ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

16

ISSUE 2/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 16/2022

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 978-88-9335-041-9

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Social bots and synthetic interactions to stage digital extremist armies

Daniele Maria Barone

Daniele Maria Barone is a counter-terrorism analyst. He served as an Italian Coast Guard officer and worked as a project manager and digital communication specialist in the private sector. He graduated in Marketing & Communication at IULM University, obtained a master's degree in International Relations at ASERI Graduate School of Economics and International Relations – Catholic University of the Sacred Heart, and specialized in counter-terrorism studies earning an Executive Certificate at the International Institute for Counter-Terrorism (ICT) – Herzliya. His research interests are cyber-jihad, terrorist financing, and terrorist organizations' communication strategies.

Abstract

Artificial intelligence (AI)-made bots for social media platforms are becoming increasingly sophisticated and able to impersonate average users, developing either as valuable AI tools in the communication field or as an instrument for online deception.
As AI keeps advancing, also terrorist organizations will benefit from these technological developments to increase the efficiency of their use of social media. For instance, they could increasingly avoid being flagged by users or detected and banned by the platforms, supporting radicalization or propaganda with less risk while gaining greater resonance.
From this perspective, the analysis will firstly focus on how social bots work, their role in helping to perceive synthetic interactions as authentic interactions, and their potential contribution to social manipulation. Then, the paper will delineate how AI-bot developments intersect with terrorist or extremist communication environments.

I social media bot creati attraverso l'intelligenza artificiale (IA) diventano sempre più sofisticati e in grado di imitare con maggiore efficacia il comportamento degli utenti. Questo li ha resi sia strumenti particolarmente validi nel settore della comunicazione sia una risorsa utile per ingannare gli utenti.
Con l'avanzamento e la diffusione dell'IA, anche le organizzazioni terroristiche potranno beneficiare di questi sviluppi in campo tecnologico, migliorando la loro efficenza nell'utilizzo dei social media. Ad esempio, i social bot potrebbero aiutare le organizzazioni terroristiche a diminuire le possibilità di essere segnalati dagli utenti e sospesi dalle piattaforme social, supportando i loro processi di radicalizzazione e diffondendo la loro propaganda con un rischio inferiore ma garantendo una maggiore risonanza.
Partendo da questa prospettiva, dopo aver analizzato il funzionamento dei social bot, in quale misura questi ultimi possono favorire la percezione di interazioni sintetiche come autentiche ed il loro contributo alla manipolazione sociale, la ricerca delineerà le aree principali attraverso cui lo sviluppo tecnologico dei bot si interseca con i contesti comunicativi di gruppi terroristici o estremisti.

Keywords

Social media bot, jihad, far-right, conspiracy theories

1. Introduction

On June 16, the European Commission welcomed the strengthened Code of Practice on Disinformation, a framework to set out commitments by platforms and industry to fight disinformation.[1] The first 2018 anti-disinformation Code consisted of self-regulatory standards to fight disinformation to which tech-industry representatives agreed voluntarily.[2] The reinforcing process of the Code has been signed by 34 actors from the tech industry as online platforms, ad-tech companies, fact-checkers, and civil society organizations.[3] Amid its measures, it includes to "cut financial incentives for spreading disinformation" to "empower users with better tools to recognize, understand and flag disinformation" and to "expand fact-checking in all EU countries and all its languages." The Code also provides measures to prevent malicious actors from covering manipulative behaviors used to spread disinformation using fake accounts, deepfakes, and bot-driven amplification.[4]

In this respect, the use of artificial intelligence (AI), even at its rudimentary level, is creating a growing interest in its possible exploitation not only to spread disinformation but also for extremist or terrorist purposes.

In particular, the creation of AI-made fake accounts and bots for social media platforms are becoming increasingly sophisticated and able to impersonate average users[5] developing, on the one hand, as the most used AI tools in the communication field and, on the other hand, as an instrument for online deception.

[1] European Commission (June 16, 2022) *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3664.

[2] European Commission *2018 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[3] European Commission (June 16, 2022) *Signatories of the 2022 Strengthened Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

[4] European Commission *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[5] Kilcher Y. (June 3, 2022) *This is the worst AI ever*. YouTube. https://www.youtube.com/watch?v=efPrtcLdcdM.

As explained by a joint report by UNICRI and UNCCT,[6] as AI keeps advancing, also terrorist organizations will benefit from these technological developments to increase the efficiency of their use of social media. They could become more and more able to avoid being flagged by users or being detected and banned by the platforms, supporting radicalization or propaganda with less risk, while gaining greater resonance.[7]

To define in which ways AI-bot developments intersect with terrorist or extremist communication environments, the analysis will first understand how bots work, in which ways social bots could help perceive synthetic interactions as authentic interactions and their potential contribution to social manipulation.

2. A how-to guide to normalize "synthetic realness"

Even though AI is not a new technology,[8] only in the last decades it has shown its impact on businesses and people's everyday lives, making it hard to discern where it stops and humanity begins.[9] To better understand the pervasiveness of AI in the digital communication environment, it is useful to highlight some major areas in which its acceptance degree and uses are evolving.

2.1 A growing, promising business

The potential pervasiveness of the whole AI sector is allowing the AI market, which was valued at USD 65.48 billion in 2020, to be projected to reach USD 1,581.70 billion by 2030.[10] Indeed, AI-enabled systems will continue to support many sectors, for instance, healthcare, education, financial services,

[6] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

[7] Ciancaglini V., Gibson C., Sancho D., Amann P., Klayn A., McCarthy O., and Eira M. (November 19, 2020). *Malicious Uses and Abuses of Artificial Intelligence. Trend Micro*. EUROPOL and UNICRI. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf.

[8] Harvard special edition: *Artificial Intelligence*. https://sitn.hms.harvard.edu/special-edition-artificial-intelligence/.

[9] Forsbak Ø. (March 25, 2022) *Six AI Trends To Watch In 2022*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/03/25/six-ai-trends-to-watch-in-2022/?sh=3e1c36e62be1.

[10] PR Newswire (June 13, 2022) *Artificial Intelligence Market USD 1,581.70 Billion By 2030, Growing At A CAGR of 38.0%*. Bloomberg press release. https://www.bloomberg.com/press-releases/2022-06-13/artificial-intelligence-market-usd-1-581-70-billion-by-2030-growing-at-

engineering, security, and transport, and are already changing the way businesses understand both internal and external processes.

2.2 Big (artificial) data to kickstart the modern economy

AI is changing the foundation of the modern economy: big data.[11] AI systems work by combining large sets of data with intelligent, iterative processing algorithms to learn from patterns and features in the data that they analyze, allowing machines to learn from experience, adjust to new inputs and perform human-like tasks.

To train AI, companies used to rely exclusively on data generated by real-world events until they realized there wasn't enough data to support the algorithm's training.[12] This limit brought to provide synthetic data, which consists of a technology that enables to digitally generate the data, on demand, in whatever volume, and artificially manufactured to precise specifications.

