicazione dell'attacco, pubblicato sui social network, termina con un monito [rivolto al leader della Repubblica Islamica](#): "Khamenei, scherzare con il fuoco ha un costo".

Un conflitto ben poco virtuale

Che tra Israele e Iran si stia consumando da tempo un conflitto a intensità variabile che vede operazioni cinetiche alternarsi ad attività di

intelligence cibernetica, gesti dimostrativi e operazioni di sabotaggio vere e proprie è un dato di fatto documentato.

Proprio a Israele, insieme agli Stati Uniti, è attribuita la paternità di Stuxnet: il primo malware a noi noto a essere stato sviluppato e scagliato contro un altro Paese per sabotarne la capacità di produrre uranio arricchito. Correva l'anno 2010 e dopo quasi quindici anni l'episodio è considerato all'origine del concetto moderno di cyberwarfare, cioè dell'impiego di "Internet per attaccare i computer di un Paese per danneggiarne comunicazioni, sistemi di trasporto e forniture idriche ed elettriche", per dirla con la [definizione](#) impiegata dall'Oxford Dictionary.

Tuttavia, col diradarsi delle nubi della guerra cibernetica, fatta prevalentemente di intelligence e gesti scenografici, sul campo predominano ancora droni, missili e carri armati. Non fanno eccezione i recenti sconvolgimenti geopolitici quali l'invasione russa dell'Ucraina o l'offensiva scagliata da Israele nei confronti di Gaza, all'indomani dell'attentato del 7 ottobre compiuto da Hamas contro civili israeliani. In nessuno di questi episodi, né in alcuna delle risposte, la tecnologia sembra aver giocato un ruolo cruciale - quando non decisamente estetico -, lasciando che a parlare fossero ancora oggetti detonanti e proiettili. E anche Predatory Sparrow e Charming Kitten hanno diminuito le loro azioni, sempre puntualmente rivendicate tramite i canali social.

Lo rivela il [report Tool of First Resort](#) di Google, con cui gli esperti del colosso di Mountain View a febbraio hanno analizzato il conflitto cyber tra Israele, Hamas e l'Iran, sia prima sia dopo l'attentato del 7 ottobre. "I gruppi collegati ad Hamas sono stati attivi per tutto settembre 2023 con le loro tipiche attività - si legge - e non è stato osservato alcun incremento di queste (nel periodo, ndr) precedente al 7 ottobre".

Secondo i tecnici del Threat Analysis Group di Google e di Mandiant le offensive si sarebbero limitate a campagne di phishing e all'impiego persistente di malware contro entità israeliane. "Attività in linea con le tipiche operazioni cibernetiche condotte da gruppi collegati ad Hamas", osservano gli esperti. Un'ulteriore conferma arriva dal numero uno per la cybersicurezza della National Security Agency statunitense, Rob Joyce, che ha confermato come intorno al 7 ottobre le operazioni dell'organizzazione palestinese non abbiano visto incrementi degni di nota.

Parimenti si può dire dell'Iran, le cui attività a oggi note non sembrano aver preparato il campo all'attacco del 7 ottobre (l'Iran da tempo foraggia i gruppi di palestinesi a Gaza), né coadiuvato i palestinesi nelle settimane successive. Intorno all'operazione terroristica che ha visto la morte di oltre mille israeliani e il rapimento di 250 persone i sismografi del mondo cibernetico non hanno registrato scosse.

La risposta di Tel Aviv

Nonostante la grande considerazione di cui gode Israele nel mondo dell'innovazione tecnologica e della sorveglianza digitale, l'operazione fisica e sul campo di Hamas è andata perfettamente a segno incontrando pochi o nessun ostacolo. A poco sono servite le sparute informazioni di intelligence di cui si aveva conoscenza, che non hanno comunque sortito l'effetto di rafforzare le difese del Paese, o le avanguardistiche tecnologie nella disponibilità dei tecnici legati al governo. La risposta, al contrario, è stata immediatamente muscolare - con oltre 30mila morti tra i cittadini gazawi in sei mesi di operazione a Gaza. "Non sono a conoscenza di particolari attività o investimenti governativi nel campo della cybersecurity negli ultimi mesi" ha spiegato a Guerre di Rete Chuck Freilich, ex vice consigliere per la sicurezza nazionale di Israele e ricercatore dell'Istituto per gli studi sulla sicurezza nazionale dell'Università di Tel Aviv: "Ci sono stati

sicuramente molti attacchi cibernetici contro Israele dal 7 ottobre, specialmente dall'Iran, ma devo dire che me ne sarei aspettati di più, non solamente in quantità ma soprattutto in qualità: si è trattato perlopiù di attacchi relativamente poco sofisticati e non sensazionali", ha spiegato l'esperto.

Proprio Freilich è autore di [uno studio](#) pubblicato a gennaio del 2024 nel quale è analizzata l'attività informatica dei principali antagonisti di Israele all'indomani del 7 ottobre. Le prime settimane del conflitto hanno visto l'attivazione di quindici gruppi di hacker affiliati all'Iran, Hezbollah e Hamas. Tuttavia è chiaro che le operazioni condotte non fossero premeditate né coordinate con Hamas, ma che abbiano semplicemente provato a sfruttare l'attacco terroristico a sorpresa operando in modo reattivo, cogliendo le opportunità man mano che si presentavano, secondo quanto si sostiene nello studio.

