La propaganda computazionale e le interferenze hacker

Arturo Di Corinto

Sommario

Gli hacker e gli attivisti digitali sono entrati a pieno titolo nelle guerre guerreggiate con gli strumenti propri della propaganda digitale, del sabotaggio elettronico, dello spionaggio cibernetico e dell'hacking. Lo fanno con attacchi DDoS, malware, ransomware, ma anche con algoritmi, deepfake, troll e bot. È così che partecipano alla guerra ibrida combattuta tra gli stati.

In tale scenario diversi autori ritengono che le tecniche di manipolazione delle percezioni che sfruttano gli strumenti digitali offerti dal web rientrino a pieno titolo tra gli strumenti della guerra ibrida, in quanto capaci di influenzare la reattività dell'avversario. Si parla a questo proposito di Guerra cognitiva.

Questo vuol dire anche che le campagne informative non si basano più soltanto sui media tradizionali, ma anche sui media digitali, le piattaforme social, i canali della messaggistica diretta.

Tra gli strumenti di queste campagne quelli della propaganda computazionale, usati per modificare il mindset del target, e generare incertezza, sfiducia e dubbio, destano sempre di più le preoccupazioni degli Stati. Il motivo è facile da intuire: laddove l'opinione pubblica è in grado di influenzare le scelte delle parti in guerra, riuscire a manipolarla può modificare le fasi del conflitto.

In questo paper cercheremo di descrivere le tecniche della propaganda computazionale e di come hacker attivisti e hacker di stato possano farne uso. Nell'anno elettorale mondiale che abbiamo davanti, il 2024, infatti, la propaganda computazionale potrebbe rappresentare un rischio per il processo democratico.

Abstract

Hackers and digital activists have fully entered the wars waged with digital propaganda, electronic sabotage, cyber espionage and software hacking tools. DDoS attacks, malware, ransomware, but also algorithms, deepfakes, trolls and bots are their weapons. This is how they participate in the hybrid war fought among States.

In this scenario, it is alleged that the techniques for manipulating perceptions that exploit digital tools are fully included among the weapons of hybrid warfare, as they are capable of influencing the reactivity of the adversary. In this regard we speak of Cognitive War.

This also means that information campaigns are no longer based only on traditional media, but also on digital media, social platforms and direct messaging channels.

Among the tools of these campaigns, those of computational propaganda, used to change the mindset of the target, to generate fear, uncertainty, and doubt, are increasingly arousing the concerns of States. The reason is easy to understand: where public opinion is able to influence the choices of the warring parties, manipulation can change the phases of the conflict.

In this paper we will try to describe the techniques of computational propaganda and how hacker activists and State hackers can use them. Indeed, in the global election year ahead of us, 2024, computational propaganda could represent a risk for the democratic process.

Keywords: Cybersecurity; disinformation; fake news; hacking; hacktivism; persuasion; propaganda computazionale

"According to some authors the impact of disinformation can be split into the following areas: a) Spread (superficial online/offline behaviour towards dis/misinformation), b) Attitude change or reinforcement (e.g. the psychological effects of dis/misinformation on beliefs, cognition), c) Behaviour change (e.g. altering voting behaviour, disengagement from politics and d) Broader societal impact (e.g. reducing institu-tional trust, undermining social cohesion)"[1].

1. Introduzione

Nell'ambiente mediatico attuale la disinformazione viene diffusa attraverso algoritmi di intelligenza artificiale, fake news, troll[2] e fantocci digitali, cioè attraverso i moderni strumenti della propaganda computazionale.

Non è semplice dare una definizione condivisa di cosa sia la propaganda computazionale, ma ogni concettualizzazione che la riguarda tende ad asseverarla come l'influenza esercitata attraverso l'uso di algoritmi e strumenti cibernetici sulla percezione degli individui.

Una definizione operativa, che ha mostrato negli ultimi anni tutto il suo valore euristico, è quella di Wooley e Howard dell'Università di Oxford, secondo cui "La propaganda computazionale è l'uso di algoritmi, automazione e cura umana per

[1] DOI: https://doi.org/ 10.37458/nstf.24.2.5
[2] I troll sono soggetti che disturbano le conversazioni che abbiamo sui social con interventi provocatori. Possono essere automatizzati come bot che ripetono costantemente gli stessi messaggi.

distribuire intenzionalmente informazioni fuorvianti sui social media" (Computational Propaganda Research Project, Working Paper No. 2017.11)[3] .

Per meglio comprendere come questo accada, cominciamo spiegando cos'è la propaganda.

Propaganda è un termine antico che può essere fatto risalire alla creazione dell'Istituto De Propaganda Fide ad opera dei vertici della Chiesa Cattolica Romana nel 1600. La propaganda della fede aveva come obiettivo l'evangelizzazione degli individui e la loro sottomissione all'unico Dio. Come tutte le religioni, anche quella cattolica è basata su narrazioni, e poiché il loro successo dipende generalmente dal numero di individui che cooperano in accordo con queste narrazioni, la loro propagazione è fondamentale.

In tempi moderni, il suo teorico storicamente più influente, Edward L. Bernays, ha descritto la *propaganda* come l'insieme delle azioni necessarie a guidare le masse, per il loro bene (Bernays, 1928)[4]. Bernays, nipote di Sigmund Freud, teorico della mente collettiva e della fabbricazione del consenso, era convinto che l'uomo della strada non avesse opinioni affidabili e che potesse votare per la persona sbagliata o desiderare la cosa sbagliata; quindi, riteneva che dovesse essere guidato dalla propaganda a fare le scelte giuste.