This approach helps to bypass, for instance, confidentiality and privacy issues when gathering data to train AI for healthcare purposes, detect specific and rare patterns in credit-card frauds, and generate data required to build a safe autonomous vehicle.[13] Furthermore, synthetic data in AI systems could help remove bias in machine learning, allowing algorithmic decision-making to avoid infinitely reproducing human errors, reducing face-to-face discrimination in markets prone to implicit and explicit biases as, for example, in the context of consumer lending.[14]

2.3 Synthetic authenticity becomes the new real

With these premises, the widespread implementation of AI has brought either developments or new challenges in business, organizations, and society

a-cagr-of-38-0-valuates-reports#:~:text=Artificial%20Intelligence%20Market%20USD%201%2C581.70,38.0%25%20%2D%20Valuates%20Reports%20%2D%20Bloomberg.

[11] The Economist (May 6, 2017) *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[12] Castellanos S. (July 23, 2021) *Fake It to Make It: Companies Beef Up AI Models With Synthetic Data*. Wall Street Journal. https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601.

[13] Towes R. (June 12, 2022) *Synthetic Data Is About To Transform Artificial Intelligence*. Forbes. https://www.forbes.com/sites/robtoews/2022/06/12/synthetic-data-is-about-to-transform-artificial-intelligence/?sh=5e6a76c07523.

[14] Bartlett R., Morse A., Stanton R., and Wallace N. (June 2019) *Consumer-Lending Discrimination in the FinTech Era*. National Bureau of Economic Research. https://www.nber.org/papers/w25943#:~:text=FinTech%20algorithms%20also%20discriminate%2C%20but,borrowers%20on%20low%2Dshopping%20behavior.

at large, in an ongoing process of creation of a world of synthetic realness, where AI-generated data convincingly reflect the physical world.[15] Thus, given developments and potential improvements of AI, the question, as expressed in a report by Accenture, is: "What's real, what's not and perhaps more importantly, when do we care?"[16]

In this context of blurred divergences between synthetic and real, the most evident direct interaction with AI is in the intersection between technology and communication through the use of bots in the now-familiar social media/chat services environment.

A bot is a software agent or third-party service programmed to perform certain actions on a regular or reactive basis, without having to rely, or partially relying, on human intervention. The bot analyzes the circumstances and autonomously decides what action to take. In particular, a social bot can mimic human behavior in social networks, taking part in discussions, pretending to be a real user. Social bots can post content, mostly through fake accounts, like, share, and comment. To perform efficiently a bot needs a technical infrastructure, which, in a nutshell, consists of a combination of the profile on a social media platform and the technical preconditions for partial automation of the account's behavior, through the chosen platform's Application Programming Interface (API)[17] or proprietary mechanisms[18] to interact with the website or app.[19]

Then, bots require a low level of human management: hundreds or even thousands of social bots can be managed by a single person.[20] In that regard, it has been roughly estimated that, only in 2017, there were 23 million bots

[15] Accenture (June 17, 2022) *The unreal – making synthetic, authentic*. https://www.accenture.com/th-en/insights/health/unreal-making-synthetic-authentic.

[16] Accenture (March 16, 2022) *Technology Vision 2022: "Metaverse Continuum" Redefining How the World Works, Operates and Interacts.* https://newsroom.accenture.com/subjects/metaverse/accenture-technology-vision-2022-metaverse-continuum-redefining-how-the-world-works-operates-and-interacts.htm.

[17] "An application programming interface, or API, enables companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments within their companies. This allows services and products to communicate with each other and leverage each other's data and functionality through a documented interface." IBM *Application Programming Interface (API)*. https://www.ibm.com/cloud/learn/api.

[18] *Bots: An introduction for developers*. Telegram. https://core.telegram.org/bots.

[19] Assenmacher D., Clever L., Frischlich L., Quandt T., Trautmann H., and Grimme C. (September 1, 2020) *Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*. Social media and Society. https://journals.sagepub.com/doi/10.1177/2056305120939264.

[20] Cloudfare. *What is a social media bot? | Social media bot definition*. https://www.cloudflare.com/it-it/learning/bots/what-is-a-social-media-bot/#:~:text=Experts%20who%20have%20applied%20logarithms,designed%20to%20mimic%20human%20accounts.

on Twitter (8.5% of all accounts), 140 million bots on Facebook (5.5% of all accounts), and about 27 million bots on Instagram (8.2% of all accounts).[21]

Moreover, according to the University of California,[22] in 2020, about 13% of all Twitter users that retweeted or engaged in conspiracy theories were bots,[23] while Facebook banned 1.6 billion accounts actioned on fake accounts only in the first quarter of 2022.[24]

2.4 The manipulative side of social bot

The use of social bots to manipulate is not new but has been spreading faster over time.

For instance, social media platforms, such as Facebook and Twitter, were used to organize protests and spread awareness of updates and movements during the Arab spring.[25] Almost a decade later, those same social media platforms found and removed hundreds of bot accounts "for engaging in coordinated inauthentic behavior," as disinformation, spamming,[26] and state-backed manipulation[27] during the spring 2011 events.

Another example comes from studies claiming that the key to the success of Farage Brexit party is related to the clarity and simplicity of its messaging, compared to Change UK, the Greens, and the Liberal Democrats, and by an effective social media echo chamber of pro-Brexit bot accounts.[28] In this respect, a study in the Social Science Computer Review uncovered the deployment of a network of 13,493 Twitterbots that tweeted mainly messages

[21] Vosoughi S., Roy D., and Aral S. (March 9, 2018) *The spread of true and false news online*. Science. https://www.science.org/doi/10.1126/science.aap9559.

[22] Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

[23] Botometer https://botometer.osome.iu.edu/.

[24] Meta, Community Standards Enforcement Report – Q1 2022 report. https://transparency.fb.com/data/community-standards-enforcement/?source=https%3A%2F%2Ftransparency.facebook.com%2Fcommunity-standards-enforcement.

[25] Roach S. (December 7, 2021) *3 TIMES BOTS HAVE IMPACTED MAJOR WORLD EVENTS*. Natacea. https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/.

[26] Guesmi H. (January 27, 2021) *The social media myth about the Arab Spring*. AlJazeera. https://www.aljazeera.com/opinions/2021/1/27/the-social-media-myth-about-the-arab-spring.

[27] The Economic Times (November 30, 2021) *Arab Spring: The first smartphone revolution*. https://economictimes.indiatimes.com/news/international/saudi-arabia/arab-spring-the-first-smartphone-revolution/articleshow/79487524.cms.

[28] Savage M. (June 29, 2019) *How Brexit party won Euro elections on social media – simple, negative messages to older voters*. The Guardian. https://www.theguardian.com/politics/2019/jun/29/how-brexit-party-won-euro-elections-on-social-media.

supporting the Leave campaign, that were deactivated or removed by Twitter shortly after the ballot.[29]

In most recent times, a study by Carnegie Mellon University[30] on more than 200 million tweets discussing coronavirus from January to May 2020, found that about 45% of tweets on Covid were posted by accounts that behaved more like computerized robots than humans, spreading more than 100 false narratives about the virus.[31]

Nowadays, using recent developments in AI, it is possible to unleash human-like crowds of social bots, in coordinated campaigns of deception and influence[32] fueled by bots socialization with humans for attention, information, and money.[33] With advancements in natural language processing (NLP), a branch of AI that helps computers understand, interpret and manipulate human language,[34] bots can learn over time on the basis of their interactions with social media users, enabling them to respond in a manner that better resembles a human.[35]

Nevertheless, besides cutting-edge technologies or the exploitation of rudiments of AI, the manipulative use of social bots is a consequence of real people behavior and choices;[36] from programming, spreading manipulative content, and influencing communication exchanges on polarizing topics,[37] to choosing to believe those contents.