Gli attacchi iraniani includevano un numero vasto di attacchi DDoS relativamente semplici (attacchi distribuiti di negazione del servizio che puntano a rendere temporaneamente inaccessibile un servizio), progettati per interrompere i siti web israeliani, in particolare quelli dei media e delle aziende software, oltre a banche, istituzioni finanziarie e siti governativi. Secondo [l'analisi](#) dell'ex vice consigliere nazionale per la sicurezza di Israele, questi attacchi hanno raggiunto il picco di un milione di tentativi di accesso al secondo nei primi sei giorni di guerra, per poi diminuire nelle settimane successive.

Un'operazione di particolare rilievo ha colpito il sito web del Jerusalem Post, che è stato messo offline per alcuni giorni, mentre un'altra ha puntato a interrompere le attività dell'Ospedale Ziv. Ma, per quanto intensi, gli attacchi non sembrano aver avuto un impatto significativo sulle infrastrutture critiche.

"Mi sarei aspettato di vedere più "cyber" in Ucraina (nel conflitto russo-ucraino, ndr) così come me ne sarei aspettato di più in questo conflitto: credo che la prospettiva di una cyberwarfare sia stata un po' gonfiata nel tempo", riconosce Freilich. Secondo l'esperto, il periodo di maggiore attività intorno a Israele risale agli anni tra il 2020 e il 2021, quando "hacker iraniani hanno concentrato i loro attacchi contro una serie di aziende israeliane sottraendo dati particolarmente sensibili e conducendo attacchi ransomware con un'intensità maggiore". Ma le difese sono migliorate e il costo degli attacchi (principalmente nel rapporto tra tempo necessario e risultati ottenuti è lievitato): "Le capacità cibernetiche si sono dimostrate particolarmente efficaci sul lato dell'intelligence e dello spazio informativo, ma è qualcosa che, con metodi diversi, la gente ha fatto fin dalle origini della civiltà e che funziona meglio prima dell'esplosione del conflitto vero e proprio".

Ne è una prova il peculiare insieme di capacità in cui si sono specializzati gli hacker palestinesi, che negli anni hanno sviluppato una routine nella creazione di profili falsi dalle sembianze di ragazze avvenenti, utilizzati per attirare i soldati israeliani nelle loro trappole virtuali. Come riportato nel libro *Israel and the Cyber Threat* (Freilich, M. Cohen, G. Siboni; Oxford University Press), si contano a centinaia gli episodi in cui operativi dell'esercito israeliano sono stati indotti a rivelare informazioni o addirittura a installare dei software che contenevano segretamente degli spyware, tramite app di dating e social network.

"Ma anche queste operazioni rientrano più nella sfera della intelligenza umana che della cyberwarfare", spiega a Guerre di Rete Stefano Zanero, professore ordinario di sicurezza informatica del Politecnico di Milano. "È il tipico cliché dei film di 007, che ovviamente si è aggiornato nel tempo in quanto dispone anche di strumenti diversi, ma anche questo tipo di operazioni ha un valore strategico intrinseco prevalentemente

nelle fasi precedenti allo scoppio di un conflitto - insieme alle operazioni di sabotaggio, propaganda e demoralizzazione: come vediamo, la guerra vera e propria si risolve in un conflitto sempre e comunque tradizionale". Con buona pace della Nato, che già dal 2016 annovera quello cibernetico quale quinto dominio della warfare, insieme ad aria, terra, mare e spazio.

"Una definizione con cui in tanti non siamo d'accordo - commenta Zanero - dal momento che tutti gli altri domini hanno una componente topologica e la possibilità per uno stato tecnologicamente avanzato di mantenerne o difendere il controllo e di esercitare una propria superiorità, quello cibernetico è più un elemento verticale agli altri domini: può garantire un bonus sul campo se sfruttato dal nemico e costituisce un asset da difendere su tutti gli altri domini. Basti pensare all'esigenza di proteggere o, al contrario, di attaccare un radar per esempio. È il concetto di electronic warfare che è sempre stato spalmato sugli altri domini".

In pratica più che uno spazio a sé stante, l'elemento cyber sarebbe integrato in tutti gli altri domini.

A valle di tutte le promesse non mantenute di un mondo moderno che avrebbe dovuto condurre le proprie battaglie sui server e non nelle trincee, resta l'importanza della rete nel diffondere e acquisire informazioni, dare prova della propria forza sul campo e organizzare campagne di disinformazione il cui impatto può essere difficilmente calcolabile al netto dell'episodio scelto per condurre una narrazione a sé favorevoli. Proprio come un crogiuolo che si rovescia dentro una fabbrica e il terrore che da simili immagini può scaturire.