Bernays ha espresso compiutamente questo concetto nel 1928, nel suo libro più famoso, Propaganda. Erano gli anni ruggenti del capitalismo e il coevo consumismo non aveva ancora incontrato la Grande Depressione dei successivi anni '30. Ma si presentò subito un'occasione per guidare le masse e convincere le persone a fare quello che non avrebbero fatto di propria iniziativa: arruolarsi e partecipare alla Seconda guerra mondiale. Già all'epoca il termine divenne sinonimo di propaganda politica.

Vista come qualcosa di negativo, capace di influenzare il libero arbitrio delle persone, ma anche di facilitarne la coesione, la propaganda veicolata dai mass media è stata massicciamente usata nel secolo scorso da regimi dittatoriali - fascismo, nazismo e comunismo -, come pure dai governi democratici, ma ancora oggi il concetto moderno di propaganda ci rimanda alla disseminazione di idee e informazioni che hanno lo scopo di indurre alcuni specifici tipi di scelte o azioni in ambito sociale e politico.

La propaganda, che secondo Bernays doveva essere basata su fatti e informazioni accurate, è stata spesso confusa con la disinformazione, che risulta invece da un miscuglio di elementi veri ed elementi falsi. La propaganda, esplicita, organizzata da attori noti, per creare consenso intorno a un bene da promuovere, è però diversa dalla disinformazione, che può essere concettualizzata come il tentativo occulto di manipolare l'informazione per

[3] Samuel C. Woolley & Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk. 14 pp.
[4] Bernays, E. L. (2020). Propaganda. L'arte di manipolare l'opinione pubblica, a cura di Raffaele Scelsi, Milano, Shake Edizioni 2020; ed. or. Propaganda, 1928, Horace Liveright, New York.

fuorviare il ricevente di una comunicazione. E proprio questo era l'obiettivo della polizia segreta sovietica (GPU), che creò il termine "dezinformatzija", (дезинформация), intesa come "arma tattica".

La parziale sovrapposizione dei due concetti dipende dal fatto che propaganda e disinformazione servono allo stesso scopo, che è quello di usare l'informazione per influenzare le percezioni del ricevente allo scopo di modellarne il comportamento.

Con una sottile differenza: se la persuasione applicata alla propaganda può essere definita come l'innesco di un comportamento non spontaneo, facendo però leva sul ragionamento e gli appelli emotivi, la disinformazione si basa sulla sovversione delle informazioni che gli individui, supposti razionali, usano per agire le loro scelte, anche a dispetto dei propri interessi.

La stessa Unione Europea, mentre considera legittima la propaganda, ha avviato una serie di azioni per contrastare la disinformazione che oggi viaggia in rete in quanto: "informazioni altamente persuasive o fuorvianti create, presentate e diffuse per un guadagno economico o per ingannare intenzionalmente il pubblico, possono causare un danno pubblico. Il danno pubblico include minacce al processo politico democratico e al processo decisionale, nonché al bene pubblico, come la tutela della salute dei cittadini dell'UE, dell'ambiente o della sicurezza."[5]

Le campagne di manipolazione delle percezioni che oggi usano propaganda e disinformazione per seminare dubbio e scontento nella popolazione vengono infatti diffusamente distribuite sui social network principali, Facebook, X, Instagram, Truth, e altri ambienti ingegnerizzati per favorire il coinvolgimento delle persone e la polarizzazione delle opinioni. In aggiunta, propaganda e disinformazione sono diventate un problema cibernetico perché i suoi attori usano strumenti digitali automatizzati e interattivi per colpire le certezze dei bersagli con un esercito di troll, di bot[6] , e facendo largo uso di meme[7] e notizie online fasulle, create ad arte da gruppi di guerriglia digitale che usano anche tecniche di software hacking[8] per manipolare l'informazione e i suoi protagonisti, i cui contenuti viaggiano in misura consistente anche su forum come Reddit, Discord, e 4chan.

[5] Europarlamento, (2021), The impact of disinformation on democratic processes and human rights in the world, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf [aprile 2021]

[6] I bot sono software programmati per sostituire l'intervento umano e svolgere compiti di raccolta, analisi, catalogazione. I bot in grado di fare conversazione, sono detti chatbots.

[7] I meme, unità minime di informazione che si auto-propagano grazie alla loro semplicità. Si tratta spesso di immagini e slogan ad effetto, facile da comprendere e memorizzare. Sono uno strumento di disinformazione.

[8] Hacking è l'insieme dei metodi, tecniche e operazioni volte a conoscere, accedere e modificare un sistema informatico hardware o software.

2. Che cos'è la propaganda computazionale

La propaganda computazionale può essere quindi concettualizzata come veicolo di propaganda e disinformazione da parte di attori singoli e associati, volontari e mercenari, fasulli o reali, che usano le piattaforme digitali, i social network, i social media, per diffondere fake news[9], narrative distorte e contenuti persuasivi. Questi attori fanno un ampio uso di bot, troll, meme e tecniche di hacking per influenzare la percezione del ricevente ed elicitare, in chi vi è esposto, una reazione che sia in accordo con gli interessi dell'attore.

Se l'ambiente digitale è il luogo di elezione della propaganda computazionale, i suoi effetti, tuttavia, vengono amplificati dai media tradizionali - radio, tv, stampa -, che gli fanno eco, e che la posizionano all'interno dell'agenda mediatica, legittimandola. La propaganda diffusa dai media viene successivamente sfruttata dagli attori della propaganda stessa che la rimbalzano nei circuiti mediatici in un loop virtualmente infinito che è spesso all'origine di comportamenti complottisti.