[29] Bastos M.T., Mercea D. (2017) *The Brexit Botnet and UserGenerated Hyperpartisan News*. Social Science Computer Review. https://journals.sagepub.com/doi/10.1177/0894439317734157.
[30] Allyn B. (May 20, 2020) *Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots*. NPR. https://www.npr.org/sections/coronavirus-live-updates/2020/05/20/859814085/researchers-nearly-half-of-accounts-tweeting-about-coronavirus-are-likely-bots?t=1655890800628.
[31] Roberts S. (June 16, 2020) *Who's a Bot? Who's Not?*. The New York Times. https://www.nytimes.com/2020/06/16/science/social-media-bots-kazemi.html.
[32] Terrence A. (June 2017) AI-Powered Social Bots. https://www.researchgate.net/publication/317650425_AI-Powered_Social_Bots.
[33] Liu X. (April 2019) *A big data approach to examining social bots on Twitter*. Journal of Services Marketing. https://www.researchgate.net/publication/332331554_A_big_data_approach_to_examining_social_bots_on_Twitter.
[34] Natural Language Processing (NLP) SAS. https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html.
[35] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.
[36] CITS *How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting*. https://www.cits.ucsb.edu/fake-news/spread.
[37] Chen W., Pacheco D., Yang K., Menczer F. (September 22, 2021) Neutral bots probe political bias on social media. Nature. https://www.nature.com/articles/s41467-021-25738-6.

Then, the malicious use of social bots needs to be contextualized in the ideology of terrorist or extremist groups. Thus, the next step of the analysis will be to outline how these actors have already and could further empower the consolidated acceptance of human-bot interaction through their ideology.

3. Social bots and jihad: different uses serving different purposes

Jihadist groups' ability to build and maintain a large online community through social media is well known, as well as their capacity, growing out of a state of necessity or creativity, to be early adopters of new technologies. In this respect, the nexus between AI and jihadist communication strategies is no exception: over time, jihadist groups have proven they can get out the most even with basic notions of AI or lack of financial resources.

Every day, bots are being used by jihadis, especially on Telegram,[38] for a wide variety of purposes.

The evolution of jihadists' exploitation of social bots can be analyzed by relating some topic cases with the objectives bots were meant to fulfill in the jihadist landscape.

3.1 Exploit users to expand the organization's influence

In 2014, long before the stricter policy adoption on terrorist propaganda by social media platforms, Daesh spread its official app "Dawn of the Glad Tidings" also known as "Dawn." It was an Arabic-language Twitter app, advertised by its top users as a way to keep up on the latest news about the jihadist group.[39] As a result, thousands of their Twitter followers installed the app on the web or their Android phones through the Google Play store and, after releasing a fair amount of personal data and signing up, they allowed the app to post tweets from their accounts.[40] Thus, Daesh was able to share, through thousands of accounts, simultaneously, content decided by its social-

[38] ISIS watch on Telegram claims that, only on June 22, 2022, 685 terrorist bots and channels has been banned and, since the beginning of June 2022, a total of 11387 terrorist bots and channels has been banned. https://t.me/ISISwatch/1049.

[39] Berger J.M. (June 16, 2014) *How ISIS Games Twitter*. The Atlantic. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[40] Kingsley P. (June 23, 2014) *Who is behind Isis's terrifying online propaganda operation?* The Guardian. https://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq.

media operation branches, gaining a far larger online reach than only top users would otherwise allow.

Dawn allowed to spread news of Daesh advances, trending hashtags, and propaganda videos, interrupting ongoing conversations and letting IS content seeps into popular discourse while contributing to create the organization's image of a violent and unstoppable force.[41]

3.2 Instruct and inform a digital community

The "Bot Mujahideen" Telegram Channel[42] worked as a centralized online interface meant to provide information on a wide range of topics related to jihad fighters in Syria.[43] It was launched in 2016 and, even though it stated it was "not affiliated with any organization and adheres to the path of the Sunnah and jihad," the correspondence published on the channel indicated its support for Jabhat Fateh al-Sham (formerly Al-Nusra Front, which was identified with Al-Qaeda) and other jihad factions tied to the group.[44]

The operative functions of the Bot Mujahideen declined through the management of several other Telegram channels, called "rooms"; each room was dedicated to a different issue and had over 1,000 members. As reported in a research by the ICT, among other rooms, the bot controlled: the "Military Sciences room" ('Ulum 'Askariyya) focused on military topics (e.g. study and operation of various weapons, defense against aircraft shootings, the study and assembly of explosive devices, etc.); "The Public Market of the Brothers," a virtual market for the sale and purchase of weapons; "Network Mujahideen Newsletter" a bot aimed to keep supporters updated on events about the jihad in Syria.

[41] Garfield L. (December 14, 2015) *ISIS has created thousands of political bots – and hacktivists want you to destroy them*. Business insider. https://www.businessinsider.com/anonymous-battles-isis-political-bots-2015-12?r=US&IR=T.

[42] Antinori A. (April 10, 2017) *The "Jihadi Wolf" Threat*. Europol. https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf.

[43] "On the profile of the channel it states that the channel expressed a "unique military jihadist collective program on the Telegram social network, as it is not affiliated with any organization and adheres to the path of the Sunnah and jihad". In addition, it states that "the Bot is a complete jihadist library. Its membership is composed of unique groups that are supervised by mujahideen and experts in their fields". @bot_mojahed2016_bot" ICT Cyber Desk (December 2016) *Cyber-Terrorism Activities Report No. 19*. International Institute for Counter-Terrorism (ICT).

[44] Barak M. (February 12, 2017) *The "Bot Mujahideen" Telegram Channel*. International Institute for Counter-Terrorism (ICT). https://ict.org.il/the-bot-mujahideen-telegram-channel/.

3.3 Secure and enlarge the recruitment process

As reported by MEMRI, the pro-Al-Qaeda Jaysh Al-Malahim Al-Electronic Telegram channel, in July 2020, announced the beginning of a recruiting process for supporters with expertise in programming, "media raids," film montage, hacking, translation, and graphic design. Those interested were directed to contact two Telegram bots.[45]

Meanwhile, the pro-ISIS Basa'ir Da'wah Foundation, on Telegram, urged supporters specialized in graphic design, poetry, and religious studies, to join the foundation's team by contacting its bot (Ghiras11bot) on the platform.[46]

Another example regards Bahrun Naim, one of former Daesh's top Indonesian propaganda distributors and mastermind of several terrorist attacks,[47] who also established a bot on Telegram to communicate with potential Indonesian recruits. The bot was also used as a propaganda vector, greeting users with an automated message in Bahasa Indonesian and subsequently sharing messages and videos, such as interviews with militants or guides for the fabrication of homemade explosives.[48]

Regarding the recruitment, same as for propaganda, these clusters of bots were employed so that if one account were suspended, other bots from the same cluster could continue its activities.[49]

3.4 Maintain the presence of digital archives widespread and permanent

Jihadist groups are also able to deploy bots designed to ensure access to digital archives of jihadi content produced by groups and media organizations.

