Social Bots and Their Coordination During Online Campaigns: A Survey

Tuja Khaund, Baris Kirdemir, Nitin Agarwal, *Member, IEEE*, Huan Liu, *Fellow, IEEE*, and Fred Morstatter

***Abstract*— Online social networks (OSNs) are a major component of societal digitalization. OSNs alter how people communicate, make decisions, and form or change their beliefs, attitudes, and behaviors. Thus, they can now impact social groups, financial systems, and political communication at scale. As one type of OSN, social media platforms, such as Facebook, Twitter, and YouTube, serve as outlets for users to convey information to an audience as broad or targeted as the user desires. Over the years, these social media platforms have been infected with automated accounts, or bots, that are capable of hijacking conversations, influencing other users, and manipulating content dissemination. Although benign bots exist to facilitate legitimate activities, we focus on bots designed to perform malicious acts through social media platforms. Bots that mimic the social behaviors of humans are referred to as social bots. Social bots help automate sociotechnical behaviors, such as "liking" tweets, tweeting/retweeting a message, following users, and coordinating with or even competing against other bots. Some advanced social bots exhibit highly sophisticated traits of coordination and communication with complex organizational structures. This article presents a detailed survey of social bots, their types and behaviors, and how they impact social media, identification algorithms, and their coordination strategies in OSNs. The survey also discusses coordination in areas such as biological systems, interorganizational networks, and coordination games. Existing research extensively studied bot detection, but bot coordination is still emerging and requires more in-depth analysis. The survey covers existing techniques and open research issues on the analysis of social bots, their behaviors, and how social network theories can be leveraged to assess coordination during online campaigns.**

***Index Terms*— Bot detection, coordination, online social networks (OSNs), social bots, social media, social network analysis (SNA).**

I. Introduction

ONLINE social networks (OSNs) are dynamic social interaction platforms with billions of users worldwide. They attract everyone regardless of their age, gender, socioeconomic status, and so on and produce a tremendous amount of digital data for analysis [1]. The number of OSN users is increasing every year. According to the Pew Research Center's survey report in [2], 65% of adult Americans use at least one social networking site. Information is rapidly disseminated among these users through online social interactions. The interactions among OSN users generate a huge volume of data that provide the opportunity to study human behavioral patterns [3]. An in-depth investigation of OSNs is important to enhance the understanding of the social and behavioral dynamics, as well as addressing pressing societal issues.

A social network (SN) is generally conceptualized as graphs, for which vertices represent users and edges represent relationships among them. Social network analysis (SNA) is a field that leverages existing methods of graph theory, data mining, and machine learning to analyze social phenomena [4]. It provides both visual and mathematical representations of human-influenced relationships, where the patterns or regularities in relationships among interacting agents in a social environment can be studied [5]. SNA can facilitate a multitude of goals, such as understanding the relations (edges) between the actors (vertices), such as interaction during an event, identifying trending hashtags, detecting fake accounts, learning the sentiments of users, and discovering hidden communities. Events and campaigns on OSNs gain momentum when a large audience is engaged in discussion. Users use hashtags to either promote or criticize them.

Over the years, foreign interference has infiltrated political events [6] to increase polarization; the increasing amount of bots spreading disinformation/misinformation has also caused havoc in several countries [7]–[9]. Bots are highly capable of manipulating public opinion, and existing literature shows

Manuscript received October 1, 2020; revised May 26, 2021; accepted July 24, 2021. Date of publication August 19, 2021; date of current version April 1, 2022. This work was supported in part by the U.S. National Science Foundation under Grant OIA-1946391, Grant OIA-1920920, Grant IIS-1636933, Grant ACI-1429160, and Grant IIS-1110868; in part by the U.S. Office of Naval Research under Grant N00014-10-1-0091, Grant N00014-14-1-0489, Grant N00014-15-P-1187, Grant N00014-16-1-2016, Grant N00014-16-1-2412, Grant N00014-17-1-2675, Grant N00014-17-1-2605, Grant N68335-19-C-0359, Grant N00014-19-1-2336, Grant N68335-20-C-0540, and Grant N00014-21-1-2121; in part by the U.S. Air Force Research Laboratory; in part by the U.S. Army Research Office under Grant W911NF-20-1-0262 and Grant W911NF-16-1-0189; in part by the U.S. Defense Advanced Research Projects Agency under Grant W31P4Q-17-C-0059; in part by the Arkansas Research Alliance; in part by the Jerry L. Maulden/Entergy Endowment at the University of Arkansas at Little Rock; and in part by the Australian Department of Defense Strategic Policy Grants Program (SPGP) under Award 2020-106-094. *(Corresponding author: Tuja Khaund.)*

Tuja Khaund is with Walmart Inc., Bentonville, AR 72719 USA (e-mail: tuja.khaund@walmart.com).

Baris Kirdemir and Nitin Agarwal are with the Department of Information Science, University of Arkansas at Little Rock, Little Rock, AR 72204 USA (e-mail: bkirdemir@ualr.edu; nxagarwal@ualr.edu).

Huan Liu is with the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ 85281 USA (e-mail: huan.liu@asu.edu).

Fred Morstatter is with the Information Sciences Institute, University of Southern California, Los Angeles, CA 90272 USA (e-mail: morstatt@usc.edu).

Digital Object Identifier 10.1109/TCSS.2021.3103515

how it has negatively affected political discussion rather than improving it [10]. Researchers suspect an organized crime, and a few studies have shown traces of coordinated bot behavior [11]. Recently, bots also played a major role during the ongoing pandemic related to Covid-19 across multiple social media platforms [12]–[14]. Therefore, it is crucial to understand what bots are, what they are capable of, and how they coordinate with other bots or humans during online campaigns.

Coordination has been extensively studied by researchers across various disciplines, such as organization theory, management science, computer science, economics, and psychology. Malone [15] emphasized the need for an articulated definition and theory of coordination. He stated that, often, "good coordination is nearly invisible, and we, sometimes, notice coordination most clearly when it is lacking" [15], [16]. In this work, we adopt the definition that coordination is "the additional information processing performed when multiple, connected actors pursue goals that a single actor pursuing the same goals would not perform" [15] or the process of "managing dependencies between activities" [16].

A. Motivation

SNs can provide insights at various levels of granularity, from studying the dynamics of small groups to international relations. They provide ways to solve problems, run organizations, and show the degree to which individual actors successfully reach their goals [17]. SNAs can promote knowledge-sharing and assist in evaluating the performance of individuals, groups, or entire networks [17]. Effective investigation of networks helps researchers to identify properties, such as strength and direction of network relationships among actors [18], [19]. Bradshaw and Howard [20] monitored and reported how government and political parties organize trends to manipulate social media on a global scale. They presented evidence of computational propaganda in 70 countries in 2019, up from 48 countries in 2018, and 28 countries in 2017. They also listed the evolving tools, capacities, strategies, and resources used in organized social media manipulation campaigns. At least one political party or government agency used social media to domestically influence public opinion in each country. These organizations collaborate with youth groups, social media influencers, volunteers, and fake accounts to mold public opinion, set political agendas, and disseminate information. The report stated that around 87% of the countries used human accounts, 80% of the countries used bots, 11% of the countries used cyborg accounts combining automation with human activity, and 7% of countries used hacked or stolen accounts [20]. This study aims to connect all these attributes vis-à-vis the analysis and measure coordination of actors in a network that participates in influence campaigns on social media.

Sections II–V will elaborate on bots and botnets, their types, their impact, various detection methods, and some of the coordination strategies observed by researchers. We further explore disciplines, where coordination has been studied, and try to leverage some of the theories and metrics used to evaluate coordination on social media during information campaigns. Since social media consists of connections in the form of networks, we explore various SN measures that may be helpful in assessing coordination.

TABLE I
BOT TERMINOLOGY

Terminology	Definition
Bot	A computer application designed to perform automated tasks over the Internet.
Cyborg	A human leveraging bots to automate tasks such as posting content on social media platforms faster, longer and more frequently.
Social Bot	Bots that mimic social behaviors of humans.
Botnet	A network of bots created to coordinate with each other.

II. IDENTIFYING BOTS AND BOT BEHAVIORS

To uncover and understand manipulation in OSNs, the first task is to identify bots and botnets. It is crucial to understand why they are created and what roles they play inside a botnet, or an OSN. Once their purpose is recognized, the next step is to identify tactics that reveal sophisticated bot behaviors.

A. Understanding Bots and Botnets

A bot is created to run simple, structurally repetitive tasks at a rate much higher than humans. In Table I, we define some of the popular terms that are often associated with bots.

Boshmaf *et al.* [21], [22] revealed how adversaries can invade OSNs by deploying social bots at a large scale. Social bots have various capabilities [23]. They learn the social graph to analyze user's posts and decide ways to communicate and affect their perceived influence. These capabilities enabled social bots to affect public discourse in online spaces, such as social media and chat forums.[1] For the past few years, social bots have populated social media platforms [24], [25] as statistics reveal their presence in more than 50% of Twitter space. The Imperva Incapsula Bot Traffic Report shows that nearly half of the Internet is made up of bots.[2] SN administrators are aware of such harmful bots, and their algorithms are successfully detecting and suspending them. One study estimated that Twitter has suspended 28% of its accounts created in 2008 and about half created in 2014 [26]. However, researchers are still struggling to understand the role that these bots play in facilitating malicious activities. In one study [27], 1 45 000 accounts were found undetected. Today, 16% of spammers on Twitter are bots. Not all bots are created to be harmful, which is why it is important to distinguish between good and bad bots in this era of hyperconnectivity.

B. Types of Bots and Their Behaviors

Social bots could appear as entertainment bots, spam bots, influence bots, and so on. Table II lists a few types based on

[1] @DFRLab: Le Pen's (Small) Online Army (2017).
[2] 2017. Bot Traffic Report 2016 | Imperva. Blog.

TABLE II
BOT TYPES BASED ON THEIR PURPOSE

Bot Type	Definition
Propaganda Bot	Bots that sway political opinion often by drowning dissenting opinions.
Influence Bot	Bots designed to influence behavior or opinion.
Promotional Bot	Digital marketing bots designed for seamless customer experience.
Spam Bot	Bots that send spam to other users.
Hackers	Bots designed to distribute malware, attack websites, and sometimes entire networks.
Chat Bot	Bots designed to conduct conversations with humans via auditory or text-based methods.
News Bot	Bots facilitate news dissemination, often via push notifications, including content such as breaking news stories.

TABLE III
SOPHISTICATED BOT BEHAVIORS

Behavior	Definition
Mimicry	Social bots mimicking human behavior on social networks to remain unnoticed and improve their chances of influencing the social graph.
Misdirection	Social bots try to get their audience to interact with unrelated content while pushing its narrative such as posting irrelevant tweets with a pro-narrative hashtag.
Smoke Screening	Social bots serve as a smoke screen to provide cover for obscure activity during botnet campaigns as it infiltrates the social graph with unrelated content.
Hashtag Latching	Social bots associate trending hashtags to their narrative to get a bigger crowd exposure.
Thread-Jacking	Social bots alter discussion in a comments thread by interjecting unrelated topics.
Reverberation	Social bots retweet and amplify selected tweets to reach a larger audience.

their various roles. News bots, promotional bots, and suicide helpline bots are benign bots that do not pose a threat to society. Influence bots, on the other hand, are automated accounts that attempt to affect or influence user behavior with whom they interact [28]. For the rest of the study, we will emphasize malicious social bots that are intended for misuse of OSNs.

