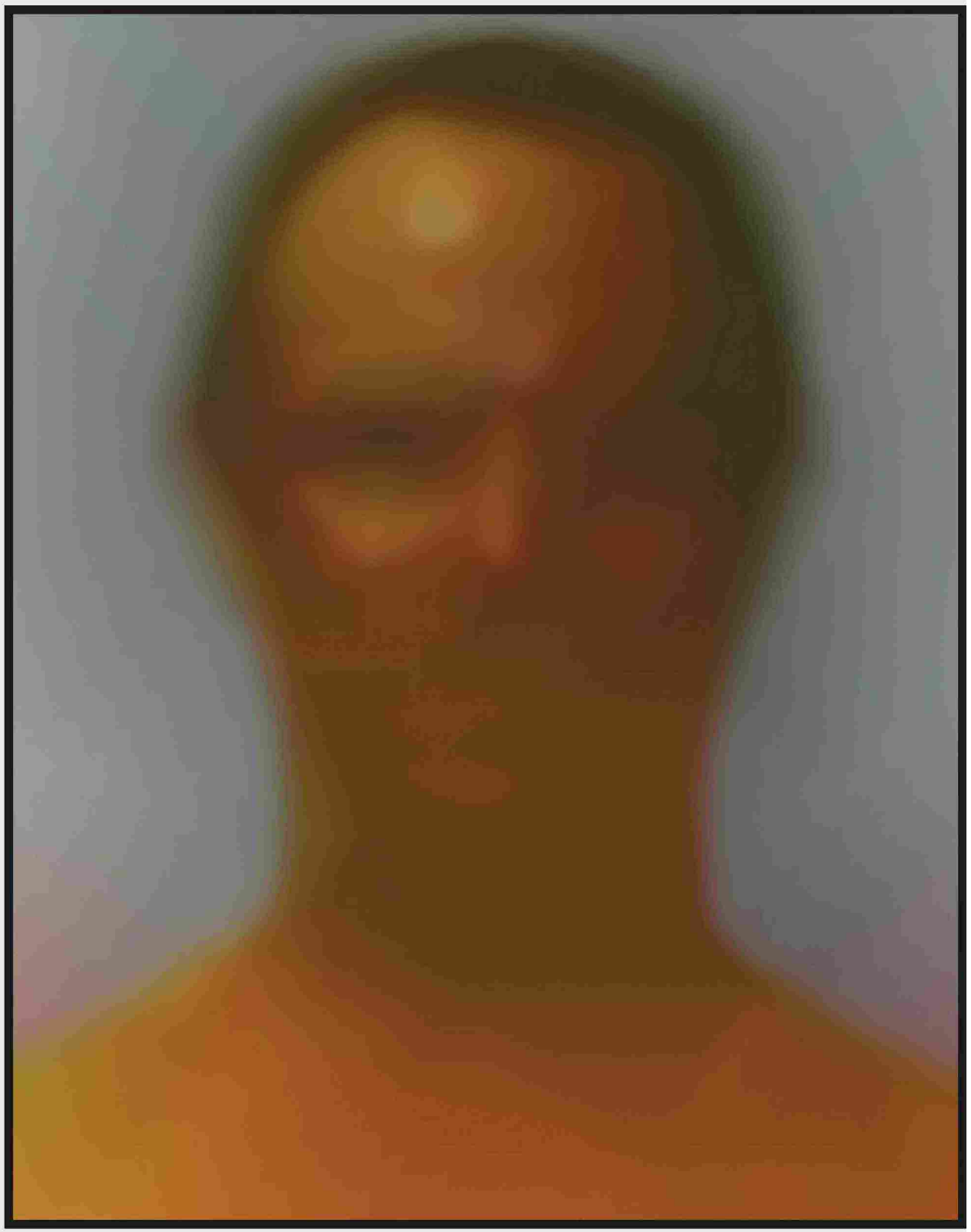