SE IL FEED È UN CAMPO MINATO

Le campagne di disinformazione online sono ormai parte integrante delle operazioni militari, assegnando alle reti sociali un ruolo sempre più strategico negli scenari di guerra. Ma le piattaforme sono tutt'altro che neutrali.

di Irene Doda

Social Media

Quando il 7 ottobre 2023 Hamas ha attaccato i villaggi e le città israeliane, e ancor prima la Russia ha invaso l'Ucraina, il pubblico e gli osservatori internazionali si sono trovati a dover raccogliere gran parte delle informazioni dai social media. Le piattaforme hanno dunque svolto (e continuano a svolgere) un ruolo attivo nella nostra percezione dei conflitti e nei comportamenti delle parti in causa. Sono state usate non solo come canali per diffondere informazioni e narrazioni, ma anche come armi, diventando quello che gli esperti Emerson Brooking e Peter Singer hanno [definito](#) “un nuovo campo di battaglia presente nei nostri smartphone”. Prendendo ad esempio i più recenti conflitti, in Medio Oriente e in Ucraina, cerchiamo di fare un punto sull'evoluzione del ruolo dei social, che mai come ora hanno un peso negli scenari di guerra e nelle relazioni internazionali.

Brooking e Singer hanno pubblicato un'approfondita analisi sulla weaponization (espressione che può essere tradotta come “trasformazione in armi”) delle piattaforme. Il libro, dal titolo LikeWar, è uscito nel 2018. Da allora lo scenario è molto cambiato: “Nel 2018 la convergenza tra social e guerra era una novità”, racconta a Guerre di Rete Emerson Brooking: “Oggi, invece, gli attori di un conflitto

conoscono bene il potere di internet. Non si discute più se usarlo o meno, ma come farlo in modo efficace. Le campagne di marketing online sono perfettamente integrate alle operazioni militari”.

I social media come canali di (dis)informazione

In primis, le piattaforme possono diffondere e amplificare la disinformazione. Durante il primo mese del conflitto nella Striscia di Gaza un'[inchiesta](#) di ProPublica e del Tow Center for Digital Journalism della Columbia University di New York ha evidenziato come su X (ex Twitter) siano proliferati contenuti manipolati, informazioni fuori contesto, oppure semplicemente vecchie e relative ad altre zone di guerra. In tutto, questi post hanno ricevuto oltre mezzo miliardo di visualizzazioni. Verificare le informazioni condivise dagli utenti è molto più difficile da quando la piattaforma è stata acquistata dal magnate Elon Musk e la cosiddetta spunta blu - prima riservata ad account di interesse pubblico e indice di affidabilità - è diventata a pagamento. Secondo il Digital Services Act (DSA) - il regolamento europeo sui servizi digitali -, proprio per chiarire il modo in cui X tratta i contenuti violenti e illegali la Commissione Europea ha aperto [un'inchiesta](#). Uno degli esempi riportati da ProPublica è quello di Sprinter, un profilo con spunta blu che ha twittato decine di contenuti falsi, promuovendo la narrativa (più volte smentita) che Hamas stia ricevendo sostegno dall'Ucraina.

Una situazione di cui approfittano sia attori statali che non statali. In uno [studio](#) del 2020, l'Oxford Internet Institute ha identificato 81 paesi, tra cui grandi potenze come gli Stati Uniti, l'India, la Cina e l'Iran e lo stesso Israele, che utilizzano cyber truppe per diffondere narrative manipolate e disinformazione. Tra le tattiche utilizzate c'è anche quella di spendere milioni in pubblicità per creare notizie per sostenere una campagna militare e il governo, o contro gli oppositori politici. “Anche prima dell'occupazione della Crimea da parte della Russia e del

conflitto in Ucraina orientale, il Cremlino ha elaborato una sofisticata propaganda di Stato con cui ha diffuso disinformazione malevola, bugie ed esagerazioni. Come che Kyiv sia governata da nazisti e minacci la sopravvivenza delle persone di etnia russa. Tutto ciò ha giocato un ruolo cruciale nell'escalation delle tensioni in Ucraina e nell'alimentare il conflitto sin dal suo inizio, nel 2014", [riporta](#) l'ong Human Rights Watch. La propaganda di guerra russa è stata particolarmente efficace nel raggiungere l'opinione pubblica sia interna che mondiale, utilizzando tutte le piattaforme più popolari: da [TikTok](#) a [Twitter](#), passando per le applicazioni di [Meta](#).

Per quanto riguarda il conflitto Hamas-Israele, tra i casi che hanno creato più confusione - e, comprensibilmente, orrore - c'è stata la violenza contro dei minori. La corrispondente di una rete privata israeliana ha affermato che "i soldati dell'IDF (Israel Defence Forces) le hanno detto di aver visto dei bambini molto piccoli decapitati" dai miliziani di Hamas. La storia è diventata subito virale. Su [Facebook](#) alcuni post che la raccontano - come il video postato dal senatore Ted Cruz - hanno raggiunto quasi 100.000 visualizzazioni. La vicenda però non è [mai stata](#) definitivamente [confermata](#). In ogni caso, sono stati 36 i bambini uccisi nell'attacco di Hamas, [riporta](#) France24.

L'esposizione a contenuti di guerra sui social media ha anche ricadute sulla salute mentale degli utenti. Ecco perché alcuni esperti sconsigliano di leggere le notizie sulle piattaforme quando i conflitti sono in corso. Su The Conversation, Nir Eisikovits, filosofo ed esperto di etica, ha scritto: sui social "leggerete più spesso i contenuti che rispecchiano le vostre opinioni, vi sconvolgono, o entrambe le cose. In altre parole, il più delle volte l'impegno politico sulle piattaforme non crea alcuna nuova conoscenza, ma infiamma emozioni già esistenti. Quando si tratta di un conflitto storicamente contorto e così carico di emozioni, come la guerra tra Israele e Hamas, i risultati sono terribili".

