Dark Cycles: Social Engineering and Political Chatbots in Netanyahu's 2019 Election Campaigns

ANAT BEN-DAVID
The Open University of Israel, Israel[1]

ELINOR CARMI
City University London, UK

This study investigates the potential adverse effects of political chatbots operating as peer-to-peer propaganda tools that evade public and regulatory oversight. We analyze a specific case of a Facebook Messenger chatbot used by Benjamin Netanyahu's campaign during 2 Israeli elections in 2019. Applying the Walkthrough Method, we define "dark cycles" as a convergence of social engineering and dark patterns, characterized by 3 phases: reconnaissance (establishing connections and collecting data), training (using repetitive messaging and dark-pattern choice architectures to shape perspectives), and activation (instructing users to perform specific tasks). Although centered on this case, our findings suggest broader implications for studying political chatbots as AI technologies evolve. We also address the asymmetric power dynamics these chatbots create, highlighting their role in shaping compliant data subjects under surveillance and automation.

Keywords: dark cycles, political chatbots, social engineering, dark patterns, peer-to-peer propaganda, digital campaigning, platform governance

The Cambridge Analytica scandal during the 2016 U.S. presidential election reshaped political campaigns. Described as "dirty politics" by Milan and van der Velden (2018), Donald Trump's campaign merged voter data with targeted digital ads and political nudging (Pybus, 2019), pushing legal and democratic boundaries. Cambridge Analytica created voter profiles based on online and offline behaviors, segmenting audiences into "universes" to tailor messages using A/B testing (Carmi, 2020a). This method influenced other political leaders globally. For example, Jair Bolsonaro's 2018 win in Brazil involved botnets and voter segmentation, and in India's 2019 elections, Narendra Modi's campaign used WhatsApp for targeted outreach and disinformation (Campbell-Smith & Bradshaw, 2019; Santini, Salles, & Tucci, 2021).

This article examines the use of an automated Messenger chatbot in Benjamin Netanyahu's campaign during two Israeli election cycles in 2019.

Between 2019 and 2021, Israel experienced a profound political crisis marked by contentious leadership struggles. Prime Minister Benjamin Netanyahu, Israel's longest-serving leader since 2009, faced legal challenges and corruption charges that undermined his hold on power amid a fractured political landscape. Netanyahu's Likud party and the main opposition, led by Benny Gantz's Blue and White alliance, could not form a stable coalition government, resulting in four inconclusive elections (Keren, 2022). This deadlock led to unprecedented electoral uncertainty and temporary government paralysis.

During these consecutive election cycles, political campaigns in Israel employed numerous "dirty politics" strategies, including the spread of fake news, the use of bot-operated accounts, and voter data collection via social media and election apps (Haleva-Amir, 2022). The existing regulatory framework's inadequacy in addressing contemporary digital campaigning tactics enabled the widespread use of experimental tools (Ben-David, 2023). Facebook Messenger's chatbots emerged as a new tool in digital campaigning, with several politicians using them to recruit volunteers and share content through their political pages (Ben-Porat & Lehman-Wilzig, 2020; Haleva-Amir, 2022). However, Netanyahu's campaign elevated this tool with a Messenger chatbot commonly known as the "Bibi-bot," which exemplified "dirty politics" by simulating direct interaction with Netanyahu while secretly collecting voter data, influencing opinions, and mobilizing supporters to perform tasks, including reporting on others' political views. This use of the Messenger chatbot highlights a distinctive approach to peer-to-peer propaganda, making the "Bibi-bot" a valuable case study for analyzing adversarial applications of political chatbots in election campaigns.

Netanyahu was among the first Israeli politicians to recognize the value of continuous communication with followers (Keren, 2022). He hired tech and PR professionals to adopt platforms like TikTok and Telegram to engage his audience and tailor messaging (Yavetz, 2022). Reports indicated that Netanyahu's Likud campaign engaged in dubious voter profiling, including a secret database classifying more than a million voters by political inclination (Haaretz Editorial, 2019). Other reports claimed that a network of fake Twitter accounts promoted Netanyahu (Bergman, 2019). Although Likud disputed these claims, there is consensus that Netanyahu's digital campaigning tactics are more sophisticated than any other political entity in Israel (Haleva-Amir, 2022; Yavetz, 2022).

Bots are, of course, not a new thing. The literature on political manipulation on social media emphasizes the role of automated agents, or social bots, as powerful tools in manipulating and shaping public opinion (Ferrara, Varol, Davis, Menczer, & Flammini, 2016; Woolley & Howard, 2016). Although social bots usually operate in many-to-many communication spaces, aiming to amplify divisive messages in public conversations (Dubois & McKelvy, 2019), recent developments in natural language processing and artificial intelligence (AI) gave rise to the use of interpersonal conversational robots, or chatbots, in political campaigns.

Chatbots are natural dialogue software mimicking human-to-human communication across various contexts (Adamopoulou & Moussiades, 2020). We define political chatbots as technologies embedded in private conversational channels (e.g., WhatsApp, Telegram, Messenger), where an automated account

mimics a conversation between a politician and a user using conversational AI or scripted interactions. Political chatbots can be developed using a programming language or a third-party development platform. The chatbot's architecture design can either be rule-based—matching user input to predefined responses— or based on machine learning and natural language processing, contextualizing responses beyond a single turn (Adamopoulou & Moussiades, 2020). Given that political chatbots are a relatively recent phenomenon, the few studies on political chatbots, thus far, focus on their effectiveness in influencing voter intentions and turnout (Kim & Lee, 2023; Mann, 2021) and on voter perceptions of automated agents (Ben-Porat & Lehman-Wilzig, 2020). However, little research addresses the potential misuse of political chatbots as an instrument for persuasion.