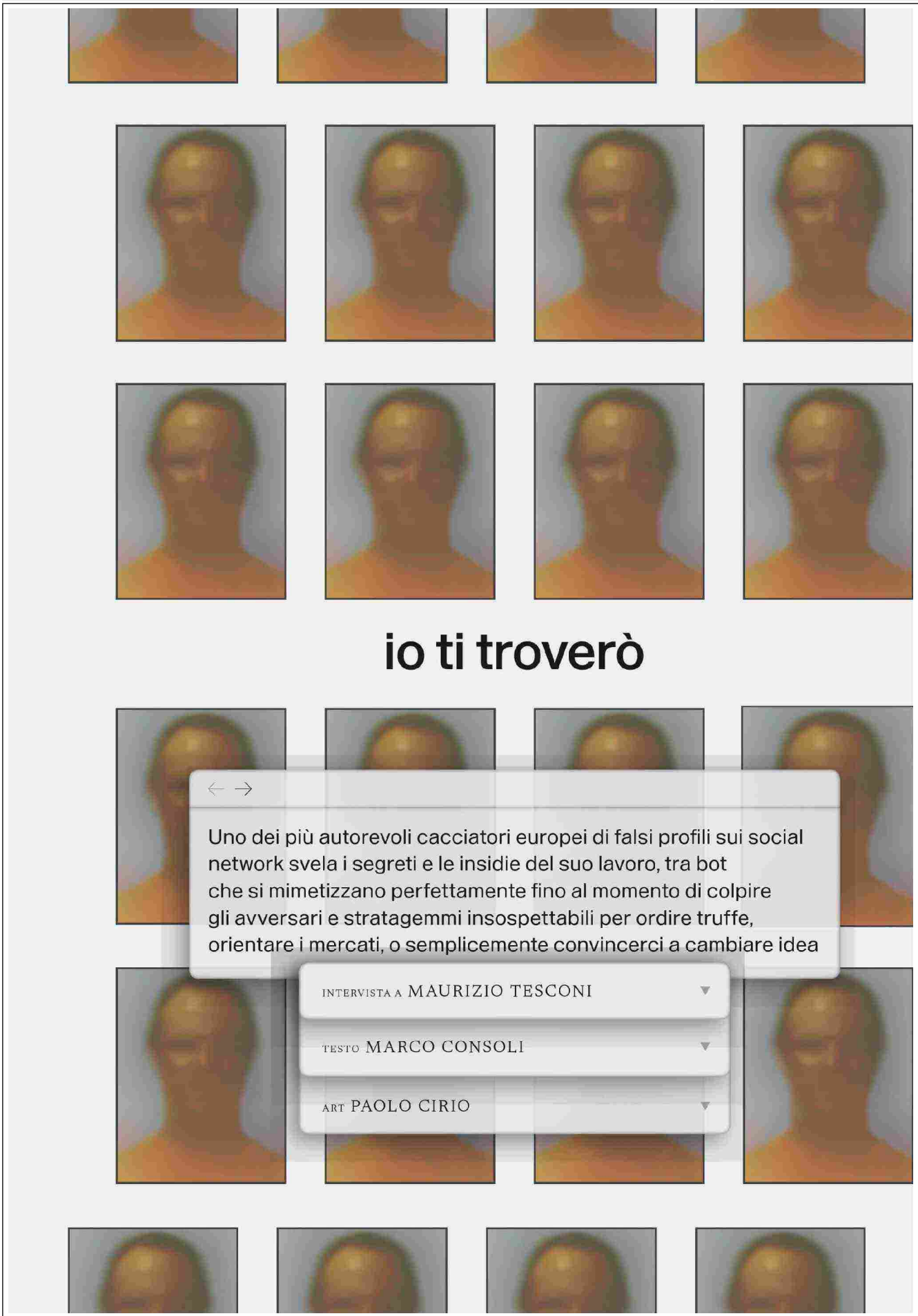
WIRED