Strategie a confronto

Talvolta, le policy interne delle piattaforme e le loro fragilità sono intenzionalmente sfruttate dagli attori in gioco. Non a caso Telegram, che ha politiche di moderazione [molto permissive](#), è stato uno dei primi social su cui Hamas ha diffuso i video dell'attacco del 7 ottobre. Prima che la piattaforma [iniziasse a limitare l'accesso](#) a diversi canali affiliati ad Hamas, il gruppo palestinese l'ha utilizzato con il preciso scopo di disorientare e terrorizzare i cittadini israeliani. "Hamas ha riconosciuto i limiti di altre piattaforme, come Meta o X, e ha concentrato i propri sforzi di comunicazione e propaganda su Telegram", illustra ancora Emerson Brooking. "Uno dei maggiori fronti su cui Israele ha fallito, e che ha contribuito a scatenare il panico nella società israeliana, è stata la disinformazione nelle prime 72 ore" ha [raccontato](#) a Wired il reporter esperto di tecnologia del quotidiano Haaretz, Omer Benjakob.

Se il pubblico ideale dei video di Hamas è stato, almeno in gran parte, il popolo, le "Forze di Difesa Israeliane (IDF) si sono rivolte in primis alle élite politiche occidentali per ottenere supporto", spiega Brooking. Inoltre, anche nel caso di attori istituzionali israeliani non è mancato l'utilizzo di piattaforme e strategie per diffondere immagini scioccanti, con l'obiettivo di ottenere supporto dal basso all'attacco militare contro la Striscia di Gaza.

"La propaganda russa prima e durante la guerra in Ucraina ha attaccato le piattaforme occidentali come si attacca uno spazio nemico" - dice Brooking. "Questo non è avvenuto nel caso israeliano. Israele, infatti, si è rivolto all'opinione pubblica occidentale ponendosi come alleato contro una minaccia comune". Una dinamica simile è stata osservata in Ucraina. Alcuni esperti hanno [analizzato](#) l'uso dei social da parte degli account ufficiali ucraini, descrivendolo come un esempio di diplomazia

digitale, efficace a diffondere la narrazione della resistenza contro l'invasione.

I doppi standard dei social

I social media, in quanto aziende, non vengono solo usati dalle parti in campo, ma sono anche parti attive nell'opera di propaganda. Lo fanno attraverso le policy di moderazione dei contenuti: decidendo cosa entra nel discorso pubblico e cosa no. "Queste aziende amano il termine piattaforma perché possono sostenere che stanno solo dando uno spazio alle persone per pubblicare i loro messaggi, ma non è mai stato vero. Il fondamento della libertà di espressione su Internet negli Stati Uniti è nella Sezione 230 (un comma del Communications Decency Act che risale al 1996, ndr) che permette a ciascun social media di regolare i contenuti in modo indipendente", conclude Brookings.

Durante i primi mesi del conflitto in Ucraina ha fatto molto discutere la [decisione](#) di Meta di non proibire forme di hate speech (discorsi d'odio) contro i soldati russi. "A seguito dell'invasione russa dell'Ucraina, abbiamo temporaneamente concesso un'autorizzazione a forme di espressione politica che normalmente violerebbero le nostre regole, come morte agli invasori russi", hanno fatto sapere ai media i rappresentanti dell'azienda.

Alcune organizzazioni per i diritti umani (tra cui Access Now e la Electronic Frontier Foundation, specializzate in diritti digitali) hanno [evidenziato](#) come il comportamento di Meta in Ucraina sia stato diverso rispetto ad altre zone del mondo. "Con questa dichiarazione (una dichiarazione congiunta firmata da 31 organizzazioni, ndr), abbiamo voluto esprimere solidarietà alla società civile ucraina, spingendo al contempo i social a fare di meglio in tutto il mondo", ha dichiarato Dia Kayyali, dell'Advocacy per Mnemonic, una ong che si occupa di archiviare e investigare le informazioni digitali che documentano le

violazioni dei diritti umani e i crimini internazionali. "Ucraina, Yemen, India, Sri Lanka, Myanmar, Siria, Sudan: l'elenco dei luoghi in cui le piattaforme devono imparare dai loro fallimenti ed essere pronte a investire nei diritti umani è piuttosto lungo". Alcuni attivisti hanno [parlato](#) di doppi standard, e di allineamento delle grandi piattaforme con le priorità politiche occidentali. Anche se le cose dal punto di vista della società civile ucraina sembrano più sfumate: "Come gli attivisti di molte altre zone di conflitto, la società civile ucraina ha cercato di convincere le piattaforme a prendere sul serio le loro preoccupazioni dopo l'invasione della Russia nel 2014. Solo dopo la pressione dei media e l'interesse degli Stati Uniti e dei Paesi dell'Europa occidentale, le piattaforme hanno iniziato ad agire", ha proseguito Kayyali, parlando con The Intercept.

Tornando al conflitto a Gaza del 2023, secondo un' [analisi](#) dell'organizzazione Eko, una serie di video, provenienti da canali ufficiali (tra cui quello dell'IDF), sono stati pubblicati su YouTube, nonostante violino le policy di moderazione della piattaforma sui contenuti violenti. "La nostra ricerca evidenzia che YouTube sta traendo profitto dalla strategia che lo Stato israeliano sta sponsorizzando per plasmare l'opinione pubblica in modo da sostenere gli attacchi militari che stanno uccidendo migliaia di civili innocenti, ignorando deliberatamente le proprie politiche sui contenuti violenti o espliciti", ha detto a [Wired](#) Flora Rebello Arduini, coordinatrice della campagna.