Political bots are part of digital manipulation tactics used in political campaigns, called *computational propaganda*. Woolley and Howard (2016) define the term as "the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion" (p. 45). Based on behavioral data and individual targeting, such manipulations enable new networked social engineering methods and shape public consent through opaque practices that exploit big data, surveillance, and computational modeling (Tufekci, 2014). Other scholars, such as Gehl and Lawson (2022), call these persuasion techniques *masspersonal social engineering*. According to them, this is:

> An emerging form of manipulative communication enabled by the unique affordances of the Internet and social media platforms. It brings together the respective tools and techniques of hackers and propagandists, interpersonal and mass communication, in an attempt to shape the perceptions and actions of audiences. (Gehl & Lawson, 2022, p. 4)

These affordances include the ability to instantly change, adapt, and customize different interfaces and features and target individuals with tailored environments and messages to push them to think and do specific things they usually do not do, otherwise known as dark patterns.

This article examines the potential adverse implications of political chatbots on voter persuasion, using Benjamin Netanyahu's election chatbot as a case study. Using the Walkthrough Method (Light, Burgess, & Duguay, 2018), recording our interactions with Netanyahu's chatbot, we coded the rhetoric, modalities, and interactional features to examine the ways the architectural, interface, and rhetorical design of conversational chatbots operate to manipulate people into doing something, especially in peer-to-peer communication channels. Our case study, therefore, demonstrates the potential misuse of political chatbots as a social engineering tool. Accordingly, our analysis is guided by the following questions:

RQ1:   *What were the chatbot's goals in terms of influencing opinion and actions?*

RQ2:   *Which choice architectures (i.e., conversational flows, interaction design) were used to meet these goals?*

RQ3:   *Which rhetorical persuasion techniques were used to meet these goals?*

It should be noted that these questions are not aimed at measuring actual influence, mobilization, voter turnout, or voter perceptions about their experiences with Netanyahu's chatbot. Instead, we seek to identify the negative implications of using dark patterns and deceitful political chatbots to engineer the opinions and actions of individual voters.

The following section reviews the literature on conversational chatbots, social engineering, and dark patterns. Then, we present the method and the findings of our case study. Finally, we discuss our findings by analyzing the asymmetric power relations resulting from under-the-radar digital advertising systems and personal political persuasion: social engineering strategies carried out through dark pattern architectural design in political chatbots.

From Social Bots to Political Chatbots

Developments in conversational AI gave rise to communicative robots—software mimicking human-to-human communication—in all walks of life (Natale, 2021). In politics, scholars examined the use of social bots to influence political campaigns and societal debates more broadly (Gehl & Bakardjieva, 2016; Woolley & Howard, 2016).

Politicians use social bots to appear more popular and shift discussions in their favor. These bots create a false impression of popularity and manipulate public opinion, suppressing civic engagement and hindering free speech (Woolley, 2016). Dubois and McKelvey (2019) show that political bots in Canada amplified conflictual messages and harassed people, leading to self-censorship and divisive discourse. Similar uses have been documented in elections in Venezuela (Forelle, Howard, Monroy-Hernández, & Savage, 2015), India (Neyazi, 2020), Japan (Schäfer, Evert, & Heinrich, 2017), and Russia (Stukal, Sanovich, Bonneau, & Tucker, 2017). These cases demonstrate that social bots mimic human behavior but exceed human capacities in speed, scale, and scope, allowing operators to quickly construct a distorted image of a political actor or issue (DiResta, Grossman, & Siegel, 2022).

Political chatbots are a relatively new phenomenon compared with the prevalence of social bots on public communication channels such as social media. We argue that although political chatbots embed many of the principles and techniques already described in the literature on computational propaganda (such as voter profiling, computational modeling, and personalized messaging), they are unique in their ability to employ personal persuasion techniques in unregulated, under-the-radar, private communication channels. In addition, political chatbots differ from targeted advertising since they offer a long-term, two-way interaction between the sender and the receiver. Through long-duration interpersonal engagement, political chatbots can collect more accurate data on voters' views; accordingly, such long-term commitment allows the chatbot's operators to mobilize voters into action.

Political chatbots also differ from other social bots in targeting individual voters rather than amplifying messages or creating false public impressions. Unlike Cambridge Analytica's approach of building psychological profiles based on third-party data from platforms like Facebook, political chatbots combine this third-party data with high-quality, first-party data collected directly through interactions with the bot. This highlights a gap in the literature about the operation of political chatbots in under-the-

radar communication channels. We address this gap by using Netanyahu's chatbot as a case study to explore its functions.

Engineering the Social

Decades before the rise of social bots, hackers have used various analog, digital, and social tools to influence and manipulate people toward specific ends, a practice commonly known as social engineering (Mitnick & Simon, 2002). Although there is no agreed-upon technique for social engineering in the hacker community, influence operations are broadly divided into four main stages, also known as "the attack cycle": (1) reconnaissance—collecting information from multiple sources to plan and conduct the operation. (2) establishing relations and rapport—connecting with the "target" to gain trust by using various methods such as phishing, impersonation, and "pretexting" (the act of inventing a scenario [the pretext] to persuade a target to release information or perform an action); (3) exploitation—using the information and rapport to get what is needed from the "target"; (4) achieving the goal (Yadav & Rao, 2015, p. 439). The goals vary from getting valuable information to scheming money from people.

There are several methods for luring people into doing something they would not normally do. Workman (2007, 2008) describes social engineering methods, such as "likeability," where people trust and comply with requests from people they find attractive, perceive as credible, and have unique expertise. Furthermore, social engineers use their "authority," which inflicts fear, meaning people obey orders to avoid negative consequences such as losing value. These character traits are coupled with continued commitment: people feel invested in a decision they make and maintain consistent behavior.

Computational propaganda and social engineering differ in scale and the communication channels used. Although social bots operate in many-to-many networks, social engineering relies on personal one-to-one communication to create an intimate relationship built on trust and simultaneously avoid being detected by others. Moreover, since social engineering is done by humans, its scope is limited.

As noted, masspersonal social engineering (Gehl & Lawson, 2022) links online propaganda with social engineering, emphasizing its scale. Gehl and Lawson (2022) argue that this approach, inspired by 1920s consent engineers, uses mass media, propaganda, and public relations to manage and manipulate populations rather than individuals. They term it "masspersonal" because it emphasizes the accessibility and personalization of messages over the communication channels. Social engineers use pretexts like social bots or personas to hide their true identities, enabling spying, data extraction, and profiling to create tailored messages that prompt specific responses.

