Domani

Quotidiano

Data 04-03-2022
Pagina 1+11
Foglio 1 / 3

ANALISI

Come funziona la macchina della disinformazione del Cremlino

ANDREA DANIELE SIGNORELLI a pagina 11

I GIORNALISTI NON ESISTONO

Come funziona la macchina della disinformazione di Putin

ANDREA DANIELE SIGNORELLI
MILANO

Le truppe russe hanno circondato Kiev. Zelensky potrebbe essere fuggito. Non ci stiamo scontrando contro l'esercito e la popolazione ucraina, ma contro mercenari stranieri e battaglioni nazisti». Il 25 febbraio, soltanto un giorno dopo l'invasione della Russia, messaggi di questo tenore hanno iniziato a comparire su dozzine di canali Telegram e su svariati social network, diffusi anche da figure istituzionali russe (tra cui lo speaker della Duma).
Era tutto falso. Non solo Kiev non era stata conquistata, ma il presidente ucraino Zelensky ha subito smentito le voci scendendo in strada, smaRtphone in mano, per riprendersi davanti al palazzo governativo assieme ai suoi più stretti consiglieri e da lì diffondere un messaggio sui social: «Siamo tutti qui. Siamo a Kiev. Il nostro esercito è qui, i nostri cittadini sono qui. Difendiamo l'Ucraina», afferma Zelensky nel video.
Quella contro Zelensky non è stata la prima plateale operazione di disinformazione condotta con l'obiettivo di scoraggiare e confondere la popolazione in una fase critica. Come rivelato dalla Cyberpolice ucraina, già il 15 febbraio molti abitanti della nazione est-europea avevano ricevuto false notizie via sms in cui li si informava che i bancomat avevano smesso di funzionare. In altri casi ancora, sono invece stati impiegati strumenti più avanzati.

I giornalisti inesistenti

Vladimir Bondarenko e Irina Kerimova, per esempio, sono due giornalisti ucraini che utilizzano Facebook per criticare il loro paese e sostenere le ragioni della Russia. Peccato che non esistano: come rivelato il 28 febbraio dal team addetto alla cybersicurezza di Meta (la società che controlla Facebook, Instagram e non solo), le foto dei loro profili social erano state generate con l'utilizzo dell'intelligenza artificiale e gli account appositamente creati per disseminare propaganda su Facebook, Instagram, Twitter, YouTube, Telegram e anche Odnoklassniki e Vk (questi ultimi sono i due social più diffusi in patria).
A occuparsi di questa specifica operazione — di cui i due finti giornalisti sono solo un esempio — sarebbe stato il gruppo hacker noto come Ghostwriter, sostenuto dal Cremlino e che agisce direttamente all'interno dei confini russi.
Sempre secondo il team addetto alla cybersicurezza di Meta, gli hacker di Ghostwriter avrebbero inoltre preso di mira migliaia di utenti social usando il classico trucco del phishing — link fasulli inviati via mail — per sottrarre le loro credenziali, prendere possesso degli account social e poi da qui diffondere disinformazione.
Ma che forma ha, esattamente, questa disinformazione?
Per andare oltre i semplici messaggi diffusi da bot su Telegram, Facebook o Twitter, bisogna osservare i due più noti gruppi mediatici finanziati direttamente dal governo russo, che da anni sono presenti anche in Occidente e che hanno il ruolo preciso di diffondere propaganda favorevole al Cremlino: Russia Today (adesso chiamata soltanto Rt) e Sputnik.
Il primo è un canale televisivo trasmesso in svariate lingue (inglese, francese, tedesco, spagnolo e arabo) e presente in passato anche in Italia su Sky; Sputnik è invece un'agenzia di stampa precedentemente nota come "Voice of Russia". Sky spiega, attraverso il suo ufficio stampa, che «agisce nel rispetto delle decisioni dell'Unione europea e, più in generale, del quadro giuridico europeo di riferimento, pertanto i canali russi non sono più disponibili nella lista automatica dei canali. È comunque possibile ricevere i canali russi *on air* sui decoder Sky attraverso una sintonizzazione manuale da parte dei clienti».