Negli ultimi anni abbiamo visto all'opera soggetti organizzati gestire vaste attività di propaganda e disinformazione, si pensi alle fake news legate alla campagna presidenziale di Trump nel 2016; all'impiego di dark ads[10] e al microtargeting[11] generato dall'uso di app psicometriche come nel caso di Cambridge Analytica[12] oppure alle notizie fasulle dei potenziali effetti della Brexit, fino al dilagare delle false narrative della "fabbrica dei troll" di San Pietroburgo[13].

In tempi recenti il caso forse più famoso di inquinamento dell'informazione è stato quello noto come "Pizzagate" in cui è rimasta coinvolta la democratica Hillary Clinton che contendeva al repubblicano Donald Trump lo scranno della Casa Bianca. La fake news che all'epoca ottenne sui social più visibilità delle smentite giornalistiche la dipingeva a capo di un'organizzazione satanista che aveva creato un circuito di abusi pedofili nello scantinato di una pizzeria. Le indagini

[9] Le fake news sono notizie non documentate né verificabili. Questa forma di pseudo-informazione agisce online innescando i bias cognitivi noti come il pregiudizio di conferma, l'echo chamber e l'effetto bandwagon.
[10] I dark ads sono post sponsorizzati dagli inserzionisti verso specifiche porzioni di popolazione, individuate secondo dei parametri selezionabili.
[11] Il microtargeting è l'utilizzo dei dati di profilazione per personalizzare messaggi pubblicitari verso singoli individui, in base all'identificazione delle vulnerabilità personali dei destinatari. Viene utilizzato per promuovere un prodotto o un candidato politico.
[12] Wilye, C. (2019). Il Mercato del consenso: come ho creato e poi distrutto Cambridge Analytica, Milano, Longanesi; ed. or. Mindf*ck: Inside Cambridge Analytica's Plot to Break the World, London, Profile Books, 2019.
[13] La "Fabbrica dei troll" russi, è l'epiteto giornalistico dell'Internet Research Agency, struttura finanziata da Evgenij Viktorovič Prigožin, imprenditore, politico e comandante mercenario russo, amico del presidente russo Vladimir Putin, con il compito di sviluppare contenuti di propaganda a favore del governo di Mosca.

successive mostrarono che non solo non esisteva il circolo pedofilo, ma neanche lo scantinato (Harari, 2021[14] ; Bianchi, 2021[15]).

Se le fake news sono state uno strumento di competizione elettorale, anche i "bot" lo sono stati a più riprese. Su Facebook, Twitter, Instagram, molti profili fasulli sono governati da bot in grado di intavolare una banale discussione in chat (i chatbots), e che producono una notevole mole di messaggi. Spesso si tratta di esche sessuali o di truffatori che offrono denaro in prestito o altri servizi a pagamento, ma tra questi primeggiano i "political bots", in considerazione del fatto che sono le organizzazioni politiche quelle più propense a investire fondi consistenti nella propaganda computazionale.

Ad esempio, nel 2017 una serie di articoli[16] rivelò che due attiviste laburiste avevano commissionato la creazione di un bot, cioè di un sistema automatico di risposta su Tinder, nota app per incontri sentimentali. Programmato per specifiche fasce di età e di interessi, il suo scopo era quello di suggerire il voto per i laburisti a ogni potenziale anima gemella incontrata. Un altro esempio è quello dei bot che hanno rilanciato migliaia di volte l'hashtag #ReasonsToLeaveEu durante il referendum per la Brexit. Questi "amplification bots", secondo i ricercatori italiani della Fondazione Bruno Kessler, sono stati usati anche durante le elezioni politiche italiane del 2018 per "dopare" la diffusione dei messaggi della Lega e del suo leader, Matteo Salvini (Bachini & Tesconi, 2020)[17].

Similmente, gli attacchi nei confronti del Presidente della Repubblica italiana Sergio Mattarella sono da attribuire alla stessa logica. All'epoca, la guerra di hashtag sulla formazione del nuovo governo italiano nel 2018 ci ha mostrato un web istericamente diviso tra i sostenitori del presidente Mattarella e i suoi detrattori con due opposti hashtag, da una parte l'hashtag #IoStoConMattarella, di chi si è schierato a difesa delle Istituzioni incarnate dal capo dello Stato e dall'altra quello di chi ne ha chiesto finanche l'impeachment, #IlMioVotoConta[18] .

La funzione dell'hashtag è infatti proprio quella di aggregare e categorizzare i contenuti presenti sulle piattaforme sociali in relazione al tema trattato e rendere quindi più facile agli utenti individuare contenuti specifici senza perdersi. Nel caso del dibattito della formazione del nuovo governo l'hashtag è diventato la bandiera di opposte fazioni: entrambi usati per essere visibili nel flusso della comunicazione di un evento che ha indotto molti a prendere posizione a favore o contro per far pesare la propria opinione. Quelli che chiedevano l'impeachment

[14] Harari, Y., N. (2018), 21 Lezioni per il XXI secolo, Bompiani, Milano.
[15] Bianchi, L., (2021), Complotti. Da Qanon alla pandemia, cronache dal mondo capovolto, Minimum Fax, Roma.
[16] Rodrigues Fowler, Y., Fowler, Goodman, C., (2017), How Tinder Could Take Back the White House, The New York Times, Disponibile in https://www.nytimes.com/2017/06/22/opinion/how-tinder-could-take-back-the-white-house.html [22 giugno 2017]
[17] Bachini, V., Tesconi, M. (2020), Fake people. Storie di social bot e bugiardi digitali, Codice Edizioni, Torino
[18] Di Corinto, A. (2018), La guerra degli hashtag e il mostro del web. IL Manifesto, Disponibile in https://ilmanifesto.it/la-guerra-degli-hashtag-e-il-mostro-del-web-2/ [31 maggio 2018]

del Presidente però provenivano da 360 account creati ad hoc lo stesso giorno della contestazione sull'allora Twitter, oggi X.