This manipulation employs strategies such as gathering data on targets, creating fake personas to interact, mixing deception and friendliness, and abusing communication channels. Although the goals behind these strategies vary, they aim to change people's actions and attitudes. The process resembles the attack cycle, incorporating a mix of personalized and targeted messages. Social engineers' manipulation in these contexts is achieved through manipulative choice architectures commonly termed dark patterns, which we review in the following section.

When Patterns Go Dark

In the field of human–computer interaction, the term *dark patterns* refers to "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest" (Gray, Kou, Battles, Hoggatt, & Toombs, 2018, p. 1). The term refers to the manipulative application of principles of behavioral economics in online environments (Lavi, 2018). However, dark patterns have mainly been examined by behavioral economics.

Behavioral economics examines decision making through psychology, based on Kahneman and Tversky's (Kahneman, Slovic, & Slovic, 1982) bounded rationality theory, which posits that choice making involves an "automated" or "reflective" cognitive system. Experimental evidence shows that slight changes in context influence decisions, such as biases created by the order of presented choices. The term "choice architecture" (Thaler, Sunstein, & Balz, 2013) describes how decision making is shaped by the design of the environment or context in which choices occur.

One widely applied choice architecture from this field is the "nudge," which guides behavior or decision making without limiting choices (Thaler & Sunstein, 2008). Digital nudging has become prevalent across various domains. Proponents argue that it helps people make beneficial decisions, such as improving health or finances (Patel, Volpp, & Asch, 2018). However, these principles can be misused to benefit the choice architect rather than the user, leading to what are commonly called dark patterns.

Mathur and colleagues (2019) distinguish between five attributes of dark patterns: asymmetric (imposing unequal choices), covert (hiding the influence mechanism), deceptive (creating false beliefs by using affirmative misstatements, misleading statements, or omissions), information hiding (obscuring or delaying the presentation of the necessary information to users), and restrictive (reducing or eliminating the choices presented to users). Later, Mathur, Kshirsagar, and Mayer (2021) added the attribute of disparate treatment, where a specific group is treated differently than others. They further distinguish between two ways these attributes change a person's choice: change of the decision space (asymmetric, restrictive, disparate treatment, and covert) or manipulation of the information flow (deceptive, information hiding). Importantly, they outline the normative concerns arising from dark patterns. Such concerns include individual welfare (e.g., invasion of privacy), diminishing collective welfare, interference with regulatory objectives (e.g., consent management features not compliant with the GDPR), and individual autonomy, whereby interfaces undermine people's decision making.

Dark patterns are also applied at datafied user interfaces, where slick front end designs conceal back-end processes (Carmi, 2020a). Yeung (2017) argues that big data-driven nudging is dynamic, adapting to a person's responses to provide a personalized, unobtrusive environment she calls "hypernudge"—a form of "soft power" (Nye, 2004) prone to manipulation and abuse.

The architectural design of commercial chatbots aims to boost productivity and cut service costs by enabling enjoyable, informative, and time-saving conversations between services and customers (Adamopoulou & Moussiades, 2020). Conversational design elements—such as visual (e.g., avatars),

linguistic (e.g., jokes, personal language, emphatic responses), and interactional features (e.g., buttons, pretyped questions)—enhance consumer engagement with commercial chatbots (Silva & Canedo, 2024). Experimental evidence also shows that nudging through a "foot-in-the-door" technique, where minor requests precede larger commitments, increases compliance with service feedback requests (Adam, Wessel, & Benlian, 2021).

However, dark pattern design in conversational agents can manipulate consumers through deceptive cues. For example, agents might nudge users to share more identifiable data, personalizing future interactions (Thomaz, Salge, Karahanna, & Hulland, 2020). The ethical concerns of dark patterns in commercial chatbots are even more critical in political chatbots, where designers influence not just purchasing decisions but political thought and actions, affecting informed voting choices in democratic elections. The following section analyzes a political chatbot Israeli Prime Minister Benjamin Netanyahu used during two national election rounds in 2019.

Method

To study Netanyahu's Messenger chatbot, we follow the principles outlined by the *walkthrough method* for studying apps (Light et al., 2018). The method specifies a step-by-step engagement and documentation of the app to examine its "technological mechanisms and embedded cultural references to understand how it guides users and shapes their experiences" (Light et al., 2018, p. 882). By mimicking the app's everyday uses, the researcher can then analyze its environment of expected use: the app's vision, target user base, and scenarios of use; its operating model, business strategy, and revenue sources; and its governance rules and guidelines.

Data Collection

We set up two research accounts on Facebook, clicked Facebook ads from Netanyahu's official page that invited users to interact with him via the chatbot, and started engaging with Netanyahu's chatbot from the day it launched (January 25) until the end of the second election cycle in 2019 (September 24). All interactions with the bot were conducted via the Messenger App on Galaxy phones. One research account mimicked an avid Netanyahu supporter and clicked interaction buttons only indicating support for Netanyahu. The second account probed other conversational paths to document as many of the bot's conversational features and scenarios as possible.

We took real-time screenshots documenting every session the chatbot initiated: 29 conversations during the April 9 election campaign (from January 25 until April 24) and 19 during the September 17 election campaign (from June 26 until September 24). As we soon show, during the last days of each campaign, the bot's interface transformed into a canvassing system that could lead to hundreds of interactions. These interaction loops were not counted in the unique number of initiated conversations. After the election cycles ended, we accessed the chat history with the bot through a desktop browser and exported the chat history to a text file (n = 26,278 words). We also preserved the chat history in video format using screen capture software, scrolling down the chat history from the first to the last interaction

(43 minutes) to preserve the multimodal content of the messages posted by the bot while replaying all videos posted by the bot.