Social bots often become consistent and highly active during political campaigns, international crises, significant geopolitical events, and conflicts. Abokhodair *et al.* [29] analyzed the life and the activities of "Syrian Social Bots" (SSBs) used throughout the Syrian civil war. They identified bots based on their shared content, such as news articles and conversational tweets, than the average Twitter legitimate users [11]. Here, we propose a simple taxonomy that leverages existing literature to classify bots based on their position in the SN.

1) *Core Bots:* Social bots that comprise the central core of a botnet. These bots are strongly connected, and they are in charge of generating content. The content is then spread with the help of other bots that lay in the periphery of the botnet.
2) *Peripheral Bots:* Twitter accounts that are being lured to participate in the dissemination process. Their task is to retweet one or more of the tweets generated by core bots 11], [30].

All bots are designed for a specific purpose, and they can exhibit several behaviors that are sophisticated enough to reach their ultimate goal. As existing literature suggests, Table III lists some of the popular social bot behaviors [29].

The majority of the listed bot behaviors can be detected through textual or SNA where researchers explore the content published by users on Twitter or YouTube. Al-Khateeb and Agarwal [11] observed several sophisticated bot behaviors and confirmed the existence of core and peripheral bots suggested by Abokhodair *et al.* [29]. Khaund *et al.* [31] also observed the above core and peripheral network structures in their bot SN while analyzing bot and human behaviors during the 2017 natural disasters event on Twitter. They also identified bots amplifying the spread of misinformation and hoaxes about "sharks on highway" through the various shared hashtags. Alternate narratives were also present where bots latched unrelated hashtags (Nuclear Test, Kim Jong Un, the demise of Israel, and so on) onto the trending ones to attract more views. Humans, on the other hand, shared more generic hashtags and maintained diverse social relationships. Luceri *et al.* [32] analyzed the characteristics of bots and humans during the 2016 and 2018 U.S. elections by comparing the volume and temporal dynamics of their shared activity, while, in 2016, bots and humans tweeted differently; in 2018, however, activity trends of bots aligned with humans. Their study confirmed the hypothesis of bots evolving to be more sophisticated around humans. The usages of retweets have reduced tremendously, both from humans and bots. Humans increased the volume of replies, discussing their opinion instead of simply resharing previously generated content. This change is beneficial since the spread of low-credibility content was associated with indiscriminate resharing [10], [33], [34] during the 2016 U.S. presidential election.

Mimicry is one of the most challenging bot behaviors that current research is trying to address by analyzing individual user patterns. Stine *et al.* [35] and Stine and Agarwal [36] explored the information foraging behavior of bots based on the change in the usage of vocabulary in their tweets over time. Their work presented potential bot behavior as follows.

1) *Explorative:* Bots that write about different sets of topics every day and their surprise in word usage patterns will be high resulting in explorative information foraging behavior.
2) *Exploitative:* Bots sharing content with a focused purpose on a day-to-day basis using a focused vocabulary result in low surprise in their word usage patterns.

Stine and Agarwal [36] argue that these are a range of behaviors that bots show, and such a behavioral profile can be built for Twitter accounts. Their work does not treat bot identification as a binary classification problem to check whether an account is a bot or not. Instead, they go deeper into characterizing these specific bot behaviors through which one can assert whether a bot is more explorative or exploitative

and at what point such behavioral transition takes place. These approaches will not only advance the behavioral bot identification technologies but also allow users to understand bot behavior more thoroughly.

Sophisticated bot behaviors can have a major impact on various online social media platforms and on society. Section III will discuss some of the domains where bots have manifested themselves as credible users to manipulate the opinions of people on social media.

III. Impact of Bots on Social Media

An increasing number of cases have been reported by researchers and journalists, among others, about the large-scale deployment of malicious social bots and the potential damages that they can do to society [37]. Evidence shows how social bots manipulate social media discourse with fake news, spam, misinformation, and so on to distract users from actual facts. Social bots constantly evolve to bypass detection tools and algorithms to appear legitimate to humans. The fake followers' market is thriving as celebrities and social media influencers are accused of purchasing bots to appear more popular. Prominent political figures have allegedly acquired such bots in the U.S. and worldwide to promote their agenda. Content analysis of the 35-week old Twitter Syrian social botnet revealed that social bots have now stopped mimicking humans and are misleading users to irrelevant content [29].

Bot activity has been reported in several domains, with the potential to affect behaviors, opinions, and choices. Health is one domain of particular concern [38], where social bots influenced polarized opinion about vaccination policies [37], [39] and smoking [40], [41], as well as the ongoing pandemic due to Covid-19 [42]. Politics is another key domain [43]. Researchers warned about bots potentially abusing the social media ecosystem for political propaganda a decade ago [44], [45]. During the 2010 U.S. midterm elections, naive social bots were deployed to show support to some candidates while attacking their opponents [46], misdirecting thousands of tweets to websites with misinformation [3]. During the 2016 U.S. presidential election, social bots were found distorting online conversations with large volumes of content. Bessi and Ferrara [10] suggested that amplifying information in the form of retweets can be dangerous as it was hard to differentiate whether humans are resharing content produced by other humans or bots. In fact, humans and bots retweeted each other at the same rate, suggesting that bots effectively reshared their content in human communication channels. The authors further explored how bots and humans discussed the two presidential candidates and found that bots were tweeting positively in support of Donald Trump [10]. Hagen *et al.* [47] demonstrated that coordinated swarms of social bots distorted the social media conversation during the investigation "into Russian interference in the 2016 U.S. elections." Bots producing more positive content in support of a candidate can trick individuals exposed to this content into believing that there exists organic, grassroots support, while, in reality, it is all fabricated.

Similar cases of political manipulation were reported in other countries [48], [49]. Suárez-Serrato *et al.* [50] studied the influence of social bots during the 2014 protest in Mexico based on the hashtag #YaMeCanse, which translates to "I am tired." On November 7, 2014, the Mexican Federal District Attorney, Jesús Murillo Karam, prompted the words "Ya me canse." to one of his aides toward the end of a press conference. This press conference was to notify citizens of the status of an ongoing investigation into the disappearance of 43 teachers in training from the rural school in Ayotzinapa, Guerrero, on September 26, 2014. To date, this gesture of fatigue has been identified as the largest use of a protest hashtag on Twitter in Mexico. During the 2017 French Presidential Election, Ferrara [8] analyzed tweets related to candidates Marine Le Pen and Emmanuel Macron in time for the election and found traces of 18 000 bots actively pushing the famous "MacronLeaks" disinformation campaign. U.S.-based alt-right users and alternative news media are mostly engaged in conversation with these bots, rather than French users. The study also found hundreds of the same bots actively engaged during the 2016 U.S. Election. This suggests the existence of a dark market for reusable political disinformation bots.

Social bots have been used to promote terrorist propaganda and violent extremism. By analyzing a sample of 20 000 Islamic State supporting accounts, Berger *et al.* [51] found that the terrorist organization was actively using social media and bots to spread its ideology. Abokhodair *et al.* [29] dissected a social botnet misdirecting online discussions during the Syrian civil war in 2012 on Twitter. The majority of these studies were conducted on Twitter bots. However, social bots exist outside of Twitter as well. Obadimu *et al.* [52] compared Facebook and Twitter bots, in terms of their popularity and impact on society. Their study found Facebook bots to be more conversational, whereas Twitter bots were more political. The term "Facebook bot" had more positive sentiment attached to it than "Twitter bot."

In addition, financial manipulation and information operations [53] constitute another significant domain of activity for coordinated social bot campaigns. However, research in the given domain is not yet as extensive as other domains, such as political campaigns and information operations. In a recent study, Tardelli *et al.* [54] highlighted the coordinated social bot speculation in the stock market. They also emphasized the unique features of financial bots aiming to fool trading algorithms. However, the influence of social bots on stock returns will have to be examined more. Recent evidence suggests that social bot retweets may have limited and varied associations with stock prices, volatility, and liquidity [55].

Brünker *et al.* [56] explored the role of bots within the context of Social Commerce (SC). They analyzed how social bots were deployed on Twitter during the Black Friday season in 2018 and came up with three metrics to identify these social bots along with manual content analysis. Their findings reveal that social bots are primarily deployed to promote goods and services, and initiate sales. Their case study also

TABLE IV
BIBLIOGRAPHIC CATEGORIZATION OF VARIOUS METHODOLOGICAL APPROACHES

Category	Methods	Research Papers
Bot detection and characterization	Feature based	[Boshmaf et al., 2016], [Wang et al., 2012], [Chu et al., 2010], [Stine and Agarwal, 2019], [Lee et al, 2011], [Rout et al., 2020], [Heidari et al., 2020], [Beskow et al., 2018]
	Graph based	[Viswanath et al., 2010], [Fortunato, 2010], [Leskovec et al.,2009], [Cao et al., 2012], [Zhao et al., 2009], [Mohaisen et al., 2010], [Boshmaf et al., 2011], [Bilge et al., 2009], [Wagner et al., 2012], [Gong et al., 2014], [Yanbin, 2019]
	Hybrid (feature + graph)	[Davis et al., 2016], [Yang et al., 2019], [Varol et al., 2017], [Yang et al., 2020] [Beskow et al., 2018], [Sayyadiharikandeh, 2020]
	Visual analytics based	[Wu et al., 2016], [Chen et al., 2017], [Khayat et al., 2020], [Shi et al., 2020]
Bot coordination	Game theoretic approaches	[Axelrod et al., 1981], [Gintis et al., 2005], [Cooper et al., 1992], [Myatt and Wallace, 2009]
	Ecological based approaches	[Overbey et al., 2019]
	Organizational approaches	[Binmore, 2005], [Gintis et al., 2005], [Nettle, 2011]
	Graph based approaches	[Agarwal et al., 2017], [Goyal and Vega-Redondo, 2005], [Young, 2011], [Chwe, 2000], [Jackson and Watts, 2002], [Jackson and Wolinsky, 1996], [Al-Khateeb and Agarwal, 2015], [Al-Khateeb and Agarwal, 2016], [Overbey et al., 2019], [Alassad et al., 2020]

reveals that bot–human relationships are emerging more in customer support. That way, practitioners can drive innovation and also mimic successful third-party approaches to increase sales and generate more revenue by implementing automatic promotional tools.

Such severe impacts on society call for researchers to devise ways to detect not only the presence of such malicious actors but also introduce methodologies to detect coordinating bots to prevent future damages. A growing body of research addresses the presence of social bot activity, how they impact the SN, and their detection [25], [37], [57], [58]. In this survey, we have collected approaches for both bot detection and coordination studies, as shown in Table IV. It is clear that researchers have conducted more studies on bot detection than bot coordination, as evident in Table IV, but it also sets the groundwork for the next two sections. We will go over the bot detection methods first, discuss all the cited works in Table IV, then proceed to bot coordination, and justify the need for more studies in bot coordination while discussing all the cited works in Table IV.

IV. BOT DETECTION METHODS

Social bot detection and characterization methods have evolved significantly since the field started to mature within the previous decade. In Sections IV-A–IV-C, we focus on the methods and techniques that were prominently used in the relevant literature cited in Table IV and practical use-case scenarios since the early applications. Furthermore, as emphasized in earlier sections, the rest of this study will survey the state of the current literature on the coordination of social bots.

Early bot detection mechanisms include online Turing tests, such as CAPTCHAs [59]. Crowdsourcing services later took over complex human-based tasks [60], [61]. This resulted in a dramatic rise of fabricated, malicious content online, such as fake reviews on Yelp [62], malware and spam on SNs [27], [63], [64] and large, and Sybil-based political lobbying efforts [65]. This opened paths for researchers to detect Sybils on OSNs, such as Facebook [66], Twitter [67], [68], and Renren [64]. Literature suggests that some of the early Sybil detection techniques used graph- and feature-based methods [37].