Secondo alcune Ong, Meta ha [sistematicamente silenziato](#) le voci dei palestinesi: sono stati sospesi degli account, rimossi dei contenuti (anche creati da giornalisti, come quello della corrispondente dalla Cisgiordania di Mondoweiss, Leila Waran), casi di "shadow banning" (un termine che indica una riduzione significativa della visibilità dei post, delle storie o dell'account di un individuo senza alcuna notifica), e

persino gravi errori, come quello in cui Instagram ha [inserito](#) la traduzione “terrorista” nella bio di un utente palestinese. In questo ha un impatto anche la disparità linguistica. Spiega Emerson Brooking: “La moderazione dei contenuti, in particolare in lingue come l'arabo, può avere un impatto significativo sul modo in cui sono raccontati i conflitti. I pregiudizi storici influenzano la maniera in cui i contenuti arabi vengono moderati rispetto ad altre lingue: le policy dei social sono radicate proprio nelle politiche anti-terrorismo degli Stati Uniti, si focalizzano quindi sull'analisi delle minacce. Un contenuto arabo innocuo può essere erroneamente segnalato più spesso rispetto a uno in inglese o in un'altra lingua”.

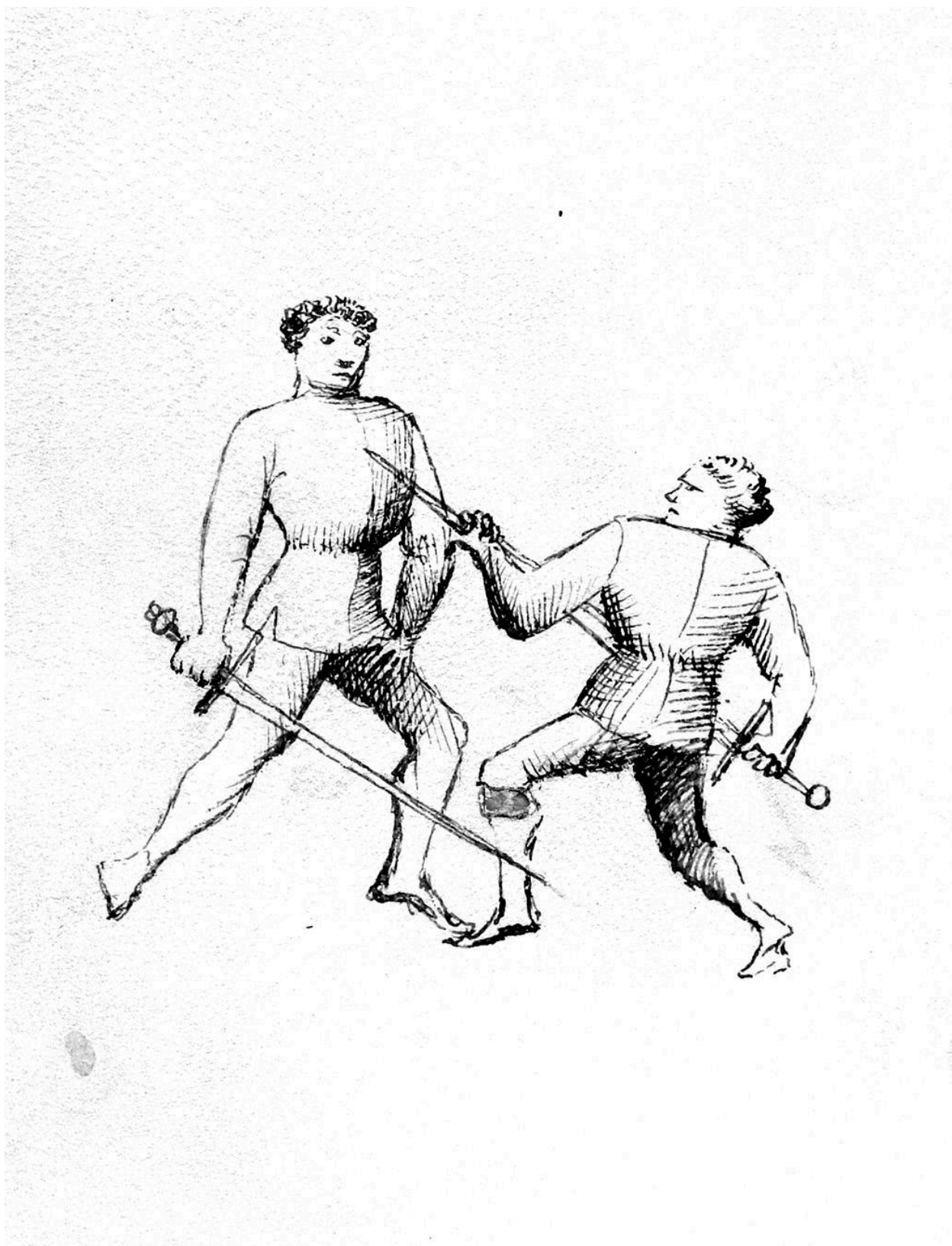
Anche i meccanismi per permettere agli utenti di fare appello contro la cancellazione arbitraria di un contenuto non sembrano funzionare. Un'[inchiesta](#) di The Markup ha rivelato che Instagram eliminava i commenti sotto i post relativi al conflitto segnalandoli come spam. Una volta che un commento veniva eliminato non sempre agli utenti era data la possibilità di richiedere una revisione. In alcuni casi compariva un'opzione per far sapere a Meta che era stato commesso un errore, ma non c'era alcun modo di sapere se una verifica fosse in corso.