[45] MEMRI Cyber terrorism and jihad lab (July 20, 2020) *Pro-Al-Qaeda Media Group Directs Supporters With Expertise In Programming, Hacking, And 'Media Raids' To Contact Telegram Bots*. https://www.memri.org/cjlab/pro-al-qaeda-media-group-directs-supporters-expertise-programming-hacking-and-media-raids.

[46] Stalinsky S., Sosnow R. (August 5, 2020) *Jihadi Use Of Bots On The Encrypted Messaging Platform Telegram*. MEMRI. https://www.memri.org/reports/jihadi-use-bots-encrypted-messaging-platform-telegram#_ednref13.

[47] Gunaratna R. (October 2018) *Mastermind of Terror: The Life and Death of Bahrun Naim*. Counter Terrorist Trends and Analyses Vol. 10, No. 10. https://www.jstor.org/stable/26501459?seq=1.

[48] Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet*. HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[49] Garfield L. (14 December 2014) *ISIS has Created Thousands of Political Bots – and Hacktivistas Want You to Destroy Them*. Business Insider. https://www.businessinsider.com/anonymous-battles-isispolitical-bots-2015-12.

In this context, in 2017, Al-Shabaab's news agency, Shahada, used a bot on Telegram to share with supporters links to the group's most recent channel,[50] to keep a constant connection with its followers, even if their channel would have been suspended.[51] This strategy is used by many jihadist groups to maintain a constant information flow with their audience and quickly spread and keep track, for instance, of their latest magazine issues.

Another topical example regards Daesh's largest digital archives, nicknamed by CTC and ISD the "Cloud Caliphate,"[52] which held 97,706 folders and files, with more than 90,000 items in more than seven different languages.

This digital repository, which counted almost 10,000 unique visitors a month, curated a shared history of the movement while providing a way to continually replenish extremist content on the net.[53]

One of the ways to reach this huge library on the history and present of Daesh was thorough a cluster of pro-IS accounts that led to the discovery of the "Cloud Caliphate" aided by the 'TweetItBot' on Telegram, which also allowed users to share links directly from Telegram to Twitter. Furthermore, researchers believe the cache was tied to a digital support group named Sarh al-Khilafah, which allegedly operated a Telegram bot tasked with disseminating portions of the cache, folder-by-folder, to assure its constant presence online.

3.5 Keep in touch with supporters to encourage and improve terrorist attacks

Following the terrorist attack perpetrated with axes by two Palestinians in the Israeli city of Elad,[54] a Telegram channel, that supports Iran-backed militias, published a statement promising free weapons to residents of the

[50] MEMRI (June 30, 2017) *Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram*. https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.

[51] Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet*. HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[52] Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

[53] Silva S. (September 4, 2020) *Islamic State: Giant library of group's online propaganda discovered*. BBC News. https://www.bbc.com/news/technology-54011034.

[54] BBC (May 5, 2022) *Elad attack: Three dead in central Israeli city*. https://www.bbc.com/news/world-middle-east-61339751.

West Bank willing to perpetrate terrorist attacks against Israel. The statement reads, "Do you live in the West Bank and want a rifle or a pistol? Please note, the weapons are free of charge. Contact us via the bot. We speak Arabic and English."[55] In this case, even though the statement did not include the address of the bot, there already were several known bots associated with the channel.

3.6 From AI basics to more complex jihadist social bots

The common denominator of the above-mentioned cases is the use of bots aimed to prevent setbacks[56] by facilitating recruitment and propaganda, displaying jihadist groups' defensive posture towards potential counter-terrorism measures.

But social bots have also the potential to help terrorist groups perpetrate active actions.

In this field, DoS or DDoS attacks,[57] already appealing to cybercriminals and other malicious actors, can be launched with very little effort and their performance has a relatively considerable impact. AI is likely to be exploited to make DoS or DDoS simpler, thanks to automating processes. For instance, machine learning algorithms[58] can be used to control the botnets behind the attack or enable them to identify vulnerable systems through sophisticated network reconnaissance.

In this respect, in 2016-2017, Daesh launched a series of DDoS attacks using a DDoS tool named "Caliphate Cannon." These attacks were quite successful and targeted military, economic, and education infrastructures, displaying the seriousness of this threat and encouraging its hacking division to perpetrate similar attacks against online services.[59]

[55] MEMRI (May 8, 2022) Telegram Channel That Supports Iran-Backed Militias Offers Free Weapons To West Bank Residents To Perpetrate Terrorist Attacks. https://www.memri.org/jttm/telegram-channel-supports-iran-backed-militias-offers-free-weapons-west-bank-residents.

[56] Cox K., Marcellino W., Bellasio J., Ward A., Galai K., Meranto S., Persi Paoli G. (November 2018) *Social Media in Africa – A Double-Edged Sword for Security and Development.* United Nations Development Programme (UNDP) Regional Centre for Africa. https://www.rand.org/pubs/external_publications/EP67728.html.

[57] Denial-of-service (DoS) attack is a denial of service attack. Distributed denial-of-service (DDoS) attack is where multiple systems target a single system with a DoS attack.

[58] Machine learning is a branch of AI and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy. IBM https://www.ibm.com/cloud/learn/machine-learning.

[59] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes.* https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

Soon, jihadist groups could also rely on more sophisticated, open-source, language AI tools to generate new content and engage with users. As some studies highlighted, among others, open-source tools like GPT-2[60] could be used to post auto-generated commentary on current events, promote likeminded posts, overwhelm conversations on social media, or re-direct conversations online to match with jihadist ideological views. Using GPT-2, with existing auto-detection technology, is not always possible to distinguish human-generated extremist content from AI-generated extremist content.

Finally, AI could be used to expand one of the major aspects that allow terrorist groups, and their various support arms, to evolve online: supporter-to-supporter learning.[61] As jihadist supporters learn from each other's methods or mistakes, the spread and development of social bots could exponentially increase, in numbers and efficiency, this emulation process from supporter-to-supporter to bot-to-supporter/supporter-to-bot learning.

4. Bots exploitation to arm digital crowds

According to a report by GNET, while Daesh (and jihadist groups in general) relied heavily on bot technology, racially and ethnically motivated violent extremist networks have so far refrained from widespread bot usage, mostly because of their different objectives and the more permissive online environment in which they operate.[62]

Nevertheless, far-right or conspiracy groups' use of social bots, deriving from different purposes and environments than jihadist groups, can highlight further communication branches in which AI can be exploited.

However, this part of the analysis is not detached from the previous one dedicated to jihadist groups.

[60] "GPT-2, an open-source unsupervised language model developed by Open AI that generates coherent paragraphs of text, performs reading comprehension, machine translation, question answering, and summarization without task-specific training." Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet*. HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[61] Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

[62] Veilleux-Lepage Y., Daymon C., and Archambault E. (June 7, 2022) *Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies*. Global Network on Extremism & Technology. https://gnet-research.org/2022/06/07/learning-from-foes-how-racially-and-ethnically-motivated-violent-extremists-embrace-and-mimic-islamic-states-use-of-emerging-technologies/.

The following focus on the relation between extremist or conspiracy narratives and social bots is aimed to outline additional macro-areas of communication in which social bots can be exploited to reach malicious goals. Moreover, it doesn't exclude that also other religious, ethnically, politically motivated extremist or terrorist groups could use these declinations of social bots to fulfill their purposes.