A. Early Sybil Detection

Researchers developed algorithms to perform decentralized Sybil detection on social graphs by identifying tightly connected Sybil communities. Viswanath *et al.* [69] proposed community detection algorithms, such as Mislove's algorithm [70], to detect Sybils by partitioning a social graph into several densely connected clusters with sparser connections with other clusters within the graph [67], [71]. Sybil attacks were also identified by Alvisi *et al.* [72] as a community detection problem while investigating Sybil defense protocols and its evolution through a social graph, its structure, and network properties. They suggested combining complementary detection techniques to identify Sybils in a social graph. This introduced SybilRank [73], a system that assumes Sybil accounts connect to legitimate users to appear legitimate and Zhao *et al.*'s [74] BotGraph that detects spam bots by correlating their IP addresses to that of their controller. Both mechanisms try to uncover Sybils that form tight-knit communities in social graphs. Mohaisen *et al.* [68] identified fast-mixing of social graphs as a necessary precondition for community-based Sybil detection. However, Boshmaf *et al.* [21] and a few other studies [75], [76] confirmed that attackers trick naive users into befriending them so that they can easily infiltrate OSNs ultimately making graph-based Sybil detection ineffective.

Researchers adopted feature-based methods that leverage user-level metrics along with machine learning algorithms to identify discriminative features to classify real users from fakes. Boshmaf *et al.*'s [77] Íntegro leverages user-level activities to predict victim accounts and marks them as the starting point of a random walk algorithm that ranks real users higher than a suspected Sybil account. A low-score Sybil account allows OSN moderators to quickly detect and remove them. However, their work did not provide ways to correctly classify Sybil accounts from regular accounts. Gong *et al.* overcame a number of such drawbacks from previous work with Sybilbelief [78], a semisupervised learning framework

that can classify and rank Sybil accounts. Machine learning algorithms were also successful in detecting spam behavior on Twitter [79]–[81] and Facebook [82]. Yanbin *et al.* [83] studied large-scale Sybil attacks and found strategies that the Sybils developed to build legitimate social ties. They analyzed the user's friend request and acceptance proportions in a certain period of time and used SVM-based models and threshold classifiers to obtain the differences between Sybil and ordinary users. Assuming that an actual user will never send friend requests to Sybil users, Yang suggested the VoteTrust algorithm. Unfortunately, the strategies adopted by malicious bots have evolved dramatically due to the mainstream use of social media platforms, such as Twitter. This has resulted in a crucial need for advanced detection methods to differentiate humans from bots.

B. Advanced Social Bot Detection

Researchers modified their bot detection methodologies to investigate individual characteristics of accounts on social media and look for ways to differentiate bots from humans. Wang *et al.* [84] proposed using manual annotators to examine multiple profiles of Facebook and Renren users to detect malicious bot presence, which helped the authors to analyze the effectiveness of human detection. Although the detection rate deteriorated over time, it was still helpful in detecting bots based on a majority vote. In 2010, Chu *et al.* [85] proposed a system to automatically classify humans, bots, and cyborgs on Twitter. Over half a million accounts were studied to find the difference between humans, bots, and cyborgs in terms of content and behavior. Their classifier comprises four components are given as follows.

1) Entropy-based components detect patterns of periodicity in users' tweet times. Their classifier detected high levels of entropy in humans whereas bots and cyborgs tweeted at regular time intervals.
2) The machine learning component detects if the tweet content is spam. The classifier rated bots to be the highest spammers out of the three.
3) The account properties component identifies the presence of bots by checking account-related features, such as external URL ratio in the tweets or by checking the tweeting device (web, mobile, or API).
4) The decision-maker component uses the linear discriminant analysis (LDA)[3] method to encapsulate the features identified by each of the three components to distinguish between a human, bot, or cyborg.

Stine and Agarwal [36] argued that an entropy-based characterization of users' language usage can also help detect inorganic activity. Their work analyzes whether a user's current vocabulary changes or stays the same over time. They leveraged information-theoretic measures of a cognitive surprise to study a set of Twitter users' behavior. They compared the language-production dynamics based on term frequencies at multiple levels of granularity to identify the degree to which a user's word usage is organic, inorganic, or both.

[3]LDA is a statistical method where a linear combination of features is used to distinguish among multiple classes of samples.

In 2011, Texas A&M became the pioneer in bot detection by using honeypots [25]. Honeypots use bots to generate nonsensical content, designed only to attract other bots. Thousands of bots were attracted to the honeypot laid by the Texas A&M team that later generated a labeled dataset, helping several future research efforts. Rout *et al.* [86] implemented a trust model using a learning automata-based malicious social bot detection (LA-MSBD) algorithm with a set of URL-based features, such as URL redirection, the relative position of URL, frequency of shared URLs, and spam content in URL to distinguish between legitimate and illegitimate malicious tweets. The Bayesian learning and the Dempster–Shafer theory (DST) were used to assess the trustworthiness of tweets. The model was tested on two Twitter datasets, namely, The Fake Project dataset and the Social Honeypot dataset, in terms of precision, recall, F-measure, and accuracy for MSBD in the Twitter network.

Morstatter *et al.* [87] argued that existing bot detection studies emphasize precision [3], [88], [89] to evaluate a model at the cost of the recall. A precision-based model only predicts acute bots and ignores the rest, which could lead to a high rate of false-positive results. Morstatter *et al.*'s model increased the recall in detecting bots, which reduced the number of false positives and detected a wider range of bots. Morstatter *et al.* compared their model to existing approaches for bot detection and found that the model achieves superior performance in yielding high recall with only a minor loss in precision. In an extended work by Nazer *et al.* [90], the authors introduced REFOCUS, a recall-focused supervised bot detection algorithm that prioritizes high recall without declining the overall performance. They tested their algorithm on the Arabic Honeypot dataset originally collected by Morstatter *et al.* and two other datasets consisting of social spam bots. They compared REFOCUS with state-of-the-art bot detection models to show that focusing on recall does not necessarily deteriorate overall performance in terms of F1 score.

C. State-of-the-Art Bot Detection

In 2014, Indiana University, Bloomington, IN, USA, and the University of Southern California, Los Angeles, CA, USA, launched the "Bot or Not" online API service [37], [91], [92]. They both participated in "The Twitter Bot Challenge" organized by DARPA in 2015 [93] where they had to identify influence bots that had infiltrated Twitter's informal antivaccine discussion with provaccine content. They used traditional classification models trained on the Texas A&M dataset to help users evaluate the likelihood of an account of being a bot. "Bot or Not" uses Twitter metadata to extract features, such as tweet semantics, temporal, profile, network, and sentiment, and classifies users based on the Random Forest algorithm. "Bot or Not" was later renamed to "Botometer," and their feature set is also expanded to include 1150 account related features [94]–[96]. They compared various classifiers, such as Random Forests, AdaBoost, Logistic Regression, and Decision Trees, but Random Forests outperformed all of them. They also modified their training dataset with manually annotated tweet accounts and combined them with the

initial dataset that they retrieved from the Texas A&M team in 2011.

Beskow and Carley [97] introduced Bot-hunter, a tiered approach to bot detection and characterization, while simultaneously annotating data based on events. They collected Twitter data in several tiers along with related machine learning features and models. Their Tier 1 model's performance is compared to an adequate baseline model, such as the Botometer algorithm. Unlike Botometer, Bot-hunter can run on existing data rather than waiting on the API to recollect data that the researchers may already have. However, Bot-hunter is still under development, and the API is not available for use.

In 2020, Sayyadiharikandeh *et al.* [98] proposed a new supervised learning method that trains classifiers specialized for each class of bots and combines their decisions through the maximum rule. The ensemble of specialized classifiers (ESCs) can better generalize novel bot behaviors that are learned with fewer labeled examples during retraining. ESC has been successfully implemented to their existing Botometer model to detect novel social bots. Heidari *et al.* [99] developed machine learning models to detect bots based on the extracted user's profile from a Tweet's text. More than 6900 Twitter accounts were analyzed to generate their public profiles that were later used to detect bots in social media. Their model outperformed previous bot detection models by achieving nearly 94% prediction accuracy in bot detection in two of the test datasets. This was also possible due to the use of contextualized representation of each tweet by using ELMO and GLOVE in the word embedding phase, which essentially achieved high prediction accuracy in their model. However, a practical bot detection application is not available. To the best of our knowledge, Botometer is known as the current state-of-the-art tool available for individual bot detection.

All the studies discussed in the survey so far have been looking at computational approaches to detect bots and study botnet behaviors. Throughout the years, researchers have dedicated their time and energy to identifying characteristics of individual social media accounts. It is helpful in detecting and suspending large numbers of accounts that show possible bot-like features. There also exists a community of researchers who are looking and trying to understand bot phenomena from a visual analytics perspective [100]–[103]. Both approaches complement each other in terms of providing a visual analytical methodology to advance botnet detection studies. However, the focus of this survey is not to solely look into various botnet detection techniques but to study their coordination tactics. It is important to understand the role of coordinating bots potentially working together toward a common goal.

Cresci [104] reflected on a decade of bot detection studies to show trends in strategies and suggestions on how research needs to focus more on measuring the extent of coordination rather than individual user attributes. Due to the sophistication of social bots, newer accounts are more aligned with the behavioral patterns of humans due to the increased hybridization of humans and bots, also known as cyborgs. The author suggests inventing techniques that identify suspicious coordinated and synchronized behaviors as bots act in coordination with other bots, forming botnets to amplify their effects [105]. Section V will discuss some of the previous literature that had identified traces of naive bot coordination in an online space. Coordination among users can also be found in other domains, such as biological, organizational, and online multiplayer games. This will help in utilizing some of the existing technologies to measure social bot coordination.

V. Coordination Strategies

Coordination in a network is evident when "multiple actors work together to pursue a common goal." It can be defined as the "additional information processing performed when two or more connected actors pursue a goal that a single actor pursuing the same goal would not perform" [15]. Literature suggests that involving interdependent actors to map their goals to specific activities can help increase their ability to coordinate better [106].

A considerable amount of literature cited in Table IV emphasizes the emergence of coordination in biological [107], [108] and socioeconomic [109]–[111] systems to study evolution in a society. Axelrod and Hamilton [107] developed a model in the context of the Prisoner's Dilemma game that assumes interactions between pairs of actors occur on a probabilistic basis. Their results show how reciprocity-based coordination can get started in an asocial world, thrive while interacting with other strategies, and also resist invasion once fully established. Gintis *et al.* [110] discuss reciprocity as a behavior actors can adopt to strategize conditional coordination and punishment by observing each other's behavior. Similar behavior was also observed in the early stages of naive social bots where they embrace multiple coordination strategies to interact with other bots or nonbots in order to achieve their goals. One such behavior adopted by naive bots is the "mutual reciprocity" principle observed in a case study conducted by Agarwal *et al.* [30] during the Crimean water crisis in 2014 and the NATO Trident Juncture exercise in 2015, where bots follow all of their followers to gain many followers in a short period of time. They studied the role that social bots play in disseminating propaganda and their evolution over time. Bots involved in NATO's Trident Juncture exercise in 2015 no longer displayed mutual reciprocity.