Coding and Analysis

We developed the initial coding book iteratively using the consensual qualitative research method (Hill et al., 2005). Three researchers independently coded a sample of the chatbot's interactions based on predefined categories—conversational features (e.g., free-form text, multiple-choice buttons), modalities (e.g., image, video, URL, emoji), and rhetorical devices (e.g., personal language, humor, requests, fear appeals, incitement). After this initial coding, we discussed the results to achieve consensus, refining our categories and definitions through multiple coding rounds until the entire database was coded. This iterative process allowed us to adapt the codebook, ensuring it was comprehensive and captured the chatbot's diverse strategies.

We repeated the consensual coding process, focusing on the bot's choice architectures that combine conversational features, modalities, and rhetorical devices to influence user opinions and actions. Three categories emerged from this phase, termed prescriptions: (1) influencing user opinions (e.g., quizzes inducing repetitive consent with statements); (2) influencing personal behavior (e.g., asking users to change their Facebook profile pictures); and (3) influencing peer behavior (e.g., asking users to call strangers through the app and read talking points; see Appendix 1 for the complete codebook).[2]

Findings

Our findings indicate that Netanyahu's chatbot followed three strategic stages, each characterized by distinct combinations of modalities, interactivity features, and rhetorical devices, detailed below (see Table 1 and Table 2). As the patterns identified were nearly identical across both election campaigns, our findings describe both campaigns for clarity, with examples tied to specific dates.

Stage 1

The first stage of the political chatbot's operation has two strategic goals: establishing a personal bond between the bot (pretexting as the prime minister) and the user and extracting direct and indirect data by using covert and deceptive dark patterns (Mathur et al., 2019). According to Messenger's terms of use, users must initiate conversations with a chatbot (Facebook, 2019b). After initiation, however, Messenger's API grants developers access to data collection and matching practices, including profile IDs, external customer data, and the ability to "authenticate a person's identity and link it with their Messenger account to securely add more features and information to the conversation" (Facebook, 2019a, para. 5). Consequently, users who initiated conversations with Netanyahu's chatbot likely (and unknowingly) submitted personal data to its operators on the back end.

---

[2] Appendix: Code Groups. Avalable at https://osf.io/jsh7m/files/osfstorage/6713c486e4929f40982ec5e4

Netanyahu's campaign used Facebook's targeted advertising system to lure users who liked his page into initiating interaction with the chatbot. In March 2019, Netanyahu's Facebook page ran 67 versions of targeted ads in which Netanyahu asked users: "What are the most pressing issues in these elections? I invite you to tell me in a private message here, on Facebook" (Netanyahu, 2019). The ads contained a "send message" button that directly linked the ad to the chatbot (see Figure 1). Previous research on Facebook political ads in Israel during that time showed that these ads targeted audiences by their political views, inferred through their profiles and liking newspaper pages (Ben-David, 2020).
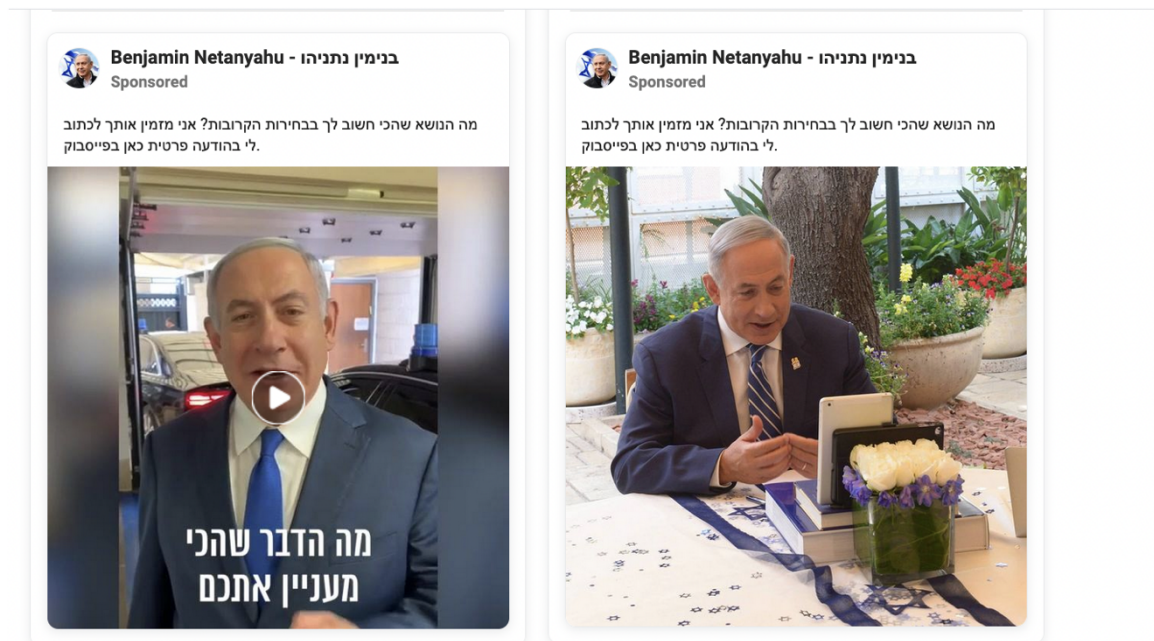

Figure 1. Two versions of Facebook ads inviting users to interact with Netanyahu's chatbot. Screenshots taken in 2019 from Facebook Ad Library (2019).[3]

The chatbot strategically leveraged Messenger's familiar affordances, such as profile pictures or the app's pop-up notifications, to impersonate interactions with users as though Netanyahu himself was chatting with his followers. Almost all interactions initiated by the chatbot contained personal language emphasizing that the sender is Netanyahu himself and the receiver is the individual user (for example: "Hello **to you**, this is Prime Minister Benjamin Netanyahu. In the near election, I **need you** more than ever. I'd be happy to keep in touch **with you** here on Facebook and **send you** private messages **from me**").[4] This extensive

---

[3] The screenshots were taken from the Ad Library in November 2023. As of October 2024, Facebook has removed the content of these ads, citing that "the disclaimer didn't comply with our policy for ads about social issues, elections, or politics." However, the ads' metadata remains accessible on the website. For a discussion on the limitations of the Facebook Ad Library as an archive, see Ben-David (2020).