Il rapporto con i governi

Le scelte politiche delle piattaforme sono anche dettate dalla loro permeabilità alle richieste dei governi di tutto il mondo. Secondo Emerson Brooking, oggi la tendenza è quella di una maggiore interferenza dei poteri pubblici nella moderazione. È il caso di Israele: già nel 2021, Human Rights Watch [sosteneva](#) che la Cyber Unit del Governo israeliano avesse un rapporto privilegiato con alcune piattaforme. “Invece di seguire l'iter legale, che prevede un'ordinanza del tribunale per rimuovere i contenuti online, la Cyber Unit si rivolge direttamente alle piattaforme. Un rapporto del 2018 dell'ufficio del Procuratore di Stato israeliano rileva un tasso di conformità

estremamente elevato a queste richieste, pari al 90% su tutte le piattaforme”, si legge in un report dell’organizzazione.

Per quanto riguarda X, il [disinvestimento](#) di Musk sui servizi di trust and safety (ovvero tutte quelle [figure tecniche, legali o operative](#) che si occupano di stilare e applicare le policy di sicurezza delle piattaforme) ha reso il social ancora più malleabile alle richieste dei governi. “Avendo tagliato anche sui servizi legali, è molto più facile che le aziende chinino la testa di fronte alle richieste dei governi”, conclude Brookings.



MASTER & COMMANDER: LA BATTAGLIA DELLE NAVI FANTASMA

Dalla guerra in Ucraina al Mar Rosso anche le navi devono nascondersi, falsificare la propria posizione o mandare messaggi. Il tutto grazie a un sistema di tracciamento marittimo che ha molte vulnerabilità.

di Eleonora Zocca

Guerra e Pirati

Negli ultimi mesi il commercio marittimo è stato stravolto dagli attacchi contro le navi del mar Rosso da parte degli houthi, la minoranza sciita che controlla gran parte dello Yemen. In solidarietà con il popolo palestinese, i pirati houthi hanno preso di mira le imbarcazioni israeliane e quelle dei paesi alleati dirottando parte del commercio marittimo sulla ben più lunga e costosa tratta che circumnaviga il Capo di Buona Speranza.

Chi, invece, ha continuato ad attraversare il Canale di Suez ha provato come poteva a difendersi e a prevenire eventuali attacchi utilizzando in diversi modi l'Automated Identification System (AIS), cioè dei messaggi inviati attraverso il sistema di tracciamento marittimo che funziona grazie alle onde radio. Qualche esempio: “norelationtoisrael” (nessuna relazione con Israele), “nocontactIsrael” (nessun contatto con Israele) e “allchinesecrew” (tutto l'equipaggio è cinese). Una pratica, rileva Spire Global, che è aumentata in modo netto soprattutto da metà gennaio in poi.

L'AIS è un protocollo internazionale introdotto dall'Organizzazione internazionale marittima che, dal 2004, è obbligatorio per tutte le imbarcazioni con passeggeri e per le navi cargo sopra le 300 tonnellate. Come spiega a Guerre di Rete Marco Balduzzi, responsabile tecnico della società di sicurezza informatica Trend Micro, "l'AIS è un sistema che viene utilizzato sia per monitorare le barche sia per permettere alle barche stesse di apprendere i rischi oggettivi a cui vanno incontro, come la conformazione del fondale nelle aree circostanti o l'interdizione di alcune zone specifiche. È uno standard internazionale e, in quanto tale, funziona nello stesso modo indipendentemente dalla posizione in cui ti trovi e dal modello di imbarcazione".

Oltre a inviare messaggi radio per manifestare la propria estraneità allo Stato di Israele, le navi in transito nel Mar Rosso spariscono dai radar per rendersi più difficilmente rintracciabili dagli houthi. In gergo tecnico si dice going dark.