Trimestrale

Consiglio Nazionale delle Ricerche

Data 06-2021
Pagina 168/73
Foglio 1 / 6





io ti troverò

Uno dei più autorevoli cacciatori europei di falsi profili sui social network svela i segreti e le insidie del suo lavoro, tra bot che si mimetizzano perfettamente fino al momento di colpire gli avversari e stratagemmi insospettabili per ordire truffe, orientare i mercati, o semplicemente convincerci a cambiare idea

INTERVISTA A MAURIZIO TESCONI

TESTO MARCO CONSOLI

ART PAOLO CIRIO

Sono in mezzo a noi. Pubblicano le foto di una vacanza o di un compleanno, condividono link a notizie, commentano il post di un personaggio famoso. Vedi i loro occhi verdi e sorrisi luminosi sui profili social e li immagini intenti a fare la spesa oppure a dare una carezza ai figli. Solo che non possono farlo, perché sono bot, programmi automatici che fingono di essere umani, si confondono tra la folla e sono pronti a sferrare attacchi coordinati: il sostegno a un politico in difficoltà, la seduzione di teenager sprovveduti, la ricerca online di potenziali vittime di truffe, la manipolazione della Borsa o delle elezioni. Un esercito di agenti dormienti, pronti a operare a comando, come terroristi della rete in attesa del loro 11 settembre.

WIRED
Trimestrale
Consiglio Nazionale delle Ricerche
Data 06-2021
Pagina 168/73
Foglio 4 / 6

«Ne esistono alcuni talmente convincenti che hanno amici veri, persone in carne e ossa ignare di seguire una persona fatta di bit», spiega Maurizio Tesconi, 46 anni, uno dei più noti cacciatori di bot, responsabile del Cyber Intelligence Lab dell'Istituto di informatica e telematica del Cnr di Pisa. Qui, il suo team di 12 ingegneri scandaglia la rete alla ricerca di prove, acquista bot per studiarne il codice di programmazione, crea nuovi esemplari in laboratorio per anticipare le mosse degli hacker, proprio come certi scienziati manipolano i virus per trovare le cure prima che si diffondano. E appronta tecniche innovative, per esempio per afferrarne il dna e paragonarlo a quello degli esseri umani. «Abbiamo sequenziato le azioni degli utenti reali su Twitter attribuendo una lettera a ciascuna: il tweet, i retweet, il reply e così via. In questo modo abbiamo creato una stringa di caratteri che risale fino ai 3200 tweet precedenti e li identifica. Poi, abbiamo preso un algoritmo usato dai bioinformatici per confrontare queste sequenze con quelle di presunti bot, e individuare discrepanze nel loro modo di agire», spiega Tesconi, che all'argomento ha dedicato anche un libro, scritto con Viola Bachini: *Fake People. Storie di social bot e bugiardi digitali*.

La rete è ormai invasa da bot (la parola è l'abbreviazione di robot): secondo un rapporto dell'azienda di sicurezza Kount generano il 40 per cento del traffico su internet. Certo, la maggior parte esegue istruzioni utili: per esempio, sono bot i *web crawler* lanciati da Google per indicizzare i siti e lo sono anche quelli che automatizzano la ricezione di feed di notizie. Da un po' di anni, però, questi programmi un tempo anonimi ci hanno rubato l'identità, trasformandosi in social bot, software che per scopi quasi sempre fraudolenti fingono di essere persone reali. «La prima pubblicazione scientifica su un account automatizzato sui social risale al 2010, anche se è dal 2001 che si parla di attacchi di reti di bot (le cosiddette *botnet, ndr*) nei programmi di messaggistica», dice il cacciatore. «Piattaforme come Twitter, Facebook e Telegram ne permettono la creazione perché vengano usati per scopi utili: per esempio, quello dell'Istituto Nazionale di geofisica e vulcanologia ti avverte ogni volta che c'è un terremoto e ci sono chatbot che servono a ordinare una pizza. Un altro molto utile è Re:scam, a cui puoi indirizzare lo spam in modo che intrattenga una conversazione via email con chi lo produce, facendogli perdere tempo. Il problema, però, sono i malintenzionati».

Quali crimini vengono commessi?