La disinformazione in Italia

Il sito di Sputnik ha anche una versione in italiano, dove, tra notizie più o meno affidabili, spuntano anche contenuti che mostrano tutta la loro natura propagandistica. Un articolo dal titolo: *Ucraina: una marionetta nelle mani dell'occidente* si presenta come se fosse un pezzo d'opinione, ma si rivela invece una semplice vignetta satirica seguita da un brevissimo contenuto che riporta solo un paio di dichiarazioni.
Finti articoli, insomma, che sembrano essere progettati quasi esclusivamente per la diffusione social, dove la fruizione di questo genere di contenuti si limita spesso all'immagine e al titolo.
È una strategia che funziona. Come mostra in un'analisi la testata specializzata NiemanLab, in Germania la pagina Facebook di Rt ha un tasso di engagement (like, commenti, condivisioni) superiore a quello di Der Spiegel; nel Regno Unito è molto al di sotto della BBC, ma se la gioca con il Guardian ed è davanti al Financial Times; in Francia si trova al momento poco sotto Le Monde, che in passato era riuscito a superare. Tutto ciò, però, descrive soltanto la viralità di questi contenuti. La percentuale di persone online che hanno invece visto un vero e proprio articolo di Sputnik o del sito di Rt è molto inferiore: lo 0,6 per cento in Gran Bretagna (contro il 43 per cento sia del Guardian, sia della BBC), il 3 per cento in Germania (contro il 14 per cento di ARD.de, il sito della televisione pubblica), il 2 per cento in Francia (contro il 14 per cento di Le Monde).
«Rt è una fonte di news che ben poche persone cercano attivamente, ma che

sa quali tasti premere per avere successo su Facebook», spiega il NiemanLab. «È quello che negli ultimi decenni abbiamo visto spesso avvenire con i siti che spingono la disinformazione, le teorie del complotto e i contenuti relativi alla "culture-war"». Da segnalare come Rt e Sputnik stiano venendo messe al bando nella Ue e si stia procedendo alla chiusura e penalizzazione dei loro canali Facebook e YouTube.

Gli attacchi informatici

Se tutto ciò ci aiuta ad avere un'idea di quanto il Cremlino — e non solo, ovviamente — investa direttamente nella macchina della disinformazione e della propaganda, non va però dimenticato quanto la Russia sia una nazione nota principalmente per la sua prolifica attività negli attacchi informatici. Attività che in questa fase critica si sono rese evidenti soprattutto prima dell'invasione. Il 15 e il 16 febbraio, per esempio, molti siti bancari e governativi ucraini hanno smesso di funzionare a causa degli attacchi lanciati dalla Russia, mentre 150mila soldati si ammassavano al confine in vista dell'invasione.

Negli stessi giorni, un report dei servizi segreti statunitensi segnalava come gli hacker russi al servizio del governo avessero da tempo penetrato in profondità le reti informatiche ucraine collegate all'esercito, ai trasporti e al settore energetico, per raccogliere informazioni e mettersi nelle condizioni di sabotare questi sistemi qualora ve ne fosse la necessità.

È qualcosa che la Russia ha ripetutamente fatto dal 2014 a oggi, causando blackout, paralizzando l'attività degli ospedali, bloccando le operazioni delle agenzie governative e altro ancora. A occuparsi di questo tipo di azioni non sono però collettivi hacker volontari o semplicemente finanziati dal Cremlino: «Il GRU, il servizio informazioni delle forze armate russe, può essere facilmente descritto come il soggetto più spregiudicato, sfrontato e pericoloso nelle sue azioni di hacking», ha spiegato a Slate Andy Greenberg, autore di un saggio dedicato alla cyberwar di matrice russa.

«Le due unità più attive di cui io sia a conoscenza sono l'Unità 16156, anche nota come Fancy Bear e responsabile dell'attacco al Partito democratico durante le elezioni del 2016, e l'Unità 74455, anche nota come Voodoo Bear. I membri di questi gruppi hacker indossano l'uniforme militare e siedono in un edificio governativo». Come spiega sempre Greenberg, in una fase di guerra vera e propria come quella attuale questo genere di attività informatiche passa però in secondo piano: «I cyberattacchi sono stati usati per preparare il campo di battaglia, creando un senso di confusione e spaventando le persone, mentre l'Ucraina cercava di capire che cosa stesse succedendo. Con l'inizio dell'invasione, questo genere di attacchi informatici è passato dietro le quinte. Se vuoi causare un blackout in Ucraina, adesso colpisci le centrali elettriche con i missili».