[4] Literal translation from Hebrew, emphasis ours.

personal appeal combines rhetorical devices that increase affective engagement, such as urgency and neediness: "Good evening, **I need your help**. Would you **help me** and the Likud win the election?"

Figure 2 summarizes the chatbot's primary rhetorical devices. Alongside personal language, the bot frequently uses questions, requests, and orders, employing Hebrew gender-specific pronouns that reveal the user's gender was visible to the campaign via Messenger's API. Soon after establishing a personal connection, the chatbot sent propaganda videos featuring Netanyahu in various settings (e.g., a car, a military base), thanking the user for joining his daily routine as prime minister. Another video showed Netanyahu and a reality TV celebrity announcing an alternative news channel to be aired exclusively on Facebook Live. They promised that "[this channel], unlike the fake news media, will only tell the truth" (Netanyahu, personal communication, February 2, 2019). Like later campaign conversations, this video lacked interaction buttons. Throughout both campaigns, the most common rhetorical device combined with personal language was "no option to reply," where the chatbot posed rhetorical questions or made statements without providing answer buttons (see Figure 2).
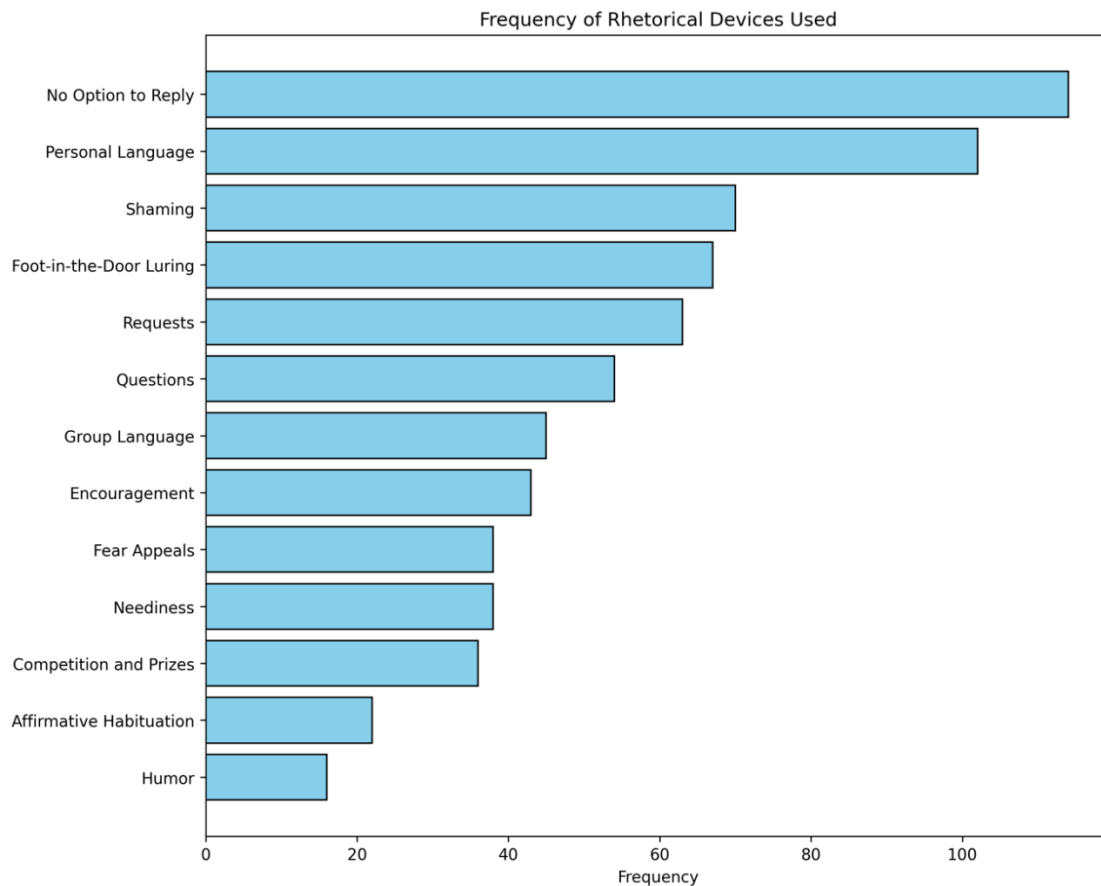

Figure 2. The chatbot's primary rhetorical devices.

Questions about the user's political opinions appeared nonchalantly between these videos. When seeking user information, the chatbot often combined personal language with a "foot-in-the-door" luring (Adam et al., 2021), starting with a general question ("Hello, this is Prime Minister Netanyahu, may I ask you a small question?"), followed by direct requests for information ("Have you voted for the Likud in the past?" or "Do you intend to vote for the Likud in the upcoming election?"). The bot used personal encouragement and affectionate emojis when the user complied with such requests. Figure 3 illustrates a February 17 conversational flow showcasing personal language, fear appeals, urgency, "foot-in-the-door" luring, and encouragement.
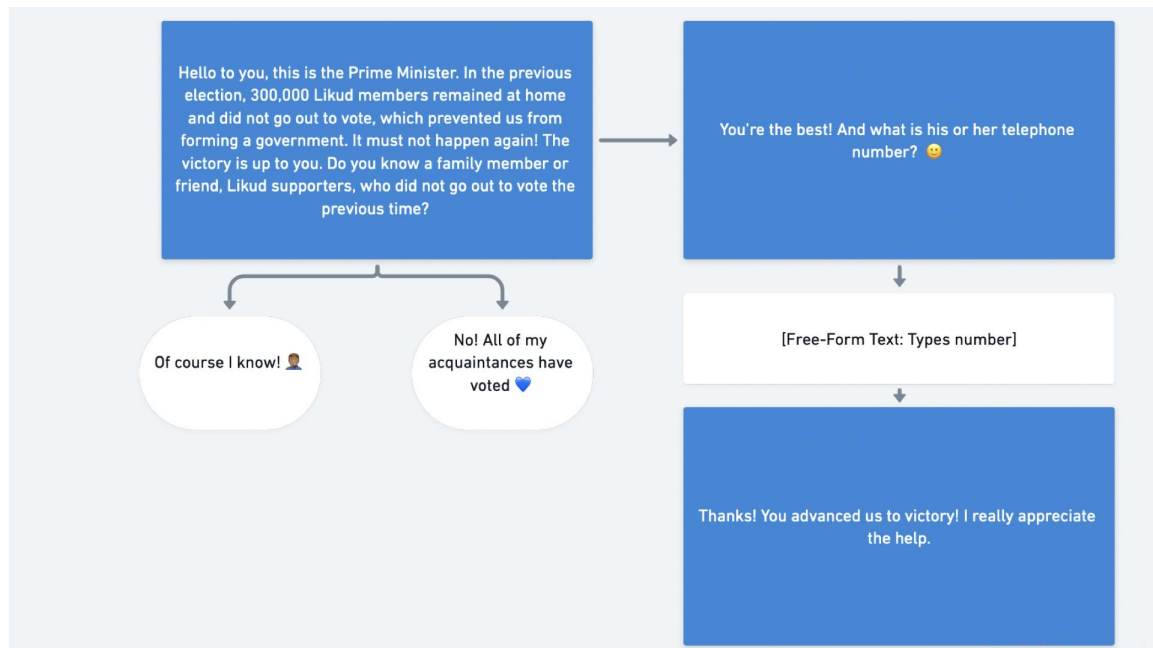