The literature on coordination games focused mainly on how coordination impacts social action [112], [113]. Cooper *et al.* [112] presented experimental evidence on nonbinding, preplay communication in bilateral coordination games. Considering two forms of communication structures, such as one-way and two-way and two types of coordination games where one uses a cooperative strategy and the other is less "risky," they evaluated the effect of "cheap talk." Some studies have explored the problem of coordination on networks [114], [115] and ways that network properties affect strategic considerations of the actors in coordination games [116]–[119]. However, it is not enough to demonstrate that a group can generate communal action. The interactions among individuals may affect their strategic considerations of actors deciding whether or not to participate in collective action. Moreover, such interactions may also affect the groups' ability to coordinate their behavior.

In the social media domain, however, collective action studies showed promising results. Al-Khateeb and Agarwal [11] detected social bot coordination after examining their information network. Their results show botnets tweeting and retweeting URLs that link to propaganda websites. Al-Khateeb and Agarwal [120] found interactions between bots and a "broker" node, revealing group-level coordination on Twitter. They claimed that botnets may or may not show mutual reciprocity, but they exhibit common shared behaviors to enact amplification without getting suspended. Echo chambers arise from coordinated behavior, such as that observed in [11]. Echo chambers may arise from communication dynamics when users coordinate to intentionally disseminate messages to large audiences. A few criteria that distinguish echo chambers from existing literature include the following.

1) Actors post identical tweets to influence public opinion or to disseminate propaganda.
2) A group of actors are tweeting the exact text/tweet but not at the same time.
3) The usernames of these actors seem legitimate [11].

Overbey *et al.* [121] leveraged the findings from Al-Khateeb and Agarwal [120] and explored common enemy graphs within the ecological systems to identify and characterize groups of actors that exhibit characteristics of automation and/or potential coordination in their shared behavior. They developed "edge weight variants of fuzzy competition graphs" to further characterize the behavior of groups of automated accounts within clusters. They identified groups that are not necessarily working together but alongside each other. However, this approach is more inclined toward detecting communities of users rather than explicitly assessing coordination between them.

Coordinating bots are going to be a nuisance, so researchers need to focus more on advancing bot coordination techniques rather than bot detection. Bot detection, bot behavior analysis, and methods are surveyed in this article, but bot coordination presents a real challenge. As we go further into the future, isolated bots are not going to be the most critical bots as also claimed by Cresci [104]. As current research struggles to find ways to assess bot coordination, future research can leverage existing concepts used in other domains to invent new methodologies that may overcome the biggest challenge of identifying synchronous group-level coordination. One way to analyze group-level features is through social graphs where users are connected to one another through a common relationship, such as common friends, shared hashtags, and URLs or simply identical texts. Alassad *et al.* [122] analyzed fake news disseminating network on YouTube to show that coordination tactics are becoming a norm among adversarial information operations. Their Focal Structure Analysis tool surpasses traditional community detection methods to find, analyze, and suspend these coordinated malicious sets of users responsible for propagating behavior through online social media platforms. Section VI will discuss existing network science concepts that can be useful in understanding relationships between users in a network. Once researchers find ways to assess coordination among groups of users, it can easily be drilled down to focus only on bots and botnets.

TABLE V
EXAMPLES OF NETWORK-LEVEL METRICS USED TO DESCRIBE NETWORKS

Measure	Definition
Network Diameter	Length of the longest shortest path between two nodes.
Average Degree	Average number of edges per node
Modularity	Measures the strength of division of a network into clusters.
Clustering Coefficient	Measures the extent to which my friends are friends with one another.
Density	Ratio of the number of actual edges to the number of possible edges in the network.
Centralization	Difference between the centrality scores of the most central actor and those of all actors in a network. Then, the ratio of the actual sum of the differences to the maximum sum of the differences is calculated.
Clique	The maximum number of actors in a network who are all directly connected to one another, but are not all directly connected to any additional individuals in the network.

TABLE VI
NODE-LEVEL METRICS ASSIGNED TO INDIVIDUAL ACTORS

Measure	Definition
Degree	Number of direct edges with other actors.
In-degree	Number of incoming directional edges to the actor from other actors.
Out-degree	Number of outgoing directional edges from the actor to other actors.
Range (diversity)	Number of links to different others. (Others are defined as different to the extent that they are not themselves linked to each other, or represent different groups or statuses).
Closeness	Degree to which an actor is close to, or can easily reach all other actors in the network.
Betweenness	Degree to which an actor mediates, or falls between any other two actors on the shortest path between those actors.
Centrality	Degree to which an actor is central to a network.

VI. SOCIAL NETWORK MEASURES FOR COORDINATION ASSESSMENT

Researchers have been leveraging SN measures and network science theories to study coordination in interorganizational networks. SN theory helps in identifying and quantifying informal networks, which operates beyond the traditional organizational structure of relationships. The metrics extracted for OSNs are important parameters for the identification of coordination techniques. We have classified the metrics extracted from OSNs into the network- and node-level measures [123].

1) Network-level metrics analyze how users are connected with one another and describe the communication network among them. These metrics are related to network structure and group interactions, and a few are mentioned in Table V.
2) Node-level metrics study the importance of a single node and its interaction with other nodes. These

metrics emphasize the user and its individual properties, as shown in Table VI.

The application of SN theory may be useful across many disciplines as they are able to assess patterns of network structure and behavior [124]. The SN theory also helps investigate a network to discover ways in which information travels within a network, which may lead to coordination [125]. Kapucu [126] analyzed the interactions and evolution of organizations, such as public, private, and nonprofit in response to the September 11, 2001, terrorist attacks. Kapucu identified SN measures, such as degree, closeness, and betweenness, to detect overall network structure and actor (node) positions within the network. These measures were based on connections (edges) between actors, the length of the shortest path between them, and the number of shared pathways between actors [126]. Granovetter's [127] theory of "Strength of Weak Ties" suggests that "individuals obtain new and novel information from weak ties rather than from strong ties within the individual's group structure." Granovetter argues that new information emerges since weak ties serve as a bridge to different node clusters [128]. Furthermore, David [129] showed that strong ties play an important role in generating trust between individuals. Also, Levin and Cross [130] found that knowledge-intensive work takes advantage of strong ties to increase performance by utilizing useful information rather than weak ties. These findings focus more on understanding the structure of a social graph and how possible relationships are formed based on specific nodes and their position in the network, which is insufficient to justify the presence of bots in OSNs.

Existing network measures provide a roadmap to show how quickly information travels between users based on the network structure and how users can successfully coordinate based on their positions within that network. Himelboim *et al.* [131] presented a series of network structures classified through four network-level metrics, such as density, modularity, centralization, and the fraction of isolated users. While exploring various topic networks on Twitter, they identified key indicators of information flow between users. The network structures include divided, unified, fragmented, clustered, and in and out hub-and-spoke networks based on a single or combination of such network measures.

A well-structured network where information not only travels faster but also reaches many users quickly can indicate successful coordination. For example, if the goal of a botnet is to divide and conquer misinformation to multiple users, existing network measures, such as clustering and modularity, can be utilized to speed up the information flow in the social graph. This can be studied at the network level or the group level by analyzing community structure and connections between them. Clustering or network transitivity shows the likelihood of two users A and B being connected if they are both connected to a third user C. With the growth of a network, nodes form smaller clusters within the network, which are densely interconnected but maintain loose ties with members of other clusters. Modularity can be used to identify the quality of a division of a network into clusters, and its score (0 to 1) indicates whether the network structure is divided or unified.

Arif *et al.* [132] analyzed an information operation led by Russia's Internet Research Agency, where social bots were created to participate in an online discourse about the #BlackLivesMatter (BLM) movement and police-related shootings in the U.S. during the 2016 Presidential Elections. Their findings reveal polarized network structures where bots formed the central core of each of the polarized clusters. Their goal was to create a division in the Twitter network, and they succeeded by using one set of accounts that post content supporting the BLM movement and another that was against it. Homophily [133] is a network phenomenon that is formed between densely interconnected clusters. When nodes with similar interests form social connections, they tend to coordinate better in achieving their goal. Despite having weaker connections with other clusters, coordination could most likely be higher if there exist bridge nodes formed by users with high betweenness centrality. This measure is calculated on a node level where these nodes serve as brokers or gatekeepers that can either liberate or restrict the spread of information across multiple clusters. If these bridge nodes are removed, the entire network will disintegrate into smaller independent clusters, which will tremendously reduce the impact of coordination. Therefore, SNA along with network science theories can be useful to understand coordination in general. To emphasize botnet coordination, an additional layer of analysis needs to be conducted where prominent nodes are identified using centrality measures, such as degree or betweenness, and run them through a bot detection algorithm.

VII. Visual Representation of Bibliography

This section presents a visual representation of our current bibliographic findings in this survey study. As mentioned in earlier sections, the number, significance, and audience of studies on social bots have grown significantly in the last decade. As part of this survey, we examined the publication trends over the years, distribution of major themes, topics, and disciplines, as well as the author networks in the surveyed field. As Sections VII-A–VII-D demonstrate, the literature on social bots has become increasingly interdisciplinary, and the range of research themes and subjects expanded.

We conducted a semisystematic review [134] of social bots literature to study the disciplinary and thematic distributions of the articles that were published within the last decade. Semisystematic review is suggested as an appropriate method when the subject at hand covers a broad spectrum in terms of the diversity of disciplines, conceptualizations, and approaches [135]. In such cases, a semisystematic review method enables an overall "mapping" of a research area and understanding how the area has "unfolded" over the years [134]. In this study, we aim to capture snapshots of the major themes in the literature of social bots and the interdisciplinary characteristics of the relevant research agendas.

A. Publication Trends

To observe trends in the literature, we collected a fraction of relevant publications as shown in Fig. 1. We acquired 177 publications that have been published since 2010 by querying

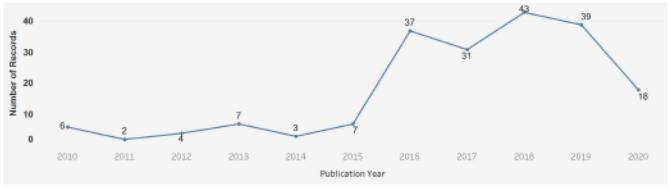

Fig. 1. Number of publications by the publication year in our selected bibliography.

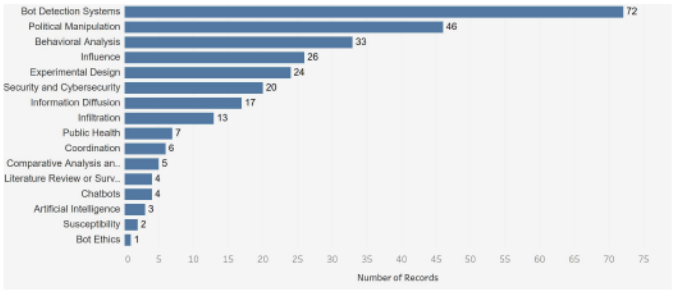

Fig. 2. Distribution of major topics and themes in our selected bibliography. Some publications have more than one primary topic or theme.

"social bots" on Google Scholar and cross-checking with the results of identical queries on several major publishers, including IEEE Xplore, ACM Digital Library, Science Direct, SpringerLink, and Taylor & Francis. We limited our collection to peer-reviewed articles and conference proceedings in English. For extracting the final list from a high number of publications, we first prioritized the relevance and strictly collected records in which the theme of social bots is central while excluding publications that primarily focus on fake news, spam accounts, Sybil accounts, and several other topics even if they briefly mention social bots. In addition, we carried out a secondary search by focusing on the articles that have been published in 2017, 2018, and 2019, as we also prioritized the recency of the publications to be able to see current thematic and disciplinary trends. Finally, we checked citations to extract both important and relatively recent publications. As a result, our final sample includes articles from the publishers, which we did not query in the beginning.