Non ci sono solo i bot. A volte sono le persone in carne ed ossa che approntano messaggi, li automatizzano per pubblicarli a una certa ora e con una certa frequenza e, in una continua azione di propaganda, riempiono i social di informazioni e commenti destinati a sostenere il proprio beniamino. É il caso di Daniel John Sobiesky, un fanatico di Trump scovato dal Washington Post che ne ha raccontato le gesta[19] . Viola Bachini e Maurizio Tesconi nel loro libro Fake People. Storie di social bot e bugiardi digitali, li chiamano "cyborg".

3. Il futuro della disinformazione

È certamente possibile influenzare la narrazione di eventi in corso. Se ancora oggi viene fatto attraverso i titoloni dei giornali e le veline televisive, la novità è che si può fare anche via Internet senza ricorrere a persone in carne ed ossa, ma usando software che si comprano per pochi euro sia nel Dark Web sia in quello di superficie e che i più esperti possono programmare da soli.

Questi software possono fingere di essere utenti della rete e con i loro post, tweet, like e click, spacciarsi per una "opinione pubblica" inesistente il cui messaggio sarà amplificato dai media mainstream a seconda delle convenienze.

La propaganda computazionale è quindi esattamente questo: l'uso di reti di computer, le botnet, e sistemi intelligenti per simulare il comportamento di persone reali nella diffusione di messaggi politici e sociali attraverso il web.

I troll, i molestatori che chiedevano l'impeachment di Mattarella all'epoca del suo rifiuto di nominare ministro Paolo Savona ne rappresentano un esempio: 360 profili Twitter automatizzati creati quasi contemporaneamente per rilanciare post, commenti e hashtag contro il Presidente della Repubblica.

Durante la conferenza Black Hat di Las Vegas nel 2018, una delle più importanti per il mondo della sicurezza informatica, gli esperti dell'azienda Duo Security hanno rilasciato però un insieme di strumenti open source per identificare le botnet che invadono Twitter.

I ricercatori ci sono arrivati a partire dall'analisi di 88 milioni di account Twitter e del loro mezzo miliardo di post sulla piattaforma omonima.

È usando una ventina di euristiche che sono riusciti a individuare in maniera efficace i bot che amplificano messaggi propagandistici. Queste euristiche includono il numero di cifre che ne compone il nome, il rapporto tra follower /following, il tempo tra i tweet, le ore medie twittate al giorno e altri parametri. Per semplificare, un profilo che twitta tutto il giorno probabilmente è un bot perché gli esseri umani tendono a dormire almeno un quarto della giornata, un profilo che

[19] Timberg, J, (2017). As a conservative Twitter user sleeps, his account is hard at work, The Washington Post, Disponibile on line https://www.washingtonpost.com/business/economy/as-a-conservative-twitter-user-sleeps-his-account-is-hard-at-work/2017/02/05/18d5a532-df31-11e6-918c-99ede3c8cafa_story.html [5 febbraio 2017]

non diversifica link, hashtag e messaggi e cita sempre gli stessi utenti è con buona probabilità un bot, e così via.

Quindi nel caso di Twitter scovarli è relativamente semplice: i profili fasulli tipo «GiUsY12345», hanno pochi follower, producono sempre gli stessi messaggi, lo fanno di notte, e replicano raramente a quelli degli altri.

Anche evitare di cascarci dovrebbe essere abbastanza semplice: si scrive il nome del profilo sospetto su un motore di ricerca e se la persona compare su siti di notizie e altri social potrebbe essere una persona vera; incollando nella sezione immagini di Google il suo volto, si potrà poi facilmente scoprire con un confronto incrociato se quella persona esiste realmente oppure è solo il parto di un software.

Oggi però le cose si sono fatte complicate a causa degli «Attacchi Sybil». Questo tipo di attacchi coinvolgono organizzazioni che creano e controllano più account fasulli, i sockpuppet [20], utilizzando come avatar immagini provenienti da social legittimi o da foto di archivio.

Per ora, questo tipo di guerra dell'informazione (troll, bot, cyborg, meme) è relativamente rilevabile e prevedibile, ma gli strumenti e le tattiche moderne stanno diventando sempre più complessi e difficili da contrastare, come quelli che l'intelligenza artificiale consente di creare.

Ad esempio, prima i "fantocci" degli attacchi Sybil potevano essere individuati col "reverse engineering" delle immagini di profilo, ora è più difficile perché con tecniche di intelligenza artificiale è possibile generare immagini uniche di persone inesistenti come dimostra il sito This Person Does Not Exist (thispersondoesnotexist.com)[21] .

Da quando nel novembre del 2022 è stato reso pubblico l'utilizzo di uno strumento di Intelligenza Artificiale generativa (Gen AI), come ChatGPT (Chat Generative Pre Trained Transformer), si è sviluppato un ampio dibattito circa la disponibilità di strumenti come gli LL.MM. (Large Language Models) su cui si fondano, per creare deep fake video[22], deep fake audio, fake images.

A questo proposito si consideri lo scalpore suscitato dalle false immagini di Papa Francesco, atteggiato come un modello in passerella vestire un elegante piumino Moncler in stile trapper[23].