Figure 3. A reconstruction of a conversation initiated by Netanyahu's chatbot on February 17, 2019 (translated from Hebrew).

The timing of chatbot interactions is crucial for building intimacy and commitment through rhythm and intensity, a concept we term *rhythmedia*—how platforms and political actors shape tempo-spatial experiences by altering algorithmic architecture to create specific sociality (Carmi, 2020b). First, there is an asymmetry in conversation initiation, with the chatbot always starting exchanges. When we tried to initiate conversations, the bot consistently replied, "I got your message; I'll be in touch soon." This asymmetry establishes the chatbot's authority and the user's passive role. Second, as Election Day approached, the chatbot increased its nudging frequency to pressure users into action.

Stage 2

In the second stage (weeks 3–10 of the April campaign [February 3–March 23], weeks 2–10 in the September campaign [July 2–August 25]), the political bot initiated interactions that combined video

messages—to which there was no option to reply—with gamified quizzes that mixed everyday life scenarios and political opinions. Common rhetorical devices in this stage combine rhetorical questions with incitement against political rivals and the news media. For example, a message from March 16 incited against Netanyahu's opponent, Benny Ganz: "Say, would you vote for a candidate supported by Iran?" The available response buttons seem like multiple-choice answers but are, in fact, variations of "no": "No way"; "Never"; "Are you nuts?" (Netanyahu, personal communication, March 16, 2019).

Another example of inducing agreement through repetition is gamification. In the April election campaign, the chatbot initiated a looping interaction based on the popular Israeli social game, "Countries and Capitals by First Letter." On March 23, the bot sent a video of Netanyahu playing this game with an actor. In the video, the actor randomly picks a first letter, after which Netanyahu boasts the names of countries that were part of his successful diplomatic efforts. A follow-up message from Netanyahu asked: "I hope you liked the video. Say, do you want to play with me?" The single-answer button included slang words that insinuated familiarity and playfulness: "Yalla, I flow with you" (wherein Hebrew, "Yalla" is slang for "let's go"). The interaction evolved into a looping gamified quiz, reconstructed in Figure 4.
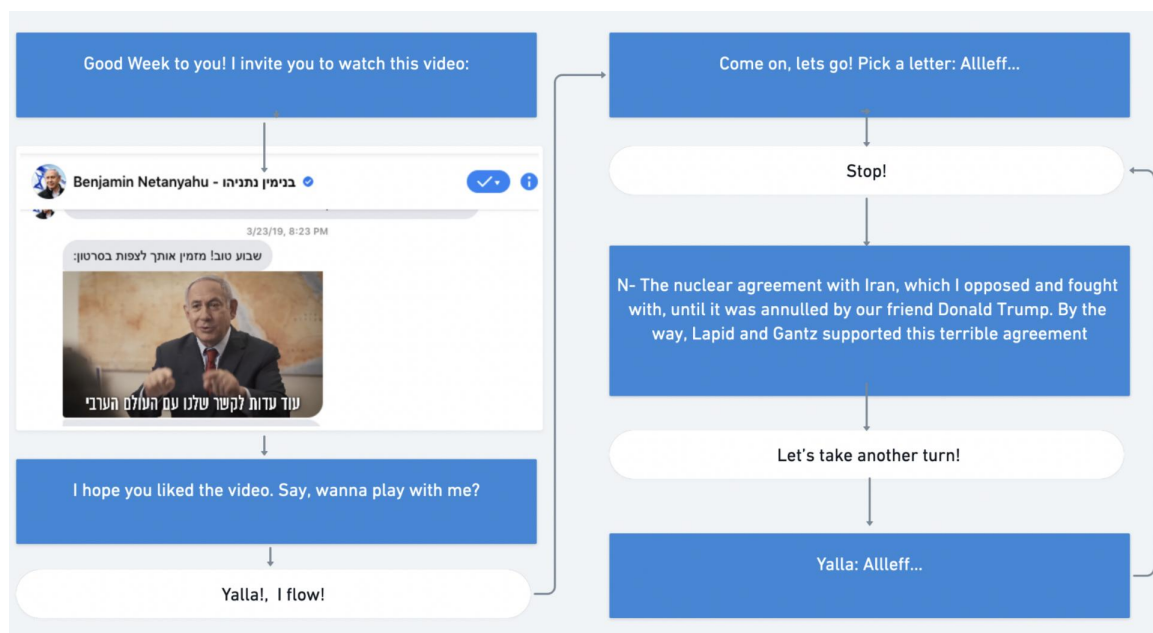
Figure 4. A gamified quiz interaction from March 23, 2019. Translated from Hebrew.