A significant portion of records in our selected bibliography includes studies that have been published since the beginning of 2016. To note, this distribution is partly due to our prioritization of recent publications. Nevertheless, this trend represents the overall growth of research interest in social bots, as the research, public attention, and the number of empirical cases also grew within the same timeframe. From 2016 onward, the most frequent topics and themes in our selected bibliography were "bot detection systems," "political manipulation and propaganda," and "behavioral analysis."

B. Major Topics and Themes of Publications

The major themes of social bot research (see Fig. 2) discuss the usage of bots vis-à-vis bot detection systems, political manipulation and propaganda, behavioral analysis, security, influence, and information diffusion. Publications on bot detection systems focus on improving existing algorithms to identify

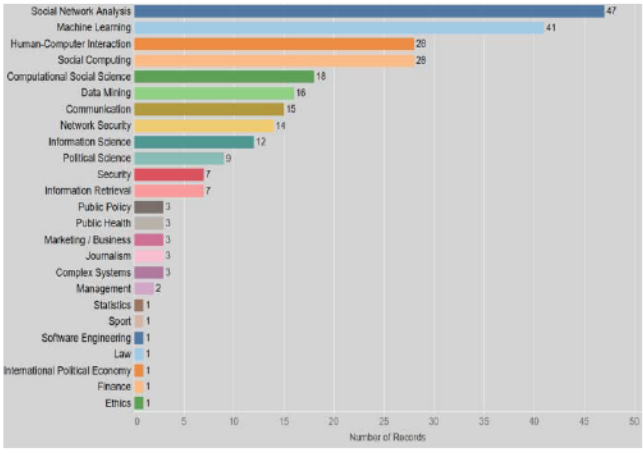

Fig. 3. Distribution of primary disciplines in our selected bibliography. Some publications are categorized under more than one discipline.

sophisticated bots that still remain undetected. The following is an illustration of topic distribution in our collection of publications.

C. Disciplinary Distribution

Fig. 3 shows that studies of bots, fake news, and disinformation on social media are not limited to a particular domain. Instead, it is an issue that researchers from every possible discipline are trying to overcome. While there has been tremendous advancement in research, bots have also evolved, which makes it difficult to eradicate them at once.

Overall, our collection of social bot studies illustrates the multidisciplinary characteristics of the relevant literature. Although we categorized the selected publications in accordance with their primary disciplines, often, social bot studies contain a combination of methods and conceptual frameworks from a multitude of disciplines. SNA, computational social science, machine learning, and human–computer interaction are the most frequent disciplines in our dataset. Fig. 4 shows that a significant number of publications belong to more than one discipline.

However, the network of publishing disciplines also indicates the lack of strong interdisciplinarity in the given domain. Accordingly, any potential wide-ranging solution to the problems in relation to sophisticated botnets and botnet coordination would require greater collaboration across disciplines. As Fig. 4 indicates, the study of botnet coordination needs greater engagement from disciplines, such as complex adaptive systems research, communication, security, political science, public policy, and various other social science disciplines. Similarly, Fig. 5 demonstrates that groups and clusters of researchers engage with the botnet detection, characterization, and coordination assessment problems. However, greater collaboration between research groups, labs, and clusters would strengthen interdisciplinarity in the growing domain, potentially leading to stronger engagement with the policy domains and better tackling of relevant contemporary and emerging sociotechnical problems.

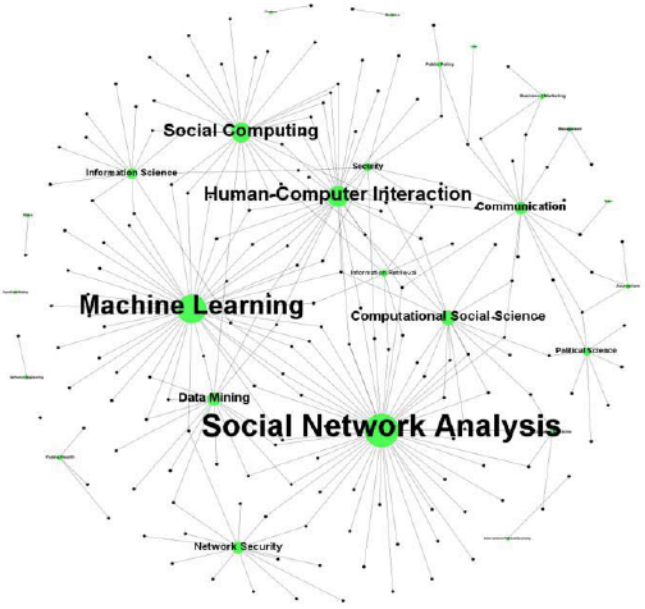

Fig. 4. Network of publications and their disciplines in our bibliography. Black nodes represent publications, while green nodes represent disciplines. The size of nodes and names represent their in-degree.

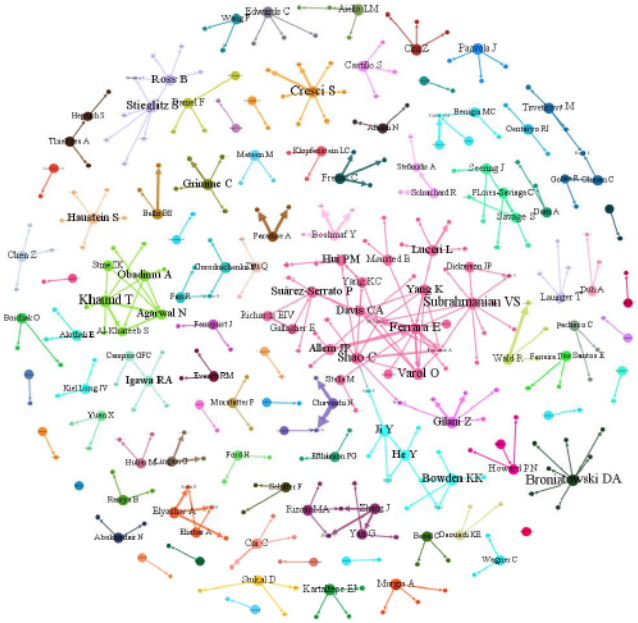

Fig. 5. Author network from our selected bibliography.

D. Network of Authors

The network in Fig. 5 is a directed network between the first author of a published article and their coauthors. The nodes with an outgoing link represent the lead author, and the nodes that have an incoming link represent a coauthor. The edge weight is based on the number of times two authors who have collaborated on multiple articles. We ran a modularity-based community detection algorithm to find clusters of authors and found 87 communities. Every cluster signifies the different authors that have collaborated in publishing an article from 2010 to 2019 on the social bot research domain. This coauthor network helps study the most productive and best-connected authors with the strongest coauthorship relations. It also helps us identify important authors based on their publication history. We also observe independent clusters, which helps us identify prominent authors within a particular group that may not have collaborated.

The findings of Figs. 4 and 5 can be combined to identify prominent researchers in their respective domains, who have collaborated with other experts from a different domain. This shows that social-bot-related issues are not limited to a single discipline, and subject matter experts can work together to mitigate the impact of malicious bots on society. It also helps reveal areas where the research collaboration is lacking.

VIII. Discussion

Social bots exist to play various roles. Bots, such as entertainment bots, stock bots, and suicide helpline bots, are often benign and are designed to provide meaningful information and support. Malicious bots, on the other hand, have a severe impact on society and require strict preventative measures. The approach to reduce the impacts of social bots from causing havoc on social media platforms is threefold. It begins with the researchers where their primary goal is to provide adequate results that show potential bot presence and bring awareness to the public. Existing tools, such as Botometer [91], allow users to examine Twitter accounts and identify whether or not they are bots. This then helps educate and bring awareness to users, and they can react accordingly. However, these efforts are ineffective if the source where these bots originate does not actively eradicate them. Finally, reporting these bots to respective social media companies can be helpful in prevention by utilizing the findings to improve their own bot detection technologies. Social media companies can do a better job at suspending or shadow banning these bot accounts.

Eradicating social bots entirely from an online space can be challenging. Social bots have been constantly evolving as the literature suggests, which enables filtering algorithms to retrain their models to keep up with this race. Researchers are given a very small segment of information to analyze from an online space due to restrictions on data retrieval. This limits the capabilities of existing technologies and algorithms to successfully detect and understand the sophisticated nature of social bots. However, social media companies have full access to their repository and can handle such issues differently. However, there could be other factors that may constrain their actions. These companies may not be held accountable even if they fail to actively suspend accounts that have been identified as bots. Their failure to regulate some of the inorganic discourse that takes place on their platforms could be due to the fact that it could suppress free speech and the infringement of liberties of citizens. Companies could be concerned about the consequences of eliminating such bot accounts, or there could be market forces at play in which stakeholders have investments that may restrict them to take drastic measures

TABLE VII
LIST OF PUBLICLY AVAILABLE DATASETS FOR SOCIAL BOT STUDIES

Dataset	Source
Information Operations	Twitter Elections Integrity Hub
Social Honeypots [25]	Infolab, Texas A&M University
Cresci-17[136]	Social Spambots
Botwiki [96], Gilani [137], Stock [138]	Botometer Repository

against social bots. Either way, there has to be a more proactive approach from these companies if they want to reduce the spread and effects of malicious bots.

Overall, the presence, use, and prevention of coordinated malicious social bots, as part of influence campaigns aiming to achieve political or economic gains, have significant implications for technical, regulatory, legal, and policy domains. Moreover, the given issue has distinct and interconnected societal, normative, and ethical aspects. Given the state of the underlying sociotechnological changes at systemic levels, preventing the harmful use of coordinated social bots can range from the critical thinking and digital literacy skills of individuals to decision-making processes in international organizations. Although the concept of prevention is outside the scope of this survey study, it is potentially one of the core areas that can benefit from the interdisciplinary growth that we demonstrated in relevant sections.

The massive growth of research in this domain, as presented in Section V, suggests that it is an issue that affects everyone, including society and science. The state-of-the-art technology for detecting social bots has also evolved tremendously alongside such sophisticated bot behaviors. Some of the open research areas for the future would require researchers to stop exploring the individual nature of bots and plan strategies to identify inorganic group-level coordination, as suggested by Cresci [104].

Table VII presents a few publicly available data sources for social bot analysis. It is to be noted that the datasets that were available during the time the research was conducted may not be available now, so we have listed some of the possible repositories that host popular datasets for bot detection and can be obtained by requesting for access.

IX. CONCLUSION

Social media and its ubiquitous adoption have enabled researchers to explore the deepest corners of social interaction among its users. We examined the different approaches and algorithms that were developed over the years to find connections and identify room for improvement. The state-of-the-art techniques for evaluating the performance of detecting inorganic accounts and coordinated activity are also reviewed. We reviewed the different SN measures that have been used to study SN interactions. Furthermore, we have highlighted the various behaviors some actors portray while disseminating information to a large scale of audience. It is important to note that existing literature mostly focuses on bot detection and its roles in information campaigns. Coordinated activity is often qualitatively analyzed and reported from a single user interaction networks' perspective. Existing research suggests coordination based on empirical observation and/or community detection algorithms. Therefore, it is important to leverage existing or known instances of coordination from previous literature and develop a network measure-based assessment framework. Bots play an active role in content dissemination; however, it is important to note that these accounts are monitored by actual human users. Indicators based on resource sharing, such as identical texts and URLs, at the same time along with concrete network science theories, will help us identify patterns to study coordination. Therefore, future work will analyze dynamic networks to demonstrate synchronicity or harmony among actions of individuals on social media. Once coordination can be correctly assessed within an SN, it would be much easier to detect the presence of bots in it.