---

[20] Sockpuppet, letteralmente "pupazzo di calzino", è traducibile in maniera figurata come "impostore". Nel gergo informatico, indica un'identità digitale fraudolenta, governata da un burattinaio nascosto

[21] Di Corinto, A, (2019), L'«astroturfing» e i bot di Virgina Raggi, Il Manifesto, Disponibile in https://ilmanifesto.it/lastroturfing-e-i-bot-di-virgina-raggi [18 luglio 2019]

[22] I deep fake sono contenuti multimediali falsi prodotti con algoritmi di intelligenza artificiale

[23] Lana, A. (2023), Dopo Trump, anche il Papa: la foto fake con il cappotto bianco che tutti scambiano per vera, Disponibile in https://www.corriere.it/tecnologia/cards/dopo-trump-anche-il-papa-la-foto-fake-con-il-cappotto-bianco-che-tutti-scambiano-per-vera/il-nbsp-monclero.shtml [27 marzo 2023]

Tuttavia, gli autori della disinformazione cibernetica non hanno certo atteso la comparsa sul mercato di strumenti gratuiti per realizzare immagini fasulle e falsare la percezione e il giudizio del pubblico. Si pensi all'uso che è stato fatto del finto video del presidente ucraino Volodymyr Zelensky ritratto durante una videoconferenza con accanto tutto lo strumentario per farlo apparire come un cocainomane colto sul fatto da una foto rubata: "Quella che dovrebbe sembrare cocaina, è stata aggiunta con un software di video editing al video originale in cui non c'è traccia dell'ipotetica sostanza stupefacente. La prova evidente è proprio il video originale pubblicato su Instagram, il 6 marzo scorso, dallo stesso Zelensky sul suo account ufficiale." (Pisa, 2022)[24].

Oggi i falsi sono prodotti con tecniche di generazione avanzate e quindi risultano difficilmente identificabili; inoltre sono divulgati attraverso canali social creati ad hoc, popolati di maggioranze adoranti indifferenti a ogni statuto di verità dell'oggetto comunicato, bolle filtro di individui con la stessa opinione che riproducono all'infinito i contenuti facendogli da cassa di risonanza.

Secondo l'ultimo Rapporto sui Rischi Globali 2024[25] diffuso dal World Economic Forum a gennaio si prevede che la cattiva informazione, e la disinformazione, costituiranno un vero rischio per i prossimi due anni. Il 2024, è l'anno della più importante tornata elettorale della storia in cui si decideranno il governo dell'India, degli Stati Uniti, del Regno Unito, dell'Europa. Senza contare che già oggi, le operazioni di disinformazione e propaganda computazionale corrono parallele agli attacchi informatici nei conflitti armati. L'invasione russa dell'Ucraina lo ha dimostrato in maniera evidente.

4. La disinformatia russa e le interferenze hacker

Ormai da diversi anni hacker criminali e hacktivisti sono stati "reclutati" per mettere a segno attacchi informatici, azioni di spionaggio e sabotaggio per conto di gruppi di interesse, fazioni politiche, e stati nazione. Gli stessi hacker di stato, che spesso coincidono con gruppi APT, Advanced Persistent Threat, che prendono il nome dalla tecnica usata[26] , collaborano con individui politicamente o economicamente motivati, hacktivisti o cybercriminali, che fanno uso di tecniche di hacking per perseguire la propria agenda. Gli hacktivisti, coinvolti nei conflitti aperti, dall'Ucraina a Israele, e in quelli silenti, ad esempio tra l'Iran e gli USA,

[24] Pisa, P. (2022), Il falso video di Zelensky con la droga sulla scrivania: diffuso sui social dagli account pro-Russia, La Repubblica, Disponibile in https://video.repubblica.it/tecnologia/tech/il-falso-video-di-zelensky-con-la-droga-sulla-scrivania-diffuso-sui-social-dagli-account-pro-russia/414139/415066

[25] World Economic Forum, (2024), Global Risk Report 2024, Disponibile in https://www.weforum.org/publications/global-risks-report-2024/ [10 gennaio 2024]

[26] APT, Advanced Persistent Threat, minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per l'esfiltrazione di informazioni dalle infrastrutture IT del target. É una tecnica peculiare degli hacker di stato finanziati dai governi.

usano le tecniche che prima erano del sabotaggio culturale (Di Corinto & Tozzi, 2022)[27] per far avanzare la propria agenda politica. Questi hacker, qualunque sia il loro livello organizzativo e di comando, sono stati coinvolti a più riprese in operazioni di "hack and leak" (hackera e fai trapelare), "steal and publish" (ruba e pubblica), con l'obiettivo di creare confusione, panico e paranoia nel pubblico (Rid, 2021/2022)[28].

Ad esempio, secondo la società di consulenza Graphica, gruppi cinesi sono stati coinvolti in operazioni di disinformazione verso il governo americano, il presidente Biden e i manifestanti di Hong Kong[29] ; paesi come l'Iran hanno agito attraverso dei proxy informatici, hacktivisti e ransomware gangs, per sostenere la causa arabo-palestinese o per mostrare i muscoli agli USA[30] ; la Corea del Nord lo ha fatto per inquinare le prove delle incursioni dei propri hacker di stato[31] ; i servizi segreti russi per legittimare la causa dell'annessione della Crimea alla Federazione Russa, vestendo i panni di Anonymous.

La cifra comune di azioni tanto diverse è che ogni attacco informatico si svolge parallelamente ad un'azione di disinformazione per negare l'accaduto oppure per amplificarne la portata, ad esempio nei canali Telegram, laddove i risultati si siano rivelati modesti. Questo ultimo è il caso degli attacchi DDoS[32] portati da gruppi filorussi come Killnet (Di Corinto & Rociola, 2022)[33] , o di hacktivisti con vocazione religiosa come Anonymous Sudan o Mysterious Team Bangladesh.