4.1 Programmed defamation campaigns

According to the US Department of Homeland Security, social media bots can be used to harass users, overwhelming them to the point of deactivation.[63]

Harassment campaigns have long been an issue in online spaces[64] and can bring a twofold implication when perpetrated by extremist groups: reinforce their community and narratives while depriving their targets of the use of communication to defend themselves.

For instance, as reported by MEMRI, the neo-Nazi National Socialist Club's Telegram channel posted an invitation to its supporters, called "the white nationalist community" to "come together and Harass" companies whose employees "risk losing their employment" if their white supremacist and antisemitic views become known. The post suggested to act by creating bots able to "call and email these companies constantly to the point it disrupts their business and hurts their revenue."[65]

Harassing campaigns can also have the purpose of defaming targets, directly undermining their credibility or social influence. In these cases, bots can be deployed to amplify vitriolic attacks at scale.[66]

In 2017 U.S. far-right activists helped amplify a leak of hacked emails belonging to Emmanuel Macron, during its campaign for the French presi-

[63] US Department of Homeland Security (May 2018) *NATIONAL PROTECTION AND PROGRAMS DIRECTORATE – Office of Cyber and Infrastructure Analysis*. https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

[64] Geiger S.R. (2016) *Bot-based collective blocklists in Twitter: The counterpublic moderation of harassment in a networked public space*. Information, Communication, and Society 19(6). https://stuartgeiger.com/blockbots-ics.pdf.

[65] Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

[66] Nyst N., Monaco N. (2018) *STATE-SPONSORED TROLLING How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future. https://www.iftf.org/statesponsoredtrolling/.

dential election, with a disinformation campaign consisting of rumors, fake news, and forged documents. An analysis by the Atlantic Council found that, on Twitter, the hashtag #MacronLeaks reached 47,000 tweets in three and a half hours and appeared in almost half a million tweets in twenty-four hours.[67] The hashtag was first used by Jack Posobiec, an internet performer and writer for the far-right news organization The Rebel, who declared to have shared a post he saw on 4chan.[68] Researchers found that the #MacronLeaks hashtag, due to the immediate, frequent, and concentrated engagement,[69] clearly indicated the use of social bots,[70] which also helped move the hashtag from the United States to France.[71]

4.2 Support and spread polarized views and fake news

Research from the University of California analyzed the use of social bots on left-leaning tweets and right-leaning tweets during the 2020 US elections.[72] From both macro-groups, the study highlighted six major types of Twitter bots: "Astroturf: manually labeled political bots that systematically delete content; Fake follower: bots purchased to increase follower counts; Financial: bots that post using "cashtags"; Self declared: bots from botwiki.org; Spammer: accounts labeled as spambots from several datasets; Other: miscellaneous other bots obtained from manual annotation, user feedback, etc."

In particular, in the macro-group of bots that tweeted right-leaning content, researchers found also clusters of bots posting highly structured conspiracy theory-related tweets with links and references to conspiracy theories

[67] Jeangène Vilmer J. (June 2019) *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/.

[68] Volz D. (May 7, 2017) *U.S. far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers. Reuters*. https://www.reuters.com/article/us-france-election-cyber-idUSKBN1820QO.

[69] Hayden M.E. (January 29, 2021) *Twitter personality Jack Posobiec worked alongside other American far-right extremists in amplifying the fruits of an apparent Russian military intelligence (GRU) hack intended to disrupt the outcome of the French elections in May 2017*. Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2021/01/29/jack-posobiec-central-spreading-russian-intelligence-led-macronleaks-hack.

[70] Ferrara E. (August 2017) *Disinformation and social bot operations in the run up to the 2017 French presidential election*. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/8005.

[71] Southern Poverty Law Center. Jack Posobiec. https://www.splcenter.org/fighting-hate/extremist-files/individual/jack-posobiec.

[72] Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

(i.e. Qanon,[73] "gate" conspiracies as #obamagate,[74] Covid conspiracies)[75] and links to conspiracy news organizations and web sites.

These kind of bot networks are established on bots designed to post content based on the major topics discussed inside the communities they try to blend into. Once they have gained a credible profile, they can disseminate disinformation or conspiracy theories as efficiently as users' accounts.[76] This mechanism leverages the increasing tendency for users on social media to interact prevalently with like-minded groups of people. This approach tends to make fake content more and more realistic, with the risk of blurring the line between legitimate political views and extremist narratives, while attracting broader support.[77]

Furthermore, the next generation of bots will threaten to move beyond text generation to audio and video manipulation.[78] Indeed, over time, disinformation campaigns on social media are likely to be aided by deepfakes,[79] a type of fake audio or visual content that has been manipulated or generated using Generative adversarial networks[80] (GANs).[81] Deepfake has been used, for instance, to produce the fake video, entirely fabricated using AI and wi-

[73] Roose K. (September 3, 2021) *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?* The New York Times. https://www.nytimes.com/article/what-is-qanon.html.

[74] Wolfe J. (May 14, 2020) *Explainer: Trump keeps raising 'Obamagate.' What's that*? Reuters. https://www.reuters.com/article/us-usa-trump-obamagate-explainer-idUSKBN22Q1JL.

[75] Pertwee E., Simas C., and Larson H.J. (March 10, 2022) *An epidemic of uncertainty: rumors, conspiracy theories and vaccine hesitancy*. Nature. https://www.nature.com/articles/s41591-022-01728-z.

[76] Bontridder N., Poullet Y. (November 25, 2021) The role of artificial intelligence in disinformation. Cambridge University Press. https://www.cambridge.org/core/journals/data-and-policy/article/role-of-artificial-intelligence-in-disinformation/7C4BF6CA35184F149143DE968FC4C3B6#r1.

[77] Rovny J. (February 29, 2012) *Where do radical right parties stand? Position blurring in multidimensional competition*. Cambridge University Press. https://www.cambridge.org/core/journals/european-political-science-review/article/abs/where-do-radical-right-parties-stand-position-blurring-in-multidimensional-competition/69358EA1E09F6AD5B302631306AA4B16.

[78] Marcellino W., Magnuson M., Stickels A., Boudreax B., Helmus T.C., Geist E., and Winkelman Z. (2020) *Counter-Radicalization Bot Research – Using Social Bots to Fight Violent Extremism*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2705.html.

[79] CNN Business. *When seeing is no longer believing*. https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

[80] Generative adversarial networks (GANs) are algorithmic architectures that use two neural networks, pitting one against the other (thus the "adversarial") in order to generate new, synthetic instances of data that can pass for real data. They are used widely in image generation, video generation and voice generation. Pathmind. *Generative Adversarial Network Definition*. https://wiki.pathmind.com/generative-adversarial-network-gan.

[81] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The*

dely shared on social media,[82] showing Ukrainian President, Volodymyr Zelenskyy, calling on Ukrainian citizens to stop fighting Russian soldiers and surrender their weapons, also claiming he had already fled Kyiv.[83]

4.3 Promote events

Neo-Nazis and white supremacists use bots to announce and promote events, such as marches and conferences.