ACKNOWLEDGMENT

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations.

REFERENCES

[1] S. Raghavan, "Digital forensic research: Current state of the art," *CSI Trans. ICT*, vol. 1, no. 1, pp. 91–114, Mar. 2013, doi: 10.1007/s40012-012-0008-7.
[2] A. Perrin. (Oct. 2015). Social media usage: 2005–2015. Washington, DC, USA. [Online]. Available: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/
[3] J. Ratkiewicz, M. Conover, M. R. Meiss, B. Gonçalves, A. Flammini, and F. Menczer, "Detecting and tracking political abuse in social media," in *Proc. 5th Int. AAAI Conf. Weblogs Social Media*, Barcelona, Spain, Jul. 2011, pp. 297–304.
[4] E. Otte and R. Rousseau, "Social network analysis: A powerful strategy, also for the information sciences," *J. Inf. Sci.*, vol. 28, no. 6, pp. 441–453, Dec. 2002, doi: 10.1177/016555150202800601.
[5] S. Wasserman and K. Faust, *Social Network Analysis: Methods and Applications*, vol. 8. Cambridge, U.K.: Cambridge Univ. Press, 1994.
[6] C. A. Bail *et al.*, "Assessing the Russian internet research agency's impact on the political attitudes and behaviors of American Twitter users in late 2017," *Proc. Nat. Acad. Sci. USA*, vol. 117, Nov. 2019, Art. no. 201906420, doi: 10.1073/pnas.1906420116.
[7] A. Bovet and H. A. Makse, "Influence of fake news in Twitter during the 2016 U.S. Presidential election," *Nature Commun.*, vol. 10, no. 1, p. 7, Jan. 2019, doi: 10.1038/s41467-018-07761-2.
[8] E. Ferrara, "Disinformation and social bot operations in the run up to the 2017 French presidential election," *1st Monday*, vol. 22, no. 8, pp. 1–33, Jul. 2017, doi: 10.5210/fm.v22i8.8005.
[9] P. N. Howard and B. Kollanyi, "Bots, #strongerin, and #brexit: Computational propaganda during the UK-EU referendum," *SSRN Electron. J.*, p. 6, Jun. 2016, doi: 10.2139/ssrn.2798311.
[10] A. Bessi and E. Ferrara. (2016). *Social Bots Distort the 2016 U.S. Presidential Election Online Discussion*. Accessed: Aug. 16, 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2982233
[11] S. Al-Khateeb and N. Agarwal, "Examining botnet behaviors for propaganda dissemination: A case study of ISIL's beheading videos-based propaganda," in *Proc. IEEE Int. Conf. Data Mining Workshop (ICDMW)*, Nov. 2015, pp. 51–57.
[12] J. Jiang, E. Chen, S. Yan, K. Lerman, and E. Ferrara, "Political polarization drives online conversations about COVID-19 in the United States," *Hum. Behav. Emerg. Technol.*, vol. 2, no. 3, pp. 200–211, 2020, doi: 10.1002/hbe2.202.
[13] A. K. M. N. Islam, S. Laato, S. Talukder, and E. Sutinen, "Misinformation sharing and social media fatigue during COVID-19: An affordance and cognitive load perspective," *Technol. Forecasting Social Change*, vol. 159, Oct. 2020, Art. no. 120201, doi: 10.1016/j.techfore.2020.120201.
[14] A. Gruzd and P. Mai, "Going viral: How a single tweet spawned a COVID-19 conspiracy theory on Twitter," *Big Data Soc.*, vol. 7, no. 2, pp. 1–9, Jul. 2020, doi: 10.1177/2053951720938405.
[15] T. W. Malone, "What is coordination theory?" Sloan School Manage., Massachusetts Inst. Technol., Cambridge, MA, USA, Working Papers 182, 1988, p. 32.

[16] T. W. Malone and K. Crowston, "The interdisciplinary study of coordination," *ACM Comput. Surv.*, vol. 26, no. 1, pp. 87–119, Mar. 1994, doi: 10.1145/174666.174668.

[17] A. Abbasi and J. Altmann, "A social network system for analyzing publication activities of researchers," in *On Collective Intelligence* (Advances in Intelligent and Soft Computing), vol. 76, T. J. Bastiaens, U. Baumöl, and B. J. Krämer, Eds. Berlin, Germany: Springer, 2010, doi: 10.1007/978-3-642-14481-3_5.

[18] K. K. S. Chung, L. Hossain, and J. Davis, "Exploring sociocentric and egocentric approaches for social network analysis," in *Proc. 2nd Int. Conf. Knowl. Manage. Asia Pacific*, 2005, p. 9.

[19] B. Mullen, C. Johnson, and E. Salas, "Effects of communication network structure: Components of positional centrality," *Soc. Netw.*, vol. 13, no. 2, pp. 169–185, Jun. 1991, doi: 10.1016/0378-8733(91)90019-P.

[20] S. Bradshaw and P. N. Howard, "The global disinformation order: 2019 global inventory of organised social media manipulation," Oxford Internet Inst., Oxford, U.K., Tech. Rep., Sep. 2019. [Online]. Available: https://comprop.oii.ox.ac.uk

[21] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: When bots socialize for fame and money," in *Proc. 27th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Orlando, FL, USA, 2011, p. 93, doi: 10.1145/2076732.2076746.

[22] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Key challenges in defending against malicious socialbots," in *Proc. 5th USENIX Workshop Large-Scale Exploits Emergent Threats*, San Jose, CA, USA, 2012, p. 4.

[23] J. R. Douceur, "The Sybil attack," in *Peer-to-Peer Systems*. Berlin, Germany: Springer, 2002, pp. 251–260.

[24] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," *Comput. Netw.*, vol. 57, no. 2, pp. 556–578, Feb. 2013, doi: 10.1016/j.comnet.2012.06.006.

[25] K. Lee, B. D. Eoff, and J. Caverlee, "Seven months with the devils: A long-term study of content polluters on Twitter," in *Proc. 5th Int. AAAI Conf. Weblogs Social Media*, 2011, p. 8.

[26] Y. Koh, "Only 11% of new Twitter users in 2012 are still tweeting," *Publicado Wall Street J.*, Mar. 2014. [Online]. Available: http://blogs.wsj.com/digits/2014/03/21/new-report-spotlights-twitters-retention-problem/

[27] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: The underground on 140 characters or less," in *Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS)*, Chicago, IL, USA, 2010, p. 27, doi: 10.1145/1866307.1866311.

[28] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," *Bus. Horizons*, vol. 53, no. 1, pp. 59–68, Jan. 2010, doi: 10.1016/j.bushor.2009.09.003.

[29] N. Abokhodair, D. Yoo, and D. W. McDonald, "Dissecting a social botnet: Growth, content and influence in Twitter," in *Proc. 18th ACM Conf. Comput. Supported Cooperat. Work Social Comput.*, Feb. 2015, pp. 839–851.

[30] N. Agarwal, S. Al-Khateeb, R. Galeano, and R. Goolsby, "Examining the use of botnets and their evolution in propaganda dissemination," *Defence Strategic Commun.*, vol. 2, no. 1, pp. 87–112, Aug. 2017.

[31] T. Khaund, S. Al-Khateeb, S. Tokdemir, and N. Agarwal, "Analyzing social bots and their coordination during natural disasters," in *Social, Cultural, and Behavioral Modeling*. Cham, Switzerland: Springer, 2018, pp. 207–212.

[32] L. Luceri, A. Deb, S. Giordano, and E. Ferrara, "Evolution of bot and human behavior during elections," *1st Monday*, vol. 24, no. 9, Aug./Sep. 2019. [Online]. Available: https://journals.uic.edu/ojs/index.php/fm/article/view/10213/8073

[33] C. Shao, G. L. Ciampaglia, O. Varol, K.-C. Yang, A. Flammini, and F. Menczer, "The spread of low-credibility content by social bots," *Nature Commun.*, vol. 9, no. 1, p. 4787, Nov. 2018, doi: 10.1038/s41467-018-06930-7.

[34] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, p. 1146, Mar. 2018, doi: 10.1126/science.aap9559.

[35] Z. K. Stine, T. Khaund, and N. Agarwal, "Measuring the information-foraging behaviors of social bots through word usage," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Aug. 2018, pp. 570–571, doi: 10.1109/ASONAM.2018.8508811.

[36] Z. K. Stine and N. Agarwal, "Characterizing the language-production dynamics of social media users," *Social Netw. Anal. Mining*, vol. 9, no. 1, p. 60, Oct. 2019, doi: 10.1007/s13278-019-0605-7.

[37] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," *Commun. ACM*, vol. 59, no. 7, pp. 96–104, Jul. 2016.

[38] J.-P. Allem and E. Ferrara, "Could social bots pose a threat to public health?" *Amer. J. Public Health*, vol. 108, no. 8, pp. 1005–1006, Aug. 2018, doi: 10.2105/AJPH.2018.304512.

[39] D. A. Broniatowski *et al.*, "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate," *Amer. J. Public Health*, vol. 108, no. 10, pp. 1378–1384, Oct. 2018, doi: 10.2105/AJPH.2018.304567.

[40] J.-P. Allem and E. Ferrara, "The importance of debiasing social media data to better understand E-cigarette-related attitudes and behaviors," *J. Med. Internet Res.*, vol. 18, no. 8, p. e219, Aug. 2016, doi: 10.2196/jmir.6185.

[41] J.-P. Allem, E. Ferrara, S. P. Uppu, T. B. Cruz, and J. B. Unger, "E-cigarette surveillance with social media data: Social bots, emerging topics, and trends," *JMIR Public Health Surveill.*, vol. 3, no. 4, p. e98, Dec. 2017, doi: 10.2196/publichealth.8641.

[42] J. Uyheng and K. M. Carley, "Bots and online hate during the COVID-19 pandemic: Case studies in the United States and the Philippines," *J. Comput. Social Sci.*, vol. 3, no. 2, pp. 445–468, Nov. 2020, doi: 10.1007/s42001-020-00087-4.

[43] H. Y. Yan, K.-C. Yang, F. Menczer, and J. Shanahan, "Asymmetrical perceptions of partisan political bots," *New Media Soc.*, Jul. 2020, doi: 10.1177/1461444820942744.

[44] P. N. Howard, *New Media Campaigns and the Managed Citizen*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[45] T. Hwang, I. Pearce, and M. Nanis, "Socialbots: Voices from the fronts," *Interactions*, vol. 19, no. 2, p. 38, Mar. 2012, doi: 10.1145/2090150.2090161.

[46] P. T. Metaxas and E. Mustafaraj, "Social media and the elections," *Science*, vol. 338, no. 6106, p. 472, Oct. 2012, doi: 10.1126/science.1230456.

[47] L. Hagen, S. Neely, T. E. Keller, R. Scharf, and F. E. Vasquez, "Rise of the machines? Examining the influence of social bots on a political discussion network," *Soc. Sci. Comput. Rev.*, Mar. 2020, doi: 10.1177/0894439320908190.

[48] D. Arnaudo, "Computational propaganda in Brazil: Social bots during elections," *Project Comput. Propag.*, vol. 8, pp. 1–39, Jun. 2017.