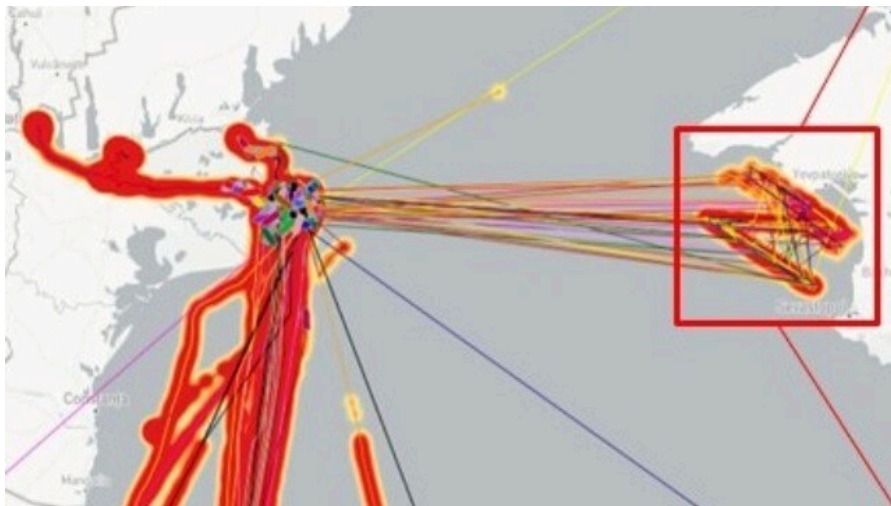
Le vulnerabilità dell'AIS

"All'epoca, l'AIS fu concepito e sviluppato in maniera molto semplice in modo tale che il dispositivo che deve implementarlo, ovvero il transponder, fosse altrettanto semplice ed economico. Nella sua semplicità, questo bellissimo protocollo è soggetto a una serie di vulnerabilità - spiega sempre Balduzzi - perché si può prendere il segnale radio e modificarlo. Quando un messaggio di questo tipo viene falsificato, si parla di spoofing".

Le aree interessate da conflitti o da contese territoriali sono quelle in cui si registrano più episodi di questo tipo. Se ne sono osservati diversi dall'inizio dell'invasione dell'Ucraina: tra giugno e luglio del 2021, ad esempio, [sono state falsificate](#) le posizioni di tre navi della NATO al largo della Crimea; il caso più eclatante rimane però quello in cui le

posizioni AIS di decine di navi mercantili sono andate a formare un enorme Z di fronte alla città di Sebastopoli, nel Mar Nero.

La Z è il simbolo usato dalla propaganda russa che sul campo di battaglia contraddistingue anche i mezzi militari russi. Come ha evidenziato Geolcollect, una società di intelligence inglese che raccoglie dati geospaziali, la lettera ha iniziato a prendere forma il 14 maggio 2023 per essere completata tra il 19 e il 21 dello stesso mese. Il 22 maggio, Putin ha dichiarato la vittoria sulle truppe ucraine a Bakhmut e la presa della città.



Le posizioni AIS di decine di navi vengono modificate per formare un enorme Z nel Mar Nero. Fonte: Geolcollect

Modificare o falsificare le informazioni che passano attraverso le onde radio ad alta frequenza dell'AIS è utile anche per eludere i controlli delle autorità internazionali e intraprendere affari commerciali con paesi soggetti a sanzioni. È il caso della nave Kingsway che per quattro anni, dal 2017 al 2021, ha sfruttato le vulnerabilità del protocollo AIS per navigare indisturbata nel Mar Cinese Meridionale e trafficare petrolio greggio con la Corea del Nord. Grazie allo spoofing, la Kingsway ha ripetutamente modificato il numero di identificazione, il nome, la bandiera e la propria posizione AIS.

O ancora: nel 2023 cinquanta petroliere sono apparse in transito verso l'oceano Atlantico attraverso il Capo di Buona Speranza. Tuttavia, Spire Maritime ha scoperto che queste navi in realtà stavano entrando nella Zona Economica Esclusiva (ZEE) del Venezuela dove con ogni probabilità hanno imbarcato petrolio venezuelano in violazione alle sanzioni internazionali. Queste navi hanno poi fatto ritorno nei porti in Cina e in Malaysia. Agli occhi di chi potenzialmente avesse seguito il tracciato AIS sarebbe apparso tutto a norma di legge.

Le modalità di attacco

Le altre modalità di attacco sono l'hijacking e la disruption. L'hijacking è analogo allo spoofing, con la differenza che se lo spoofing serve a falsificare i dati AIS della propria nave, l'hijacking interviene su quella di altri. Disruption, infine, è un tipo di attacco in cui si prende il controllo delle comunicazioni riservate alle autorità portuali: messaggi, quindi, che generalmente non possono essere generati dai transponder delle normali imbarcazioni. Potenzialmente si potrebbe lanciare un segnale in cui viene comunicato a tutte le navi a 50 chilometri di raggio da un punto specifico di cambiare frequenza: "A quel punto le barche vanno ad operare a una frequenza sbagliata e fai saltare il sistema - spiega Balduzzi -: è un terremoto. Gli effetti sono simili allo jamming, ovvero quando crei un'onda radio talmente potente da far confusione e impedire a tutti di ascoltarti".

Il problema fondamentale dell'AIS è che da sempre è rimasto uguale a se stesso, mentre le capacità tecnologiche per sfruttare le vulnerabilità sono diventate più facilmente accessibili. Esistono dei tentativi di mettere in sicurezza il protocollo sviluppando una versione AIS crittografata, ma una sua implementazione comporterebbe la sostituzione di tutti i transponder installati sulle imbarcazioni.

Il momento spartiacque per la sicurezza marittima globale è stato il 2021, quando la società Windward analizzò il primo caso di manipolazione del sistema satellitare di navigazione di una barca al largo delle Isole dei Caraibi. [Come spiegano](#) gli analisti sul sito, la scoperta è stata decisiva per comprendere che i cosiddetti attori malevoli hanno acquisito le tecnologie e le conoscenze rispetto a una serie di attacchi propri della guerra tecnologica che si pensava fossero in mano solamente agli Stati.