In June 2021 a post forwarded by a French neo-nazi channel belonging to the "Cercle des Amis d'Adolf Hitler" announced an event titled "Adolf Hitler: Une Vie, Des Valeurs" to be held in Paris. It added that those interested could use the @Cercle_Hitler_Bot to register for the event.[84]

Furthermore, extremist events can also be exploited by state-sponsored botnets to spread extremist narratives and discord.

In the aftermath of the events of the white supremacist rally in Charlottesville, Virginia, researchers found that a large number of automated bots generating Twitter posts helped make right-wing conspiracy theories, and rallying cries about Charlottesville, go viral. The analyzed social bots sample included pro-Russian accounts that were pushing content from state-controlled outlets Russia Today and Sputnik.[85] One year later, Republican Rep. Tom Garrett also claimed, in an interview with CNN,[86] that FBI officials told him that Russian-sponsored social bots were attempting to sow discord around far-right circles before the event took place.

Malicious Use Of Artificial Intelligence For Terrorist Purposes. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

[82] Atlantic Council Digital Forensic Lab (March 16, 2022) *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims.* https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

[83] Cote J. (April 1, 2022) *DEEPFAKES AND FAKE NEWS POSE A GROWING THREAT TO DEMOCRACY, EXPERTS WARN*. Northeastern. https://news.northeastern.edu/2022/04/01/deepfakes-fake-news-threat-democracy/.

[84] Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

[85] Arnsdorf I. (August 23, 2017) *Pro-Russian Bots Take Up the Right-Wing Cause After Charlottesville*. ProPublica. https://www.propublica.org/article/pro-russian-bots-take-up-the-right-wing-cause-after-charlottesville.

[86] Nobles R. (August 13, 2018) *GOP lawmaker: FBI has evidence Russian bots were fanning flames before Charlottesville violence*. CNN. https://edition.cnn.com/2018/08/13/politics/tom-garrett-russian-bots-charlottesville-violence/index.html.

5. Coordinated waves of a digital crowd

Theoretically, crowd behavior can be compared to fluid dynamics. Its density doesn't let people move forward continuously, so they need to stop and wait for another opportunity to advance, generating "stop-and-go waves."[87] In these terms, digital crowds' behavior should also be better analyzed and understood because, even though they are physically dispersed, they can be considered as a collectively intelligent complex system, with unlimited growth.[88]

Uncontrolled exposure to extremist narratives or disinformation can have an impact on collective behavior and "when perturbed, complex systems tend to exhibit finite resilience followed by catastrophic, sudden, and often irreversible changes,"[89] similarly to stop-and-go waves.

Social bots can help coordinate the extent of these waves but is still not clear how much the manipulation of digital crowds can reverberate in real life or policymaking.[90] Indeed, existing research extensively studied bot detection, but bot coordination is still emerging and still requires more in-depth analysis.[91]

Even though who is running social bots is not always detectable, as bots can be exploited either for provocative campaigns or as part of an information war[92] while conspiracies or extremist contents tend to follow current events even when there aren't coordinated campaigns,[93] recurring patterns on the to-

[87] Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

[88] Aradu C., Blank T. (2014) *The Politics of digital crowds*. Lo s uaderno Q, vol. 33. https://www.academia.edu/9989238/The_Politics_of_digital_crowds.

[89] Holtz J. (June 14, 2021) *Communication technology, study of collective behavior must be 'crisis discipline,' researchers argue*. University of Washington. https://www.washington.edu/news/2021/06/14/communication-technology-study-of-collective-behavior-must-be-crisis-discipline-researchers-argue/.

[90] Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

[91] Khaund T., Kirdemir B., Agarwal N., Liu H., Morstatter F. (August 19, 2021) Social Bots and Their Coordination During Online Campaigns: A Survey. IEEE Transactions on Computational Social Systems. https://ieeexplore.ieee.org/document/9518390.

[92] Cantini R., Marozzo F., Talia D., and Trunfio P. (January 4, 2022) *Analyzing Political Polarization on Social Media by Deleting Bot Spamming*. Special Issue – Big Data and Cognitive Computing: 5th Anniversary Feature Papers. https://www.mdpi.com/2504-2289/6/1/3.

[93] Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

pics and languages used by botnets coordinated activities can still be detected and should be better analyzed.

For instance, some cases represent a coordinated shift of social bots to different stories; coordinated attempts to expand and actualize disinformation or extremist narratives to follow an agenda, pushing new topics, new terms, and hashtags in the social media environment.

In this respect, a study on bots and misinformation on Covid analyzed social bot tweets from January 2020 to August 2020. Some of these bots, identified between 2011 and 2019, were discovered before the pandemic and were originally designed for non-COVID-19 purposes, such as promoting product hashtags, retweeting political candidates, and spreading links to malicious content.[94]

Other researchers found that, in the wake of Russia's invasion of Ukraine, online activity on Twitter surged by nearly 20%. The analysis highlighted that ethnically motivated extremist accounts, such as those posting content on New World Order (NWO) conspiracy,[95] shifted from topics related to Covid, a secret group controlling the global economy, and speculations about the end times,[96] almost entirely into Ukraine and Putin themes.[97]

Understanding the exploitation of botnets could help increase public awareness and avoid users, and public figures, from involuntarily becoming echo chambers for malicious social bots clusters. This could be a valuable tool to prevent either state or non-state malicious actors from generating unpredictable waves of digital crowds at their advantage.

These are not marginal aspects, because, as explained by the above-mentioned theory on crowd behavior and fluid dynamics: even though waves do not always portend a collapse, the stop-and-go wave can also be a warning signal for the situation in the crowd to become critical.[98]

[94] McKenzie H., Giorgi S., Devoto A., Rahman M., Ungar L., Schwartz H.A., EpsteinD.H., Leggio L., and Curtis B. (May 20, 2021) *Bots and Misinformation Spread on Social Media: Implications for COVID-19*. Journal of Medical Internet Research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8139392/.

[95] Flores M. (May 30, 2022) *The New World Order: The Historical Origins of a Dangerous Modern Conspiracy Theory*. Middlebury Institute of International Studies at Monterey. https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/new-world-order-historical-origins-dangerous.

[96] Barkun M. (May 2012) *Culture of Conspiracy: Apocalyptic Visions in Contemporary America*. California Scholarship Online.

[97] NCRI insight report (March 1, 2022) *New World Order Conspiracy Theories and Anti-Nato Rhetoric Surging on Twitter Amid Russian Invasion of Ukraine*. https://networkcontagion.us/wp-content/uploads/NCRI-Insights-SitRep-March-2022.pdf.

[98] Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-

References

Accenture (June 17, 2022) *The unreal – making synthetic, authentic*. https://www.accenture.com/th-en/insights/health/unreal-making-synthetic-authentic.

Accenture (March 16, 2022) *Technology Vision 2022: "Metaverse Continuum" Redefining How the World Works, Operates and Interacts*. https://newsroom.accenture.com/subjects/metaverse/accenture-technology-vision-2022-metaverse-continuum-redefining-how-the-world-works-operates-and-interacts.htm.

Allyn B. (May 20, 2020) *Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots*. NPR. https://www.npr.org/sections/coronavirus-live-updates/2020/05/20/859814085/researchers-nearly-half-of-accounts-tweeting-about-coronavirus-are-likely-bots?t=1655890800628.