Sono diversi i paesi che fanno ricorso agli hacker per sviluppare tool, strategie e azioni di propaganda e disinformazione, tuttavia, ritengono gli analisti, il modo di operare dei russi e dei filorussi è emblematico dell'uso che ne fanno in concomitanza con gli attacchi informatici veri e propri.

---

[27] Di Corinto, A. Tozzi, T., (2002). Hacktivism. La libertà nelle maglie della rete, Manifestolibri, Roma.

[28] Rid, T. (2022). Misure Attive. Storia segreta della disinformazione, Roma, Luiss University Press; tit. or. Active Measures: The Secret History of Disinformation and Political Warfare, Ferrar Straus & Giroux 2021.

[29] Di Corinto, A. (2020), Il Dragone attacca con le fake news, sicuri di riconoscerle? Il Manifesto, Disponibile in https://ilmanifesto.it/il-dragone-attacca-con-le-fake-news-sicuri-di-riconoscerle [20 luglio 2020]

[30] Di Corinto, A. (2020), Iran vs Usa, la cyberguerra è solo agli inizi, La Repubblica, Disponibile in https://www.repubblica.it/tecnologia/sicurezza/2020/01/09/news/iran_vs_usa_la_cyberguerra_e_solo_agli_inizi-245335228/ [9 gennaio 2020]

[31] Di Corinto, A. (2021), Corea del Nord: cybercrime di Stato per finanziare il programma nucleare, La Repubblica, Disponibile in https://www.repubblica.it/esteri/2021/02/11/news/nord_corea_cybercrime_di_stato_per_finanziare_il_programma_nucleare-287136346/ [11 febbraio 2021]

[32] DoS, Denial of Service, negazione di servizio, ovvero blocco dei servizi web, causato da numerose richieste di accesso illegittime al servizio esposto. La sua variante più nota è il DDoS, il Distributed Denial of Service attack

[33] Di Corinto, A., Rociola, A., (2022). Attacco hacker all'Italia. Cos'è Killnet, il gruppo russo che lo ha rivendicato, La Repubblica, Disponibile in https://www.repubblica.it/tecnologia/2022/05/11/news/attacco_hacker_italia_russia_killnet-349111881/ [11 maggio 2022]

Secondo Treyger et al. (2022), che hanno studiato gli sforzi della disinformazione russa sui social network, “Alcune delle attività russe che si svolgono sui o attraverso i social media non sono pura disinformazione; si tratta piuttosto di sforzi di disinformazione collegati funzionalmente a un attacco informatico di qualche tipo. Pertanto, anche se ci teniamo in gran parte lontani dalla discussione tecnica sugli attacchi informatici, tocchiamo le operazioni informatiche quando queste sono strettamente legate ad attività che utilizzano l’informazione per modellare percezioni o comportamenti, ad esempio, hack che producono informazioni che vengono successivamente trapelate”[34] .

Questo passaggio rappresenta bene il pensiero strategico dei russi rispetto al conflitto informativo che integra due aspetti: quello tecnico-informatico, che mira a influenzare “i sistemi tecnici che ricevono, raccolgono, elaborano e trasmettono informazioni”, e quello informativo-psicologico, che mira a colpire “il personale delle forze armate e la popolazione”.

Un pensiero ben descritto da Calise e Musella quando nel saggio Il Principe digitale (2019) scrivono: “Ma la vera novità del conflitto 2.0 è la sua penetrazione a livello di massa, con iniziative di propaganda o di campagna psicologica volte a influenzare quanto i cittadini sanno di sé e degli altri. In questo caso gli attacchi digitali non sono destinati a bersagli di tipo militare o infrastrutturale. Siamo invece in presenza di azioni mirate a condizionare il clima politico in un altro paese, o a mettere a repentaglio procedure di cruciale rilevanza come le elezioni. Una minaccia che preoccupa le democrazie occidentali, perché va al cuore stesso del loro sistema operativo: l'autonomia dell'opinione pubblica. E si gioca sulle piattaforme che connettono centinaia di milioni di cittadini”.

In generale, gli autori militari hanno identificato le seguenti caratteristiche che raccomandano i social media come arma informativa:

- il basso costo delle operazioni sui social media sia in termini di fondi che personale
- l'ampia portata potenziale delle operazioni di informazione online, soprattutto considerando la crescente penetrazione di Internet
- la capacità di reagire in tempo reale e in luoghi senza presenza fisica
- la negabilità delle operazioni sui social media, data la difficoltà nel distinguere l'attività ordinaria dagli atti di guerra dell'informazione sponsorizzati dallo stato
- la percezione che gli effetti psicologici dei media online e dei social media siano superiori a quelli forniti dai media tradizionali a causa del potenziale di confezionare contenuti multimediali in modo da ottenere “ulteriore influenza emotiva e psicologica”.

Un esempio di scuola è quello che è successo negli Stati Uniti con la campagna che ha portato Donald Trump alla Casa Bianca. Gli apparati di intelligence e

[34] Treyger, E. Cheravitch, J. Cohen, R. S., (2022) Russian disinformation Effort on social Media, Rand Corporation

importanti segmenti della politica statunitense, ricollegandosi al filone di indagine giudiziaria che ha preso il nome di Russiagate, hanno accusato Mosca di una intensa e duratura manipolazione delle informazioni al fine di favorire l'attuale presidente in carica. Renée Di Resta, capo di una delle due agenzie di cybersecurity incaricate dal Senato americano di studiare i meccanismi di influenza russa, ha parlato senza mezzi termini di "guerra mondiale dell'informazione"[35] .