La nave sotto esame era una petroliera di nome BERLINA che, oltre a riportare un comportamento alquanto anomalo, era riuscita in soli due minuti a eseguire una rotazione di 180°. Una manovra impossibile per una nave di quasi 300 metri. A questo punto si cercarono tracciati simili in altre imbarcazioni e si scoprirono altre dieci petroliere al largo delle isole dei Caraibi che seguivano uno schema praticamente uguale.



La rotta anomala della nave BERLINA. Fonte: Windward

Tra gli studi di Marco Balduzzi c'è quello di aver dimostrato come il sistema di sicurezza marittimo sia fallace anche per quanto riguarda gli AIS provider. Siti come VesselFinder o MarineTraffic raccolgono in tempo reale i dati AIS inviati dalle navi alle torri portuali più vicine che a loro volta li immettono nella rete internet.

Questo tipo di servizio è consultabile nella sua versione gratuita da chiunque, ma viene utilizzato soprattutto da grandi attori come aziende di e-commerce o società di intelligence che devono avere accesso a informazioni precise rispetto al percorso eseguito dalle navi che trasportano merci. Già nel 2013, Balduzzi fu in grado di far apparire la nave battente bandiera americana Eleanor Gordon nel pieno centro della città di Dallas, in Texas: “È chiaro che se non c'è più sicurezza delle informazioni che vengono condivise e vendute il sistema non ha senso di esistere”.

Negli ultimi anni, società come la già citata Windward o la HackEye 360 hanno iniziato ad utilizzare l'intelligenza artificiale per maneggiare enormi quantità di dati e sviluppare algoritmi in grado di individuare tracciati AIS inusuali. Se una nave è sospettata di spoofing, il suo segnale AIS viene messo a confronto con le immagini satellitari o il rilevamento delle radiofrequenze.

È la metodologia usata da Bellingcat per analizzare l'area intorno al porto di Sebastopoli, nella Crimea occupata dai russi. Stando ai servizi di monitoraggio marittimo, negli ultimi anni il principale terminal cerealicolo è rimasto estremamente silenzioso. Un quadro che viene contraddetto dalle immagini satellitari raccolte dalla testata giornalistica. Bellingcat ha individuato almeno 148 giorni nel primo anno di guerra russa in Ucraina in cui diverse barche erano presenti nel terminal di Avlita.

Dal contrabbando di petrolio alle azioni politiche e militari

Secondo Windward, dal 2021 al 2023 si sono registrati più di 600 casi di manomissione della posizione satellitare marittima. Più della metà (56%) sarebbe avvenuta nel Golfo Persico vicino l'Iran. Nella maggioranza dei casi vengono usate bandiere di comodo come quella di Panama (31%), Liberia (11%) e Cameroon (8%). Lo scopo è quasi sempre il contrabbando di petrolio.

Il rischio maggiore rimane, però, quello dello spoofing operato dagli stati. [Come spiega](#) Joshua Tallis del Center for Naval Analyses (CNA) a Irregular Warfare, progetto editoriale finanziato in parte dall'Università di Princeton e specializzato in temi di sicurezza militare, per paesi come Russia, Cina e Iran falsificare la posizione delle proprie navi è un'azione politica utilizzata per rafforzare i propri confini marittimi: "Aiuta a promuovere una narrazione che può fungere da pretesto perfetto per far scoppiare un incidente diplomatico o per giustificare azioni belliche di aggressione".

AUTORI & CURATORI

Raffaele Angius. Giornalista freelance. Si occupa di diritti digitali, cybercrimine, whistleblowing. Scrive per Wired Italia e IrpiMedia. Ha cofondato Indip, la prima testata online investigativa in Sardegna.

Irene Doda. Giornalista freelance che si occupa di lavoro, questioni di genere e tecnologia. Ha scritto per Wired Italia, Siamomine, Il Tascabile, e Singola. È autrice del podcast Anticurriculum e consulente di comunicazione per l'organizzazione sindacale StreetNet International.

Carola Frediani. Ha lavorato per anni come giornalista occupandosi di sorveglianza, cybercrimine e cybersicurezza. Oggi è nel team di cybersecurity di una Ong internazionale per i diritti umani. Scrive la newsletter Guerre di Rete e ha cofondato il sito Guerredirete.it.

Sonia Montegiove. Giornalista, informatica, formatrice è coordinatrice di Cybertrials, programma gratuito di formazione e gaming per studentesse delle scuole superiori organizzato dal Laboratorio Nazionale di Cybersecurity del CINI.

Federico Nejrotti. Autore e co-fondatore di Ufficio Furore, studio di progettazione che crea cultura radicale. Appassionato da sempre di internet governance, è stato responsabile delle comunicazioni di cheFare, agenzia per la trasformazione culturale, e capo-redattore dell'edizione italiana di Motherboard, il magazine di scienza e tecnologia di VICE.

Rosita Rijtano. Redattrice de lavialibera, rivista di Libera e Gruppo Abele, per cui gestisce una piattaforma di whistleblowing. Si occupa di cybercrime e diritti umani. Ha lavorato a Repubblica e scritto un libro

sui diritti dei rider (Insubordinati, Edizioni Gruppo Abele), premiato da Oxfam nel 2023.

Eleonora Zocca. Giornalista, collabora principalmente con la Rai. Per Guerre di Rete scrive di sorveglianza tecnologica e sicurezza delle comunicazioni.