«Per esempio la *sextortion*, il ricatto personale attraverso l'uso di contenuti sessuali privati: un falso profilo di una bella ragazza ti chiede alcune foto nudo e il gioco è fatto. Non è, però, un fenomeno solo maschile: mi ha contattato una vittima che ha raccolto le storie di donne sole avanti negli anni truffate da bei ragazzi che si facevano fare regali. Ma può anche capitare di mettere un annuncio sul web per vendere qualcosa ed essere agganciati su WhatsApp da truffatori».

In questi casi, che cosa c'entrano i bot?

«Vengono usati per scandagliare la rete a caccia di numeri di telefono e avvicinare le persone con profili falsi. Poi altri bot iniziano la conversazione e, quando hanno agganciato la vittima, interviene il truffatore: in questo caso anziché di bot si parla di cyborg, metà uomo e metà macchina».

In quali occasioni, invece, i social bot agiscono da soli?

«Per esempio quando a migliaia di loro viene ordinato di ritwittare il messaggio di un politico per fargli acquisire consenso o per affossarlo con commenti negativi. Questi bot svolgono un'attività di base che li fa sembrare persone, finché il botmaster non ordina l'attacco. Siccome i social media tengono d'occhio queste azioni e spesso bloccano l'account di chi usa i bot, a volte i criminali ritwittano in massa un avversario per farlo bloccare. O, allo stesso scopo, lo inondano di finti follower».

Averne tanti aiuta gli influencer a farsi pagare dalle aziende per parlare dei loro prodotti. Come si comprano e come agiscono questi bot?

«Comprarli è semplicissimo e ci sono addirittura siti che recensiscono quelli che li vendono. I più semplici costano meno, a volte non hanno neanche una foto del profilo, e servono a fare numero, ma vengono individuati presto dai social e cancellati. I più sofisticati sembrano persone reali, svolgono attività normali finché si richiede loro un attacco. Talvolta sono anche profili abbandonati o venduti da utenti in carne e ossa: in Russia si tratta di un mercato florido. Li compri e poi ti viene dato uno script per cambiare i connotati e usarli. Ma costano di più e non vale la pena usarli come follower, semmai per manipolare l'opinione pubblica. Farlo non è così difficile».

WIRED
Trimestrale
Consiglio Nazionale delle Ricerche
Data 06-2021
Pagina 168/73
Foglio 5 / 6

In che senso?

«Una *botnet* ben organizzata può far andare un argomento tra i *trending topic* di Twitter e creare un terreno favorevole per una parte politica, per esempio accendendo il dibattito sull'immigrazione. È stato dimostrato che in Arabia Saudita bastano 200 dollari per farlo. Certo, in un paese come gli Usa, dove gli utenti sono molti di più, sarebbe più difficile e costoso, ma in Italia forse no».

Come sono realizzati i bot?

«All'inizio venivano creati falsi profili rubando foto e testi di utenti dal web. Ma siccome è facile individuare questo tipo di clonazione, oggi si utilizza l'intelligenza artificiale: le immagini vengono generate da algoritmi come quelli del sito thispersondoesnotexist.com, e lo stesso vale per i testi. E poi anche le loro azioni sono sempre più autentiche: per esempio, raramente postano in piena notte, perché non sarebbero credibili. Chi li crea studia i comportamenti umani».

Per bloccare l'ondata di bot malevoli, nessuno ha pensato a interventi legislativi?

«In California è passata una legge per cui se crei un bot devi certificare che quell'account è automatico. Ma il problema delle leggi è che poi su internet mancano i confini, quindi se il reato viene compiuto in un paese privo di regolamentazione, come si fa?»

I bot sono in grado di influenzare veramente le opinioni?

«Si è detto che abbiano avuto un peso nelle elezioni americane del 2016 e in queste settimane stiamo conducendo uno studio su quelle del 2020: analizzando 250 milioni di tweet, abbiamo individuato 87mila utenti "superdiffusori", che hanno prodotto 71 milioni di retweet, e tra questi abbiamo isolato 10 gruppi interessanti, molto coordinati tra di loro, che diffondevano notizie a favore di Donald Trump. Si è discusso se i bot siano poi in grado di cambiare davvero l'orientamento al voto, ma l'unico studio in merito, anche se contestato per il campione esiguo di partecipanti, ha dimostrato il contrario».