Sono numerose le azioni di interferenza documentate di hacker russi nei processi democratici dei paesi occidentali. Dall'inizio della Guerra in Ucraina queste interferenze si sono moltiplicate, ma già prima ne abbiamo avuto numerosi esempi. Nel 2007 un vasto attacco DDoS viene compiuto in Estonia come ritorsione per lo spostamento della statua del soldato sovietico dal centro alla periferia di Tallinn, la capitale; nel 2008, in Georgia, quando all'attacco ai siti web georgiani si affianca una campagna militare vera e propria; nel 2014, quando il servizio segreto militare russo Gru crea un video falso di Anonymous per sostenere l'invasione dell'Ucraina; infine nel 2022, quando l'invasione del Donbass ucraino viene accompagnata da una serie di attacchi informatici: DDoS, defacciamenti e distribuzione di virus wiper che cancellano i registri di memoria dei computer Windows.

Il Digital Forensic Research Lab del Consiglio Atlantico pochi giorni prima[36] aveva segnalato una serie di false narrative distribuite sui social media e propagandate da giornali e televisioni pro-Cremlino. Intanto però prima dell'ingresso delle truppe russe in Ucraina, e degli attacchi informatici, i modem della rete Internet satellitare KA-SAT di Viasat venivano disabilitati in massa. In aggiunta a questo, i servizi segreti di Vladimir Putin hanno sfruttato i gruppi ransomware filorussi come Conti Team per attaccare la supply chain (ovvero la filiera di approvigionamento) di aziende dei paesi Nato con l'obbiettivo di interferire con la produzione di armi e l'erogazione di servizi essenziali come acqua e servizi sanitari.

5. Le cyber-operations russe

Il 27 aprile 2021 Microsoft pubblica un documento[37] in cui spiega il parallelismo tra le azioni di hacking e di disinformazione dei russi. Per gli esperti dell'azienda di Redmond negli Stati Uniti, da prima dell'invasione fino alla pubblicazione del rapporto, sono state lanciate 237 cyber-operations contro l'Ucraina da parte di almeno sei differenti gruppi di nation state hacker, ossia di esperti informatici governativi collegati ai servizi segreti interni ed esteri e militari russi.Si tratta in gran parte di attacchi distruttivi che hanno fatto uso di virus informatici per indebolire la capacità di reazione del Paese attaccato avendo come target le

[35] M. Calise, F. Musella, Il Principe digitale, Laterza, 2019
[36] Digital Forensic Research Lab, How ten false flag narratives were promoted by pro-Kremlin media, Feb 18, 2022, Medium [Online], https://medium.com/dfrlab/how-ten-false-flag-narratives-were-promoted-by-pro-kremlin-media-c67e786c6085
[37] Microsoft Digital Security Unit, (2022). An overview of Russia's cyberattack activity in Ukraine, Disponibile in https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. [10 settembre 2023] Microsoft Digital Security Unit

istituzioni ucraine, i servizi e le aziende informatiche, il comparto energetico, i media, le telecomunicazioni e Internet.

Secondo gli specialisti dell'azienda americana gli attacchi distruttivi sono stati accompagnati anche da ampie attività di spionaggio e sabotaggio che hanno sia degradato i sistemi informatici delle istituzioni in Ucraina, sia cercato di interrompere l'accesso delle persone a informazioni affidabili cercando di minare la fiducia nella leadership del paese.

Come dettaglia il rapporto, l'uso da parte della Russia di attacchi informatici e disinformazione sembrano essere fortemente correlati e talvolta direttamente sincronizzati con le sue operazioni militari cinetiche (quelle che in gergo militare indicano il movimento), che prendono di mira servizi e istituzioni cruciali per i civili. Il 1° marzo 2022, infatti, mentre un gruppo russo lancia attacchi informatici contro un'importante compagnia televisiva, l'esercito russo annuncia l'intenzione di voler distruggere obiettivi ucraini di "disinformazione" e dirige un attacco missilistico contro una torre della Televisione a Kiev. Ancora, mentre le forze russe assediano la città di Mariupol, gli ucraini ricevono un'e-mail da hacker russi che, fingendosi residenti di Mariupol, accusano falsamente il governo ucraino di "abbandonare" i suoi cittadini.

Gli attori coinvolti in questi attacchi insomma utilizzano una varietà di tecniche per superare le difese degli obbiettivi, tra cui il phishing, lo sfruttamento di vulnerabilità non risolte del software e la compromissione dei fornitori di servizi di Information Technology IT, gli attacchi alla supply chain.

Le operazioni di influenza e di interferenza praticate dai russi non sono sempre riconducibili ad ordini impartiti da Mosca, ma questa è proprio l'essenza della guerra ibrida teorizzata dai suoi stessi generali (Ottaviani, 2022[38] ; Bigazzi et al., 2022 [39]).

Come scrive Mark Galeotti: "Per combattere la sua guerra politica la Russia ha creato una macchina indubbiamente flessibile, economica, immaginifica e intraprendente, ma anche difficile da controllare. L'idea che tutti i troll, i propagandisti, le milizie, i corruttori, gli hacker e gli altri soldati di questo esercito siano sempre sotto lo stretto controllo del governo è assolutamente sbagliata. Certo, vi sono operazioni gestite sin dall'inizio a livello centrale e quelle di particolare importanza che, chiaramente, richiedono l'imprimatur del Cremlino. Rientrano in questo novero l'assassinio di Sergej Skripal in Inghilterra nel 2018 e l'interferenza nelle presidenziali americane del 2016. Nel grosso dei casi, tuttavia, Mosca ha incoraggiato molti «imprenditori politici» a prendere l'iniziativa, sovente con i loro tempi e a loro spese. Se falliscono, possono essere disconosciuti; se

[38] Ottaviani, M. F. (2022), Brigate Russe. La guerra occulta del Cremlino tra troll e hacker, Milano, Ledizioni LediPublishing
[39] Bigazzi, F., Fertilio, D., Germani, S., (2022). Bugie di guerra. La disinformazione russa dall'Unione sovietica all'Ucraina. Roma, Paesi Edizioni

riescono, possono essere premiati e a quel punto lo Stato può subentrare, ampliando o sviluppando l'operazione"[40] .