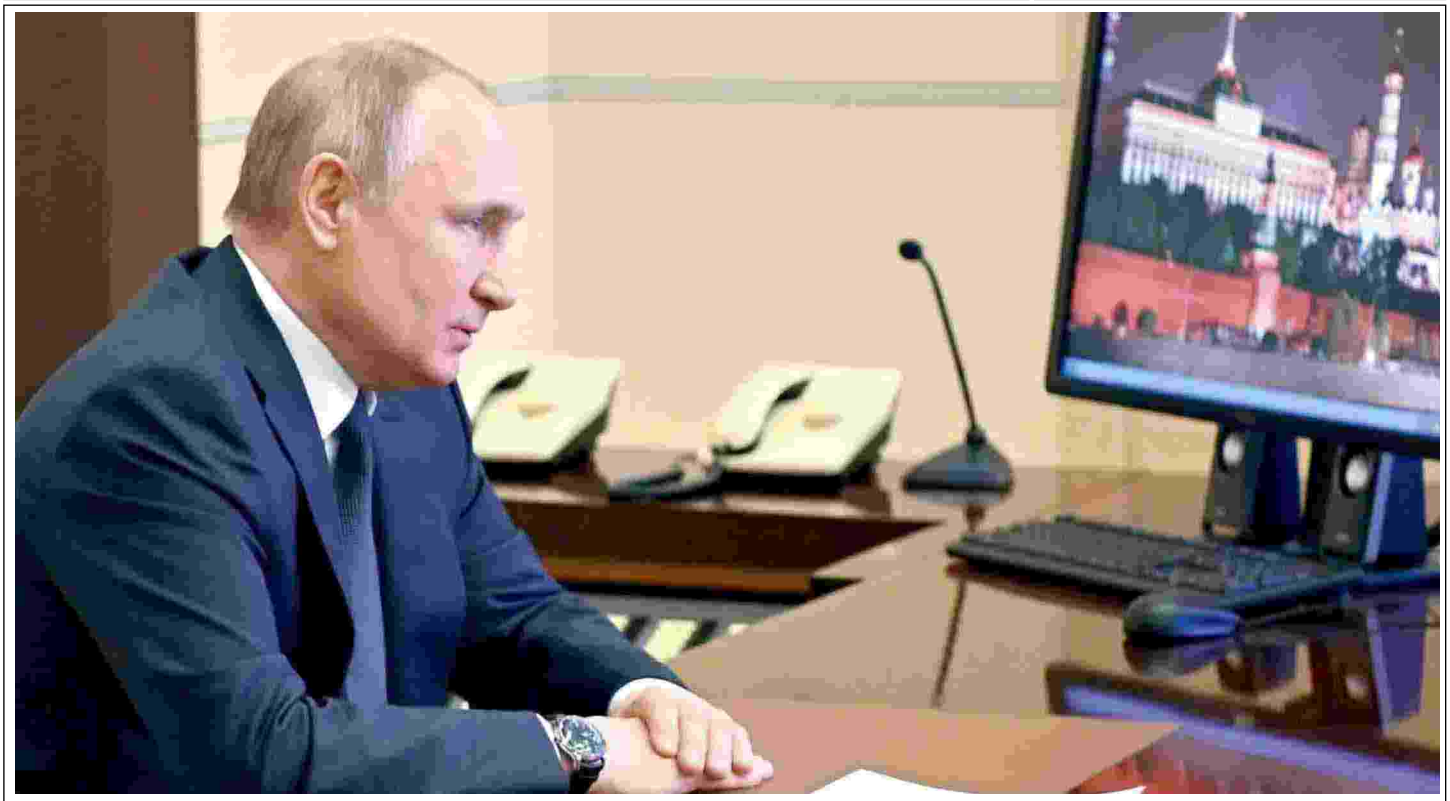
Durante la guerra vera e propria, gli attacchi fisici prendono spesso il posto di quelli informatici. Allo stesso modo, anche la propaganda smette di vivere esclusivamente nel regno digitale ed entra in quello reale: scuole comprese.

Con una nota diffusa online, il ministero dell'Istruzione russa ha spiegato come il 3 marzo alle 12 sarebbe stato mostrata una trasmissione tv in tutte le scuole russe per «spiegare agli scolari perché la missione di liberazione in Ucraina è una necessità" e perché "la Nato rappresenti un pericolo per il nostro paese». Anche nell'epoca digitale, la propaganda vecchio stile non passa mai di moda.

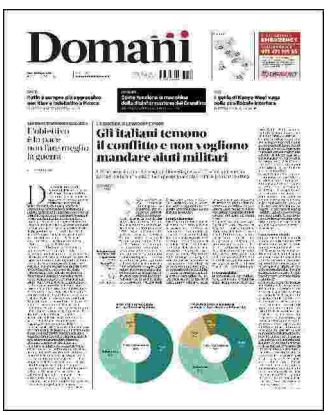
Domani

Quotidiano

Data 04-03-2022
Pagina 1+11
Foglio 3 / 3



In tutte le scuole russe *è stato mostrato un video per «spiegare perché la missione di liberazione in Ucraina è una necessità»*
FOTO AP


Domani

Gli italiani temono il conflitto e non vogliono mandare aiuti militari


Come funziona la macchina della disinformazione di Putin