Antinori A. (April 10, 2017) *The "Jihadi Wolf" Threat*. Europol. https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf.

Aradu C., Blank T. (2014) *The Politics of digital crowds*. Lo s uaderno Q, vol. 33. https://www.academia.edu/9989238/The_Politics_of_digital_crowds.

Arnsdorf I. (August 23, 2017) *Pro-Russian Bots Take Up the Right-Wing Cause After Charlottesville*. ProPublica. https://www.propublica.org/article/pro-russian-bots-take-up-the-right-wing-cause-after-charlottesville.

Assenmacher D., Clever L., Frischlich L., Quandt T., Trautmann H., and Grimme C. (September 1, 2020) *Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*. Social media and Society. https://journals.sagepub.com/doi/10.1177/2056305120939264.

Atlantic Council Digital Forensic Lab (March 16, 2022) *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

Barak M. (February 12, 2017) *The "Bot Mujahideen" Telegram Channel*. International Institute for Counter-Terrorism (ICT). https://ict.org.il/the-bot-mujahideen-telegram-channel/.

Barkun M. (May 2012) *Culture of Conspiracy: Apocalyptic Visions in Contemporary America*. California Scholarship Online.

Bartlett R., Morse A., Stanton R., and Wallace N. (June 2019) *Consumer-Lending Discrimination in the FinTech Era*. National Bureau of Economic Research. https://www.nber.org/papers/w25943#:~:text=FinTech%20algorithms%20also%20discriminate%2C%20but,borrowers%20on%20low%2Dshopping%20behavior.

about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

Bastos M.T., Mercea D. (2017) *The Brexit Botnet and UserGenerated Hyperpartisan News*. Social Science Computer Review. https://journals.sagepub.com/doi/10.1177/0894439317734157.

BBC (May 5, 2022) *Elad attack: Three dead in central Israeli city*. https://www.bbc.com/news/world-middle-east-61339751.

Berger J.M. (June 16, 2014) *How ISIS Games Twitter.* The Atlantic. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

Bontridder N., Poullet Y. (November 25, 2021) The role of artificial intelligence in disinformation. Cambridge University Press. https://www.cambridge.org/core/journals/data-and-policy/article/role-of-artificial-intelligence-in-disinformation/7C4BF6CA35184F149143DE968FC4C3B6#r1.

Botometer https://botometer.osome.iu.edu/.

Cantini R., Marozzo F., Talia D., and Trunfio P. (January 4, 2022) *Analyzing Political Polarization on Social Media by Deleting Bot Spamming*. Special Issue – Big Data and Cognitive Computing: 5th Anniversary Feature Papers. https://www.mdpi.com/2504-2289/6/1/3.

Castellanos S. (July 23, 2021) *Fake It to Make It: Companies Beef Up AI Models With Synthetic Data*. Wall Street Journal. https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601.

Chen W., Pacheco D., Yang K., Menczer F. (September 22, 2021) *Neutral bots probe political bias on social media*. Nature. https://www.nature.com/articles/s41467-021-25738-6.

Ciancaglini V., Gibson C., Sancho D., Amann P., Klayn A., McCarthy O., and Eira M. (November 19, 2020). *Malicious Uses and Abuses of Artificial Intelligence. Trend Micro*. EUROPOL and UNICRI. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf.

CITS *How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting*. https://www.cits.ucsb.edu/fake-news/spread.

Cloudfare. *What is a social media bot? | Social media bot definition*. https://www.cloudflare.com/it-it/learning/bots/what-is-a-social-media-bot/#:~:text=Experts%20who%20have%20applied%20logarithms,designed%20to%20mimic%20human%20accounts.

CNN Business. *When seeing is no longer believing*. https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

Cote J. (April 1, 2022) *DEEPFAKES AND FAKE NEWS POSE A GROWING THREAT TO DEMOCRACY, EXPERTS WARN*. Northeastern. https://news.northeastern.edu/2022/04/01/deepfakes-fake-news-threat-democracy/.

Cox K., Marcellino W., Bellasio J., Ward A., Galai K., Meranto S., Persi Paoli G. (November 2018) *Social Media in Africa – A Double-Edged Sword for Security and Development*. United Nations Development Programme (UNDP) Regional Centre for Africa. https://www.rand.org/pubs/external_publications/EP67728.html.

European Commission (June 16, 2022) *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3664.

European Commission (June 16, 2022) *Signatories of the 2022 Strengthened Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

European Commission *2018 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

European Commission *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

Ferrara E. (August 2017) *Disinformation and social bot operations in the run up to the 2017 French presidential election*. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/8005.

Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

Flores M. (May 30, 2022) *The New World Order: The Historical Origins of a Dangerous Modern Conspiracy Theory*. Middlebury Institute of International Studies at Monterey. https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/new-world-order-historical-origins-dangerous.

Forsbak Ø. (March 25, 2022) *Six AI Trends To Watch In 2022*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/03/25/six-ai-trends-to-watch-in-2022/?sh=3e1c36e62be1.

Garfield L. (14 December 2014) *ISIS has Created Thousands of Political Bots – and Hacktivistas Want You to Destroy Them*. Business Insider. https://www.businessinsider.com/anonymous-battles-isispolitical-bots-2015-12.

Geiger S.R. (2016) *Bot-based collective blocklists in Twitter: The counterpublic moderation of harassment in a networked public space*. Information, Communication, and Society 19(6). https://stuartgeiger.com/blockbots-ics.pdf.

Guesmi H. (January 27, 2021) *The social media myth about the Arab Spring*. AlJazeera. https://www.aljazeera.com/opinions/2021/1/27/the-social-media-myth-about-the-arab-spring.

Gunaratna R. (October 2018) *Mastermind of Terror: The Life and Death of Bahrun Naim*. Counter Terrorist Trends and Analyses Vol. 10, No. 10. https://www.jstor.org/stable/26501459?seq=1.

Harvard special edition: *Artificial Intelligence*. https://sitn.hms.harvard.edu/special-edition-artificial-intelligence/.

Hayden M.E. (January 29, 2021) *Twitter personality Jack Posobiec worked alongside other American far-right extremists in amplifying the fruits of an apparent Russian military intelligence (GRU) hack intended to disrupt the outcome of the French elections in May 2017*. Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2021/01/29/jack-posobiec-central-spreading-russian-intelligence-led-macronleaks-hack.

Holtz J. (June 14, 2021) *Communication technology, study of collective behavior must be 'crisis discipline,' researchers argue*. University of Washington. https://www.washington.edu/news/2021/06/14/communication-technology-study-of-collective-behavior-must-be-crisis-discipline-researchers-argue/.

IBM *Application Programming Interface (API)*. https://www.ibm.com/cloud/learn/api.

IBM *Machine learning*. https://www.ibm.com/cloud/learn/machine-learning.

ICT Cyber Desk (December 2016) *Cyber-Terrorism Activities Report No. 19*. International Institute for Counter-Terrorism (ICT).

ISIS watch on Telegram https://t.me/ISISwatch/1049.

Jeangène Vilmer J. (June 2019) *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/.

Khaund T., Kirdemir B., Agarwal N., Liu H., Morstatter F. (August 19, 2021) Social Bots and Their Coordination During Online Campaigns: A Survey. IEEE Transactions on Computational Social Systems. https://ieeexplore.ieee.org/document/9518390.