A fugare gli eventuali dubbi circa il rapporto esistente tra l'hacking e la diffusione di notizie false sono intervenuti gli stessi servizi segreti ucraini, arrestando un gruppo di cybercriminali specializzato nella vendita di account per diffondere disinformazione. Le autorità ucraine, pur non rivelando i nomi degli arrestati, hanno fornito le prove dell'attività di un gruppo di hacker operanti a Lviv in possesso di circa 30 milioni di account appartenenti a cittadini ucraini ed europei venduti sul DarkWeb. Le perquisizioni effettuate nelle case dei sospettati hanno portato al sequestro di hard disk contenenti dati personali, cellulari, schede Sim e memorie flash usate per lo scopo.

Secondo le stime degli investigatori, il gruppo, pro-russo, avrebbe guadagnato circa 400mila dollari rivendendoli all'ingrosso attraverso sistemi di pagamento elettronici come Qiwi e WebMoney.

Nel comunicato stampa il Servizio di sicurezza dell'Ucraina (SSU) sostiene che i clienti sarebbero propagandisti pro-Cremlino: "Sono stati loro a utilizzare i dati identificativi di cittadini ucraini e stranieri rubati dagli hacker per diffondere false notizie dal fronte e seminare il panico".

Nel comunicato si dice che gli hacker avrebbero operato per questo scopo: "la destabilizzazione su larga scala in più paesi", e che gli account sono stati utilizzati per diffondere false informazioni sulla situazione sociopolitica in Ucraina e nell'UE, precisando che "l'attività principale dei clienti degli hacker era proprio la creazione e la promozione di account nei social network e nei canali di messaggistica veloce".

In precedenza, le autorità avevano chiuso due farm di bot da 7.000 account per diffondere disinformazione e creare panico nella regione. Un'attività legata a una fase della guerra russo-ucraina in cui i cittadini di alcune zone, soprattutto nel Donbass occupato, non ricevono né cibo né informazioni. I pochi giornalisti che sono riusciti a parlarci infatti hanno dichiarato che gli ucraini sotto occupazione non conoscono l'entità dello scontro con Mosca, la percentuale di territorio occupata e se i propri congiunti siano vivi. Secondo Google-Mandiant[41] quando gli hacker governativi russi attaccano, passano i dati rubati agli hacktivisti entro 24 ore dall'irruzione in modo da consentirgli di effettuare nuovi attacchi e diffondere propaganda filorussa. Esempio da manuale di come il rapporto tra criminalità cibernetica, hacktivismo e hacking di stato sia anche più diretto[42].

[40] M. Galeotti, Controlling Chaos: How Russia manages its political war in Europe, European Council on Foreign Relations, 2017, https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/
[41] Mandiant, Hacktivists Collaborate with GRU-sponsored APT28, sept 2022, updated aug. 2023, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions
[42] A. Di Corinto, Hacking e disinformazione, la scuola russa, Il Manifesto, 29 Settembre 2022, [Online], https://ilmanifesto.it/hacking-e-disinformazione-la-scuola-russa

6. Conclusioni

Ogni società ricorre a delle narrazioni per fare progredire i gruppi sociali che la compongono verso mete utili alla collettività. Il senso e la direzione di queste narrazioni, politiche, sociali e religiose, cambia nei secoli, ed è in genere indifferente alla nozione di verità, concetto mobile e sfuggente per definizione. La creazione del consenso intorno a queste narrazioni si basa su storie condivise e la loro forza dipende dall'innesco di meccanismi psicologici come la credulità, il conformismo, la reciprocità, l'autorevolezza, sfruttando il principio di autorità, di similarità, di credibilità e così via.

Questi principi possono, e sono manipolati costantemente, da specifici attori.

La propaganda è una forma di narrazione di storie collettive, e la disinformazione si basa su distorsioni narrative, bias psicologici e tecniche persuasive. Con l'avvento del digitale e dei social network è più facili propagandare narrazioni vere, false, o inventate. Possono essere automatizzate, elicitano risposte rapide, non sono sempre verificabili. Gli attori della disinformazione lo sanno, e mescolano sapientemente il vero con il falso per elicitare risposte che avvantaggiano taluni e danneggiano altri.

É l'apoteosi dei servizi di intelligence che operano secondo la logica delle misure attive, l'insieme dei comportamenti volti a manipolare la percezione di un target, e che usano le fake news come una testa d'ariete per portare il loro attacco, l'attacco alla mente.

BIOGRAFIA

Arturo Di Corinto è stato professore di Identità Digitale, Privacy e Cybersecurity presso la Facoltà di Scienze Politiche, Sociologia e Comunicazione dell'Università di Roma la Sapienza, dove si è laureato in psicologia cognitiva. Attualmente ricopre il ruolo di advisor della comunicazione e degli affari pubblici presso l'Agenzia Nazionale per la Cybersicurezza (ACN) dove è responsabile anche delle pubbliche relazioni.

Giornalista interessato al tema dell'innovazione, ha lavorato anche per Il Sole 24 Ore, Wired e La Repubblica scrivendo 2300 articoli e molti libri su la governance di Internet, il copyright, la privacy e la cybersicurezza. Ha lavorato anche come giornalista esparto di temi di scienza e Tecnologia presso la televisione pubblica italiana.

Email: arturo.dicorinto@uniroma1.it