Depending on the user, this interaction could loop, showing another achievement starting with another random letter each time. Through message repetition and gamification, the user is continuously exposed to Netanyahu's accomplishments, with no options to disagree or argue. Another example from July 25 follows Netanyahu's ongoing strategy to attack the news media (Rogenhofer & Panievsky, 2020). A rhetorical question, followed by a video showing a political correspondent for a leading TV channel, reads: "Would you let the news media confuse you?" Again, the available multiple-choice buttons are synonymous:

"Never, No way," and "They are detached from reality." To each button, the corresponding reply was: "Glad to hear! Obviously," and "You are right."

Table 1. The Chatbot's Stages: Strategic Goals, Affordances, and Rhetoric.

Stage	Strategic goals	Affordances/Modalities	Rhetoric
I	Covert and overt data collection Personal connection	"Get Started" button Multiple-choice buttons Free-form text	Foot-in-the-door luring Personal language Questions
II	Influence opinions	Quizzes Emojis Video Single-answer buttons	Affirmative habituation Rhetorical questions Incitement Gamification
III	Influence personal action Influence peers' actions Collecting data about others Reinforcing commitment	Chatbot invites Share buttons Scripts Dialing buttons Free-form text Emojis	Neediness Fear appeals Requests and orders Collective language Encouragement Prizes

Table 2. Emojis Used per Stage in Both Election Campaigns.

Stage	Interactions containing emojis	Emojis used
I	7/17	😍😊😇😄 💪👍
II	8/18	😉😩😂😍 🙏💪💥💰🕵️🔍 ♂️❤️👩‍🦰🏄 😍🕺 😎🍿🥰🕵️💙👎
III	12/12	😄😍😉😇😊 👎👍🙏💪 💙🖤

Stage 3

The third stage's strategic goal is to mobilize the user to perform specific tasks. For instance, on February 1 (week 2 of the April campaign), the chatbot urged the user to change their Facebook profile

picture. On July 25 (week 5 of the September campaign), it requested personal data of family and friends who are Likud supporters. Although such action requests appeared sporadically in earlier stages, major mobilization occurred about a week before election day in both campaigns (March 23 and September 8) when the chatbot shifted to a virtual canvassing system. Here, we noticed a divergence in messages sent to the two research accounts. Although the bot initiated identical interactions in the first two stages, only the account that had shown support for Netanyahu—by indicating intent to vote for him in the first stage—was contacted in the third.

In this phase, the chatbot urgently asked the user to call random people and follow orders. Figure 5 describes the looping script of the canvassing interaction. It starts with a "foot-in-the-door" luring exchange where Netanyahu urgently asks for the user's help. When the user presses the consent button, the bot asks the user to follow directions closely and then sends scripts for calls.
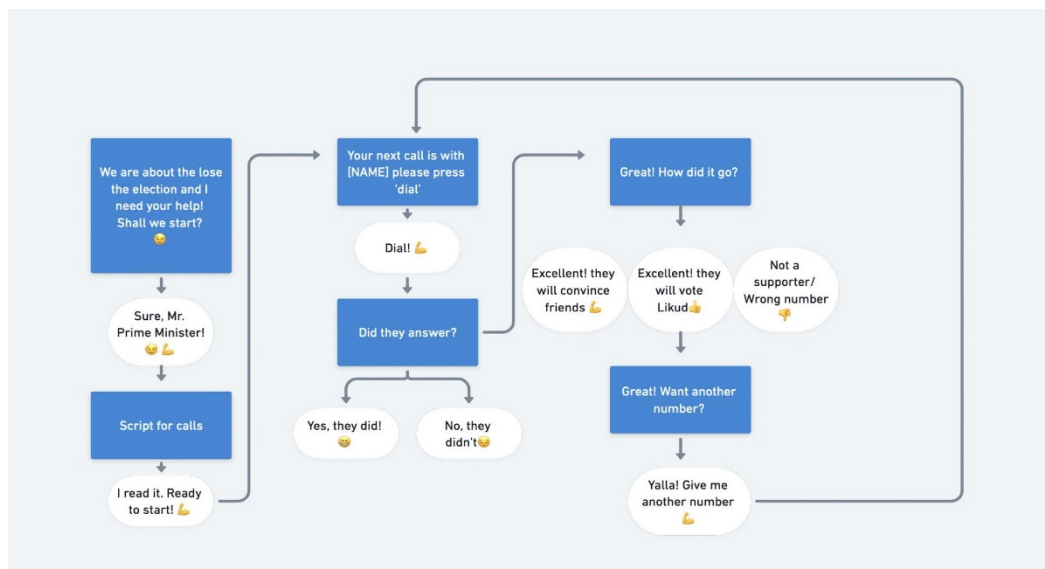

Figure 5. The conversational flow of the chatbot's canvassing system.

After the user confirms understanding the script, the chatbot prompts her to call a random person. The answer buttons—linking directly to the phone's dialer—contain the contact details of that person, pulled from a back-end database. An interaction loop follows: after sending the contact details, the bot asks the user to report the call's outcome (with buttons indicating if the voter is a supporter, a nonsupporter, or undecided) and offers another call. This quality assurance process refined the campaign's voter profiling data while involving the user.

In this stage, the chatbot's affordances and rhetorical devices shifted. Interactions included dialing buttons, single-answer buttons to reinforce consent with the call's script, and multiple-choice buttons for reporting the call's outcome as part of QA (see Table 1). Personal language shifted to group language, emphasizing collective efforts for Netanyahu. The user no longer interacted with Netanyahu but with a

system. For example, pressing "give me another telephone number" after 10:00 p.m. prompted the bot to reply, "The system is closed for the night. We'll continue tomorrow." The temporal aspect of rhythmedia reappears as the bot directs users on when to act. New scripts were sent every few hours, creating frequent nudging and urgency.