[49] M. Stella, E. Ferrara, and M. De Domenico, "Bots increase exposure to negative and inflammatory content in online social systems," *Proc. Nat. Acad. Sci. USA*, vol. 115, no. 49, p. 12435, Dec. 2018, doi: 10.1073/pnas.1803470115.

[50] P. Suárez-Serrato, M. E. Roberts, C. Davis, and F. Menczer, "On the influence of social bots in online protests," in *Social Informatics*, vol. 10047, E. Spiro and Y.-Y. Ahn, Eds. Cham, Switzerland: Springer, 2016, pp. 269–278, doi: 10.1007/978-3-319-47874-6_19.

[51] J. M. Berger and J. Morgan, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter," Brook. Project U.S. Relations Islam. World, Brookings Inst., Washington, DC, USA, Tech. Rep., 2015, pp. 1–4, vol. 3, no. 20.

[52] A. Obadimu, E. Mead, S. Al-Khateeb, and N. Agarwal, "A comparative analysis of Facebook and Twitter bots," presented at the Southern Assoc. Inf. Syst. Conf., St. Simons Island, GA, USA, Mar. 2019.

[53] L. Madahali and M. Hall, "Application of the benford's law to social bots and information operations activities," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2020, pp. 1–8, doi: 10.1109/CyberSA49311.2020.9139709.

[54] S. Tardelli, M. Avvenuti, M. Tesconi, and S. Cresci, "Characterizing social bots spreading financial disinformation," in *Social Computing and Social Media. Design, Ethics, User Behavior, and Social Network Analysis*. Cham, Switzerland: Springer, 2020, pp. 376–392.

[55] R. Fan, O. Talavera, and V. Tran, "Social media bots and stock markets," *Eur. Financial Manage.*, vol. 26, no. 3, pp. 753–777, Jun. 2020, doi: 10.1111/eufm.12245.

[56] F. Brünker, J. Marx, B. Ross, S. Stieglitz, and M. Mirbabaie, "'The tireless selling-machine'—Commercial deployment of social bots during black Friday season on Twitter," in *Proc. WI Zentrale Tracks*, 2020, pp. 1522–1527, doi: 10.30844/wi_2020_n6-bruenker.

[57] A. Beutel, W. Xu, V. Guruswami, C. Palow, and C. Faloutsos, "CopyCatch: Stopping group attacks by spotting lockstep behavior in social networks," in *Proc. 22nd Int. Conf. World Wide Web (WWW)*, Rio de Janeiro, Brazil, 2013, pp. 119–130, doi: 10.1145/2488388.2488400.

[58] N. Chavoshi, H. Hamooni, and A. Mueen, "Identifying correlated bots in Twitter," in *Social Informatics*. Cham, Switzerland: Springer, 2016, pp. 14–21.

[59] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-solving services in an economic context," in *Proc. USENIX Secur. Symp.*, 2010, p. 18.

[60] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, "Dirty jobs: The role of freelance labor in web service abuse," in *Proc. 20th USENIX Conf. Secur.*, Aug. 2011, p. 16.

[61] G. Wang *et al.*, "Serf and turf: Crowdturfing for fun and profit," in *Proc. 21st Int. Conf. World Wide Web (WWW)*, Lyon, France, 2012, p. 679, doi: 10.1145/2187836.2187928.

[62] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao, "You are how you click: Clickstream analysis for Sybil detection," in *Proc. 22nd USENIX Secur. Symp. (USENIX Secur.)*, 2013, pp. 241–256.

[63] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proc. 10th Annu. Conf. Internet Meas. (IMC)*, 2010, p. 13.

[64] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: An analysis of Twitter spam," in *Proc. ACM SIGCOMM Conf. Internet Meas. Conf. (IMC)*, 2011, p. 16.

[65] BBC News. (Mar. 2012). *Russia Twitter Protests Spammed*. Accessed: Jul. 24, 2019. [Online]. Available: https://www.bbc.com/news/technology-16108876

[66] K. Dunham and J. Melnick, *Malicious Bots?: An Inside Look Into the Cyber-Criminal Underground of the Internet*, 1st ed. New York, NY, USA: Auerbach Publications, 2008, doi: 10.1201/9781420069068.

[67] S. Fortunato, "Community detection in graphs," *Phys. Rep.*, vol. 486, nos. 3–5, pp. 75–174, 2010.

[68] A. Mohaisen, A. Yun, and Y. Kim, "Measuring the mixing time of social graphs," in *Proc. 10th Annu. Conf. Internet Meas. (IMC)*, Melbourne, VIC, Australia, 2010, p. 383, doi: 10.1145/1879141.1879191.

[69] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," in *Proc. ACM SIGCOMM Conf.*, New Delhi, India, 2010, p. 363, doi: 10.1145/1851182.1851226.

[70] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in *Proc. 3rd ACM Int. Conf. Web Search Data Mining (WSDM)*, New York, NY, USA, 2010, p. 251, doi: 10.1145/1718487.1718519.

[71] J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney, "Community structure in large networks: Natural cluster sizes and the absence of large well-defined clusters," *Internet Math.*, vol. 6, no. 1, pp. 29–123, Jan. 2009, doi: 10.1080/15427951.2009.10129177.

[72] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, "SoK: The evolution of Sybil defense via social networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 382–396, doi: 10.1109/SP.2013.33.

[73] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proc. 9th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, Apr. 2012, pp. 197–210.

[74] Y. Zhao *et al.*, "BotGraph: Large scale spamming botnet detection," in *Proc. NSDI*, Apr. 2009, p. 14.

[75] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in *Proc. 18th Int. Conf. World Wide Web (WWW)*, Madrid, Spain, 2009, pp. 551–560, doi: 10.1145/1526709.1526784.

[76] C. Wagner, S. Mitter, C. Körner, and M. Strohmaier, "When social bots attack: Modeling susceptibility of users in online social networks," in *Proc. Workshop Making Sense Microposts (WWW)*, Lyon, France, vol. 838, Apr. 2012, pp. 41–48.

[77] Y. Boshmaf *et al.*, "Integro: Leveraging victim prediction for robust fake account detection in large scale OSNs," *Comput. Secur.*, vol. 61, pp. 142–168, Aug. 2016, doi: 10.1016/j.cose.2016.05.005.

[78] N. Z. Gong, M. Frank, and P. Mittal, "Sybilbelief: A semi-supervised learning approach for structure-based Sybil detection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 976–987, Jun. 2014, doi: 10.1109/TIFS.2014.2316975.

[79] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in *Proc. 7th Annu. Collaboration, Electron. Messaging, Anti-Abuse Spam Conf.*, Redmond, WA, USA, Jul. 2010, p. 10.

[80] A. H. Wang, "Don't follow me: Spam detection in Twitter," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Jul. 2010, pp. 1–10.

[81] S. Yardi, D. Romero, G. Schoenebeck, and D. Boyd, "Detecting spam in a Twitter network," *1st Monday*, vol. 15, no. 1, 2010, doi: 10.5210/fm.v15i1.2793.

[82] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2010, p. 6.

[83] Z. B. Yanbin, Z. Yang, C. Wilson, and X. Wang, "Uncovering social network Sybils in the wild," in *Proc. 11th ACM SIGCOMM*, 2011, pp. 1–7. Accessed: Jul. 23, 2019. [Online]. Available: http://koasas.kaist.ac.kr/handle/10203/167794

[84] G. Wang *et al.*, "Social turing tests: Crowdsourcing Sybil detection," 2012, *arXiv:1205.3856*. [Online]. Available: http://arxiv.org/abs/1205.3856

[85] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Who is tweeting on Twitter: Human, bot, or cyborg?" in *Proc. 26th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2010, pp. 21–30.

[86] R. R. Rout, G. Lingam, and D. V. L. N. Somayajulu, "Detection of malicious social bots using learning automata with URL features in Twitter network," *IEEE Trans. Computat. Social Syst.*, vol. 7, no. 4, pp. 1004–1018, Aug. 2020, doi: 10.1109/TCSS.2020.2992223.

[87] F. Morstatter, L. Wu, T. H. Nazer, K. M. Carley, and H. Liu, "A new approach to bot detection: Striking the balance between precision and recall," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, San Francisco, CA, USA, Aug. 2016, pp. 533–540, doi: 10.1109/ASONAM.2016.7752287.

[88] S. Lee and J. Kim, "Early filtering of ephemeral malicious accounts on Twitter," *Comput. Commun.*, vol. 54, pp. 48–57, Dec. 2014, doi: 10.1016/j.comcom.2014.08.006.

[89] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov, "Spamming botnets: Signatures and characteristics," in *Proc. ACM SIGCOMM Conf. Data Commun.*, Seattle, WA, USA, 2008, pp. 171–182, doi: 10.1145/1402958.1402979.

[90] T. H. Nazer, M. Davis, M. Karami, L. Akoglu, D. Koelle, and H. Liu, "Bot detection: Will focusing on recall cause overall performance deterioration?" in *Social, Cultural, and Behavioral Modeling*, vol. 11549, R. Thomson, H. Bisgin, C. Dancy, and A. Hyder, Eds. Cham, Switzerland: Springer, 2019, pp. 39–49, doi: 10.1007/978-3-030-21741-9_5.

[91] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, and F. Menczer, "BotOrNot: A system to evaluate social bots," 2016, pp. 273–274, *arXiv:1602.00975*. [Online]. Available: http://arxiv.org/abs/1602.00975

[92] K. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, and F. Menczer, "Arming the public with artificial intelligence to counter social bots," *Hum. Behav. Emerg. Technol.*, vol. 1, no. 1, pp. 48–61, Jan. 2019, doi: 10.1002/hbe2.115.

[93] V. S. Subrahmanian *et al.*, "The DARPA Twitter bot challenge," *Computer*, vol. 49, no. 6, pp. 38–46, Jun. 2016, doi: 10.1109/MC.2016.183.

[94] O. Varol, E. Ferrara, C. Davis, F. Menczer, and A. Flammini, "Online human-bot interactions: Detection, estimation, and characterization," in *Proc. 11th Int. Conf. Web Soc. Media*, 2017, pp. 280–289. Accessed: Jan. 1, 2017. [Online]. Available: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15587/14817

[95] E. Ferrara, "Measuring social spam and the effect of bots on information diffusion in social media," in *Complex Spreading Phenomena in Social Systems*. Cham, Switzerland: Springer, 2018, pp. 229–255.

[96] K.-C. Yang, O. Varol, P.-M. Hui, and F. Menczer, "Scalable and generalizable social bot detection through data selection," in *Proc. AAAI Conf. Artif. Intell.*, Apr. 2020, vol. 34, no. 1, Art. no. 1, doi: 10.1609/aaai.v34i01.5460.

[97] D. M. Beskow and K. M. Carley, "Bot-hunter: A tiered approach to detecting & characterizing automated activity on Twitter," in *Proc. Int. Conf. Social Comput., Behav.-Cultural Modeling Predict. Behav. Represent. Modeling Simulation*, Washington, DC, USA, Jul. 2018, pp. 1–8, doi: 10.1007/978-3-319-93372-6.

[98] M. Sayyadiharikandeh, O. Varol, K.-C. Yang, A. Flammini, and F. Menczer, "Detection of novel social bots by ensembles of specialized classifiers," in *Proc. 29th ACM Int. Conf. Inf. Knowl. Manage.*, New York, NY, USA, Oct. 2020, pp. 2725–2732, doi: 10.1145/3340531.3412698.

[99] M. Heidari, J. H. Jones, and O. Uzuner, "Deep contextualized word embedding for text-based online user profiling to detect social bots on Twitter," in *Proc. Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2020, pp. 480–487, doi: 10.1109/ICDMW51313.2020.00071.