Ci sono altri esempi tangibili di queste azioni online sulla realtà?

«I bot oggi dominano la finanza: ci sono software che creano notizie per far crescere l'interesse degli investitori verso determinate aziende, come accaduto nel caso di Cynk Technology, le cui azioni da 10 centesimi sono schizzate a 15 dollari, portandola a valere quattro miliardi e mezzo. Ora i bot vengono usati per attirare utenti su canali Telegram dove si attuano strategie di *pump and dump*: si coordinano acquisti in massa di criptovalute per farne salire il prezzo e poi nel giro di pochi minuti si vende per guadagnare da chi non è al corrente dell'operazione e alla fine perderà soldi».

Qual è l'utilizzo più fantasioso di bot che avete studiato?

«Quello dei laburisti, che per le elezioni nel Regno Unito hanno usato bot su Tinder per impersonare belle ragazze e agganciare potenziali giovani elettori maschi di aree geografiche dominate dai conservatori. Dopo i convenevoli automatici, una persona prendeva possesso del profilo e avviava una conversazione per convincere le vittime a votare a sinistra».

Come si combattono questi falsi profili?

«Gli utenti devono stare attenti a segnali come l'uso stentato dell'italiano, visto che molti attacchi arrivano dall'estero. O al fatto che hanno profili anomali, con pochi post frutto di un copia-incolla. Noi li studiamo attraverso i software, ma mentre prima si cercava di individuarli uno per uno, adesso si analizzano le azioni di gruppo, perché certi comportamenti come un retweet diventano più sospetti se vengono eseguiti insieme da migliaia di agenti».

Può farci un esempio?

«Oltre al loro dna, ora stiamo studiando i meccanismi di sincronizzazione temporale tra i vari account per vedere quanto sono simili tra loro. Siamo molto bravi a individuare la coordinazione ormai, ma è più problematico definire comportamenti inautentici, perché spesso anche le persone vere, spinte da un ideale, agiscono in maniera dannosa o bizzarra».

Qual è la prossima frontiera della ricerca sui bot?

«L'utilizzo di reti neurali antagoniste: si creano artificialmente i falsi per dare la possibilità a un altro sistema di diventare più bravo a individuarli. In pratica, si creano potenziali bot, che magari non esistono ancora, e si insegna ad altri software a riconoscerli. Anticipando le mosse dei malintenzionati».

Alla fine di questa caccia riuscite a risalire ai responsabili?

«È difficile, al massimo risaliamo ai profili falsi, perché ci mancano dati come gli indirizzi IP in possesso dei social e che in Italia può ottenere solo l'autorità giudiziaria. Inoltre, gli hacker che organizzano queste *botnet* sono scaltri e usano sistemi per rimanere anonimi. Però, il contrasto da parte delle piattaforme è aumentato, e così il lavoro dei botmaster diventa più difficile: per creare un bot credibile, per esempio, bisogna associargli una sim, per rispondere a un eventuale sms di controllo qualora la piattaforma chiedesse conferma che si tratta di una persona reale. Tecnicamente si potrebbe creare una *botnet* con milioni di agenti, ma azioni coordinate di troppi utenti destano sospetti. E così è più proficuo creare celle di bot più ristrette e molto organizzate. Agenti dormienti che magari per molto tempo si confondono con le persone normali, per poi un giorno scatenare un attacco mirato».

MAURIZIO TESCONI

Esperto in analisi e individuazione di profili falsi sui social network, è il responsabile del Cyber Intelligence Lab dell'Istituto di informatica e telematica del Cnr. Insegna Cyber Intelligence all'interno del Master in Cyber Security dell'Università di Pisa ed è membro permanente del team del Laboratorio Europeo su Big Data Analytics and Social Mining. Insieme a Viola Bachini ha scritto il libro *Fake Peopie. Storie di social bot e bugiardi digitali* (Codice Edizioni, 2020).