Kilcher Y. (June 3, 2022) *This is the worst AI ever*. YouTube. https://www.youtube.com/watch?v=efPrtcLdcdM.

Kingsley P. (June 23, 2014) *Who is behind Isis's terrifying online propaganda operation?* The Guardian. https://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq.

Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

Liu X. (April 2019) A *big data approach to examining social bots on Twitter*. Journal of Services Marketing. https://www.researchgate.net/publication/332331554_A_big_data_approach_to_examining_social_bots_on_Twitter.

Marcellino W., Magnuson M., Stickels A., Boudreax B., Helmus T.C., Geist E., and Winkelman Z. (2020) *Counter-Radicalization Bot Research – Using Social Bots to Fight Violent Extremism*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2705.html.

McKenzie H., Giorgi S., Devoto A., Rahman M., Ungar L., Schwartz H.A., EpsteinD.H., Leggio L., and Curtis B. (May 20, 2021) *Bots and Misinformation Spread on Social Media: Implications for COVID-19*. Journal of Medical Internet Research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8139392/.

MEMRI (June 30, 2017) *Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram*. https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.

MEMRI (May 8, 2022) Telegram Channel That Supports Iran-Backed Militias Offers Free Weapons To West Bank Residents To Perpetrate Terrorist Attacks. https://

www.memri.org/jttm/telegram-channel-supports-iran-backed-militias-offers-free-weapons-west-bank-residents.

MEMRI Cyber terrorism and jihad lab (July 20, 2020) *Pro-Al-Qaeda Media Group Directs Supporters With Expertise In Programming, Hacking, And 'Media Raids' To Contact Telegram Bots*. https://www.memri.org/cjlab/pro-al-qaeda-media-group-directs-supporters-expertise-programming-hacking-and-media-raids.

Meta, Community Standards Enforcement Report – Q1 2022 report. https://transparency.fb.com/data/community-standards-enforcement/?source=https%3A%2F%2Ftransparency.facebook.com%2Fcommunity-standards-enforcement.

Natural Language Processing (NLP) SAS. https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html.

NCRI insight report (March 1, 2022) *New World Order Conspiracy Theories and Anti-Nato Rhetoric Surging on Twitter Amid Russian Invasion of Ukraine*. https://networkcontagion.us/wp-content/uploads/NCRI-Insights-SitRep-March-2022.pdf.

Nobles R. (August 13, 2018) *GOP lawmaker: FBI has evidence Russian bots were fanning flames before Charlottesville violence*. CNN. https://edition.cnn.com/2018/08/13/politics/tom-garrett-russian-bots-charlottesville-violence/index.html.

Nyst N., Monaco N. (2018) *STATE-SPONSORED TROLLING How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future. https://www.iftf.org/statesponsoredtrolling/.

Pathmind. *Generative Adversarial Network Definition*. https://wiki.pathmind.com/generative-adversarial-network-gan.

Pertwee E., Simas C., and Larson H.J. (March 10, 2022) *An epidemic of uncertainty: rumors, conspiracy theories and vaccine hesitancy*. Nature. https://www.nature.com/articles/s41591-022-01728-z.

PR Newswire (June 13, 2022) *Artificial Intelligence Market USD 1,581.70 Billion By 2030, Growing At A CAGR of 38.0%*. Bloomberg press release. https://www.bloomberg.com/press-releases/2022-06-13/artificial-intelligence-market-usd-1-581-70-billion-by-2030-growing-at-a-cagr-of-38-0-valuates-reports#:~:text=Artificial%20Intelligence%20Market%20USD%201%2C581.70,38.0%25%20%2D%20Valuates%20Reports%20%2D%20Bloomberg.

Roach S. (December 7, 2021) *3 TIMES BOTS HAVE IMPACTED MAJOR WORLD EVENTS*. Natacea. https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/.

Roberts S. (June 16, 2020) *Who's a Bot? Who's Not?*. The New York Times. https://www.nytimes.com/2020/06/16/science/social-media-bots-kazemi.html.

Roose K. (September 3, 2021) *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?* The New York Times. https://www.nytimes.com/article/what-is-qanon.html.

Rovny J. (February 29, 2012) *Where do radical right parties stand? Position blurring in multidimensional competition*. Cambridge University Press. https://www.cambridge.org/core/journals/european-political-science-review/article/abs/where-do-radical-right-parties-stand-position-blurring-in-multidimensional-competition/69358EA1E09F6AD5B302631306AA4B16.

Savage M. (June 29, 2019) *How Brexit party won Euro elections on social media – simple, negative messages to older voters*. The Guardian. https://www.theguardian.com/politics/2019/jun/29/how-brexit-party-won-euro-elections-on-social-media.

Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

Silva S. (September 4, 2020) *Islamic State: Giant library of group's online propaganda discovered*. BBC News. https://www.bbc.com/news/technology-54011034.

Southern Poverty Law Center. Jack Posobiec. https://www.splcenter.org/fighting-hate/extremist-files/individual/jack-posobiec.

Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

Stalinsky S., Sosnow R. (August 5, 2020) *Jihadi Use Of Bots On The Encrypted Messaging Platform Telegram*. MEMRI. https://www.memri.org/reports/jihadi-use-bots-encrypted-messaging-platform-telegram#_ednref13.

Terrence A. (June 2017) AI-Powered Social Bots. https://www.researchgate.net/publication/317650425_AI-Powered_Social_Bots.

The Economic Times (November 30, 2021) *Arab Spring: The first smartphone revolution*. https://economictimes.indiatimes.com/news/international/saudi-arabia/arab-spring-the-first-smartphone-revolution/articleshow/79487524.cms.

The Economist (May 6, 2017) *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Towes R. (June 12, 2022) *Synthetic Data Is About To Transform Artificial Intelligence*. Forbes. https://www.forbes.com/sites/robtoews/2022/06/12/synthetic-data-is-about-to-transform-artificial-intelligence/?sh=5e6a76c07523.

United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

US Department of Homeland Security (May 2018) *NATIONAL PROTECTION AND PROGRAMS DIRECTORATE – Office of Cyber and Infrastructure Analysis*. https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

Veilleux-Lepage Y., Daymon C., and Archambault E. (June 7, 2022) *Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies*. Global Network on Extremism & Technology. https://gnet-research.org/2022/06/07/learning-from-foes-how-racially-and-ethnically-motivated-violent-extremists-embrace-and-mimic-islamic-states-use-of-emerging-technologies/.

Volz D. (May 7, 2017) *U.S. far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers. Reuters.* https://www.reuters.com/article/us-france-election-cyber-idUSKBN1820QO.

Vosoughi S., Roy D., and Aral S. (March 9, 2018) *The spread of true and false news online*. Science. https://www.science.org/doi/10.1126/science.aap9559.

Wolfe J. (May 14, 2020) *Explainer: Trump keeps raising 'Obamagate.' What's that?* Reuters. https://www.reuters.com/article/us-usa-trump-obamagate-explainer-idUSKBN22Q1JL.

Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet.* HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

Questo volume è stato stampato
nel mese di dicembre 2022
su materiali e con tecnologie ecocompatibili
presso la LITOGRAFIA SOLARI
Peschiera Borromeo (MI)

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-041-9

Euro 20,00