[100] Y. Wu, N. Cao, D. Gotz, Y.-P. Tan, and D. A. Keim, "A survey on visual analytics of social media data," *IEEE Trans. Multimedia*, vol. 18, no. 11, pp. 2135–2148, Nov. 2016, doi: 10.1109/TMM.2016.2614220.

[101] S. Chen, L. Lin, and X. Yuan, "Social media visual analytics," *Comput. Graph. Forum*, vol. 36, no. 3, pp. 563–587, Jun. 2017, doi: 10.1111/cgf.13211.

[102] M. Khayat, M. Karimzadeh, J. Zhao, and D. S. Ebert, "VASSL: A visual analytics toolkit for social spambot labeling," *IEEE Trans. Vis. Comput. Graphics*, vol. 26, no. 1, pp. 874–883, Jan. 2020, doi: 10.1109/TVCG.2019.2934266.

[103] Y. Shi, Y. Liu, H. Tong, J. He, G. Yan, and N. Cao, "Visual analytics of anomalous user behaviors: A survey," May 2019, *arXiv:1905.06720*. Accessed: May 26, 2021. [Online]. Available: http://arxiv.org/abs/1905.06720

[104] S. Cresci, "A decade of social bot detection," *Commun. ACM*, vol. 63, no. 10, pp. 72–83, Sep. 2020, doi: 10.1145/3409116.

[105] J. Zhang, R. Zhang, Y. Zhang, and G. Yan, "The rise of social botnets: Attacks and countermeasures," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1068–1082, Nov. 2018, doi: 10.1109/TDSC.2016.2641441.
[106] T. W. Malone, "Modeling coordination in organizations and markets," *Manage. Sci.*, vol. 33, no. 10, pp. 1317–1332, Oct. 1987, doi: 10.1287/mnsc.33.10.1317.
[107] R. Axelrod and W. D. Hamilton, "The evolution of cooperation," *Science*, vol. 211, no. 4489, pp. 1390–1396, 1981, doi: 10.1126/science.7466396.
[108] S. A. West, A. S. Griffin, and A. Gardner, "Evolutionary explanations for cooperation," *Current Biol.*, vol. 17, no. 16, pp. R661–R672, Aug. 2007, doi: 10.1016/j.cub.2007.06.004.
[109] K. Binmore, *Natural Justice*. London, U.K.: Oxford Univ. Press, 2005. [Online]. Available: https://books.google.com/books?id=vV1PuLVl_vsC
[110] H. Gintis, S. Bowles, R. T. Boyd, and E. Fehr, *Moral Sentiments and Material Interests: The Foundations of Cooperation in Economic Life*. Cambridge, MA, USA: MIT Press, 2005. [Online]. Available: https://books.google.com/books?id=jsVpDIIGzQoC
[111] D. Nettle, *Evolution and Genetics for Psychology*. Oxford, U.K.: OUP, 2009.
[112] R. Cooper, D. V. DeJong, R. Forsythe, and T. W. Ross, "Communication in coordination games," *Quart. J. Econ.*, vol. 107, no. 2, pp. 739–771, May 1992, doi: 10.2307/2118488.
[113] D. P. Myatt and C. Wallace, "Evolution, teamwork and collective action: Production targets in the private provision of public goods," *Econ. J.*, vol. 119, no. 534, pp. 61–90, Jan. 2009.
[114] S. Goyal and F. Vega-Redondo, "Network formation and social coordination," *Games Econ. Behav.*, vol. 50, no. 2, pp. 178–207, Feb. 2005, doi: 10.1016/j.geb.2004.01.005.
[115] H. P. Young, "The dynamics of social innovation," *Proc. Nat. Acad. Sci. USA*, vol. 108, no. 4, p. 21285, Dec. 2011, doi: 10.1073/pnas.1100973108.
[116] M. S. Chwe, "Structure and strategy in collective action," *Amer. J. Sociol.*, vol. 105, no. 1, pp. 128–156, Jul. 1999, doi: 10.1086/210269.
[117] M. S.-Y. Chwe, "Communication and coordination in social networks," *Rev. Econ. Stud.*, vol. 67, no. 1, pp. 1–16, Jan. 2000.
[118] M. O. Jackson and A. Watts, "On the formation of interaction networks in social coordination games," *Games Econ. Behav.*, vol. 41, no. 2, pp. 265–291, Nov. 2002, doi: 10.1016/S0899-8256(02)00504-3.
[119] M. O. Jackson and A. Wolinsky, "A strategic model of social and economic networks," *J. Econ. Theory*, vol. 71, no. 1, pp. 44–74, Oct. 1996, doi: 10.1006/jeth.1996.0108.
[120] S. Al-Khateeb and N. Agarwal, "Understanding strategic information manoeuvres in network media to advance cyber operations: A case study analysing pro-russian Separatists' cyber information operations in crimean water crisis," *J. Baltic Secur.*, vol. 2, no. 1, pp. 6–27, Jun. 2016.
[121] L. A. Overbey, B. Ek, K. Pinzhoffer, and B. Williams, "Using common enemy graphs to identify communities of coordinated social media activity," in *Social, Cultural, and Behavioral Modeling*. Cham, Switzerland: Springer, 2019, pp. 92–102.
[122] M. Alassad, M. N. Hussain, and N. Agarwal, "Developing graph theoretic techniques to identify amplification and coordination activities of influential sets of users," in *Social, Cultural, and Behavioral Modeling*. Cham, Switzerland: Springer, 2020, pp. 192–201.
[123] P. R. Monge and N. Contractor, *Theories of Communication Networks*. London, U.K.: Oxford Univ. Press, 2003. [Online]. Available: https://books.google.com/books?id=X9PQCwAAQBAJ
[124] U. Brandes and D. Fleischer, "Centrality measures based on current flow," in *Proc. STACS*, vol. 3404, V. Diekert and B. Durand, Eds. Berlin, Germany: Springer, 2005, pp. 533–544, doi: 10.1007/978-3-540-31856-9_44.
[125] L. Hossain and S. Uddin, "Design patterns: Coordination in complex and dynamic environments," *Disaster Prevention Manage., Int. J.*, vol. 21, no. 3, pp. 336–350, Jun. 2012, doi: 10.1108/09653561211234516.
[126] N. Kapucu, "Interorganizational coordination in dynamic context: Networks in emergency response management," *Connections*, vol. 26, no. 2, pp. 33–48, 2005.
[127] M. Granovetter, "The strength of weak ties," *Amer. J. Sociol.*, vol. 78, no. 6, pp. 1360–1380, 1973.
[128] K. S. K. Chung and L. Hossain, "Measuring performance of knowledge-intensive workgroups through social networks," *Project Manage. J.*, vol. 40, no. 2, pp. 34–58, Jun. 2009, doi: 10.1002/pmj.20115.
[129] K. David, "The strength of strong ties: The importance of philos in organizations," *Netw. Organ. Struct. Form Action*, pp. 216–239, 1992.
[130] D. Z. Levin and R. Cross, "The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer," *Manage. Sci.*, vol. 50, no. 11, pp. 1477–1490, Nov. 2004, doi: 10.1287/mnsc.1030.0136.
[131] I. Himelboim, M. A. Smith, L. Rainie, B. Shneiderman, and C. Espina, "Classifying Twitter topic-networks using social network analysis," *Soc. Media Soc.*, vol. 3, no. 1, pp. 1–13, Jan. 2017, doi: 10.1177/2056305117691545.
[132] A. Arif, L. G. Stewart, and K. Starbird, "Acting the Part: Examining information operations within #BlackLivesMatter discourse," *Proc. ACM Hum.-Comput. Interact.*, vol. 2, pp. 1–27, Nov. 2018, doi: 10.1145/3274289.
[133] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: Homophily in social networks," *Annu. Rev. Sociol.*, vol. 27, no. 1, pp. 415–444, Aug. 2001, doi: 10.1146/annurev.soc.27.1.415.
[134] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333–339, Nov. 2019, doi: 10.1016/j.jbusres.2019.07.039.
[135] G. Wong, T. Greenhalgh, G. Westhorp, J. Buckingham, and R. Pawson, "RAMESES publication standards: Meta-narrative reviews," *BMC Med.*, vol. 11, no. 1, p. 20, Jan. 2013, doi: 10.1186/1741-7015-11-20.

Tuja Khaund received the B.S. degree in computer science, the M.S. degree in information science, and the Ph.D. degree in computer and information sciences from the University of Arkansas at Little Rock, Little Rock, AR, USA, in 2015, 2017, and 2021, respectively.

She is currently an Alumni of the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS). Her research interests include social computing, social media mining, behavior-cultural modeling, social cyber forensics, network science, data science, and graph theory.

Baris Kirdemir received the B.S. degree in international relations from Ege University, İzmir, Turkey, and the M.Phil. degree in international relations from the National Defence University, Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in computer and information sciences with the University of Arkansas at Little Rock, Little Rock, AR, USA.

In 2019, he was a Visiting Research Fellow with the NATO Strategic Communications Centre of Excellence, Riga, Latvia, and a Cyber Policy Fellow with the Robert Bosch Foundation GmbH, Stuttgart, Germany, and the Centre for Economics and Foreign Policy Studies, Istanbul, Turkey. His research interests include computational propaganda, social cybersecurity, computational conflict research, machine behavior, and algorithmic bias.

Nitin Agarwal (Member, IEEE) is currently the Maulden-Entergy Endowed Chair and a Distinguished Professor of information science with UA-Little Rock, Little Rock, AR, USA. He is also the Founding Director of the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS). His research interests include the intersection of social computing, behavior-cultural modeling, collective action, social cyber forensics, artificial intelligence, data mining, and machine learning. His research aims to push the boundaries of our understanding of digital and cyber social behaviors that emerge and evolve constantly in the modern information and communication platforms. From Saudi Arabian women's right to drive cyber campaigns to Autism awareness campaigns to ISIS' and anti-West/anti-NATO disinformation campaigns, at COSMOS, he is directing several projects that have made foundational and applicational contributions to social and computational sciences, particularly in understanding coordinated cyber campaigns.

Huan Liu (Fellow, IEEE) received the B.Eng. degree in computer science and electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 1983, and the Ph.D. degree in computer science from the University of Southern California, Los Angeles, CA, USA, in 1989.

He is currently a Professor of computer science and engineering with Arizona State University, Tempe, AZ, USA. His well-cited publications include books, book chapters, encyclopedia entries, conference papers, and journal articles. His current research interests include data mining, machine learning, social computing, and artificial intelligence, investigating problems that arise in many real-world applications with high-dimensional data of disparate forms, such as social media, group interaction and modeling, data preprocessing (feature selection), and text web mining.

Dr. Liu is also a Fellow of the Association for Computing Machinery (ACM), the American Association for Artificial Intelligence (AAAI), and the American Association for the Advancement of Science (AAAS). He was recognized for excellence in teaching and research in computer science and engineering at Arizona State University. He serves on journal editorial boards and numerous conference program committees. He is also a Founding Organizer of the International Conference Series on Social Computing, Behavioral Cultural Modeling, and Prediction.

Fred Morstatter received the B.S. and Ph.D. degrees in computer science from Arizona State University, Tempe, AZ, USA, in 2011 and 2017, respectively.

He is currently a Computer Scientist with the Information Sciences Institute, University of Southern California, Los Angeles, CA, USA. His well-cited publications include books, book chapters, conference papers, and journal articles. His current research interests include social media mining, data science, data mining, and machine learning.