Occasionally, the bot sent video and audio messages from Netanyahu, encouraging users to keep making phone calls and offering a chance to appear on a Facebook Live broadcast with him for those who made the most calls. The scripts users were required to read conveyed urgency and fear, intensifying as Election Day approached. The incitement escalated, violating Israeli law and Facebook's community standards. For example, on September 10, a week before Election Day, one talking point read:

> *** Attention, new script *** Hello {first name}, my name is ____, and I'm a volunteer for Prime Minister Netanyahu. I'm calling you because you can determine our country's future on Tuesday. Prime Minister Netanyahu brings a right-wing policy of a Jewish state, security, and a strong Israel. I'm donating my time because a dangerous left-wing government should not form with Lapid, Odeh, Gantz, and Liberman next week. A secular, weak, left government that trusts the Arabs who want to annihilate us all—women, children, and men—and will allow a nuclear Iran to destroy us. We must not let that happen! So I ask you to be the Prime Minister's Messenger, bring three friends and family next Tuesday, and see that they vote Likud. Thanks, {first name}, I trust you!

The script's incitement against Israeli Arabs prompted civil society organizations to petition the Central Elections Committee (CEC) for hate speech. In response, Facebook suspended the chatbot for 24 hours for violating community standards. However, the campaign continued testing legal boundaries by sending targeted, under-the-radar messages to supporters, avoiding public scrutiny. Although Israeli Elections Law prohibits publishing polls four days before the election, on September 15, two days before the election, the chatbot posted an image showing expected vote distribution, warning, "According to our internal polls, we are losing the election." After a second petition, the CEC ordered Facebook to suspend the chatbot for five hours on Election Day (Kershner, 2019).[5]

Discussion: Dark Cycles During Elections

Our findings suggest that the "Bibi-bot" serves as a clear example of how social engineering practices and dark pattern interaction design converge within political chatbots—a phenomenon we term *dark cycles*. This concept refers to the strategic use of dark-pattern design coupled with long-term social engineering tactics that lure, engage, and activate targets to achieve specific political objectives. Netanyahu's chatbot exemplifies this by adopting social engineers' communicative strategies while exploiting social media platforms' affordances through dark patterns. *Dark cycles* is a type of political communication that builds on multiple convergences of entities, strategies, and communication channels. First, it converges the politician's public persona with social automation to exert one-to-one influence at scale. Second, it uses

---

[5] Fair disclosure: Anat Ben-David was one of the petitioners to the CEC based on the evidence collected in real-time for this research.

peer-to-peer, stage-based persuasion techniques afforded by under-the-radar social engineering. Third, it manipulates different interface affordances offered by Facebook's Messenger chatbot by using dark-pattern attributes in private channels easily hidden from others. This section discusses the three stages of *dark cycles*—(1) reconnaissance, (2) training, and (3) activation—and how they relate to the literature we covered above. It is important to emphasize that although the progression of the cycle's stages is chronological, in some instances, the stages cooccur.

Stage 1—Reconnaissance

The first stage, *reconnaissance*, involves the bot establishing a personal connection with the user while collecting data, similar to social engineers' pretexting—fabricated identities or scenarios designed to manipulate or deceive (Gehl & Lawson, 2022). In this case, the Bibi-bot acts as a pretext, creating the illusion of personal engagement with Netanyahu while being an automated bot. As Gehl and Lawson (2022) observe, "identity performances—including pretexts—work insofar as they are recognized and legitimated by other members of a community" (p. 100). The Bibi-bot's pretexting builds on the personalization trend in Israeli politics, especially Netanyahu's long-time use of personalized rhetoric on social media (Bronstein, Aharony, & Bar-Ilan, 2018). This impersonation, we argue, leverages deceptive dark patterns by creating false beliefs and misleading users.

As our data show, political chatbots' operation in "under-the-radar" communication channels allows avoiding external scrutiny. First, combining one-to-one communication channels with personal persuasion affords under-the-radar messaging that cannot occur in public communication channels. Social bots operate on social media platforms to influence public opinion by amplifying or distorting public conversations (Dubois & McKelvy, 2019). By contrast, peer-to-peer political chatbots allow their operators, just like social engineers, to capitalize on the politician's authentic identity and attractiveness. As the literature on social engineering has shown, the private setting of direct messaging may increase followers' sense of intimacy and trust (Mitnick & Simon, 2002). The use of automation in dark cycles allows influencing individuals at scale, as Gehl and Lawson argue in Masspersonal Social Engineering (2022), but differ in that here we are dealing with the bot pretexting as the politician himself.

By embedding a chatbot in a private communication channel within Facebook, the platform blurs the lines between public and private communication, allowing smooth transitions between channels and further exploitation of personal and networked behavior. Netanyahu's campaign pretargeted users by political views, luring them into initiating conversations and using dark patterns to expose profile information for data processing covertly. This liminality allowed the chatbot to send controversial messages to a targeted audience without appearing on Netanyahu's official Facebook page, avoiding scrutiny from the platform and election regulations. Although petitions were made to the Israeli CEC, the messages had already reached their targets by the time the chatbot was suspended.

Stage 2—Training

We term the second stage *training*, where the chatbot uses repetitive messages, games, conversational features, and rhetoric to persuade users to think in specific ways without options to

disagree. This stage employs cognitive persuasion techniques, such as repetitive agreement with predetermined messages (Cacioppo & Petty, 1979). The bot aims to influence opinions through scripted conversations with limited interactivity (Carmi, 2020b). The user reads the words on a single-answer button, clicks it, and the words reappear as though they are her own, creating an illusion of conformity and identification with the chatbot's messages. This process leaves no room for disagreement or alternative actions, similar to the restrictive attribute noted by Mathur and colleagues (2019), which eliminates choice (Mathur et al., 2021). This stage impacts individual welfare (personal data extraction), collective welfare (extraction of others' data), regulatory objectives (propaganda spread), and individual autonomy (eliminating choice and discussion).

Just as social bots spread political propaganda on social media (Caldarelli, De Nicola, Del Vigna, Petrocchi, & Saracco, 2020), the political chatbot shaped what voters should focus on: Netanyahu's achievements, media lies, opponents' failures, and the threat of Arab voters. These topics served as social engineering pretexts (Workman, 2007), setting the political agenda. Simultaneously, affective rhetoric, emojis, and interactive features masked the one-directional conversations driven by dark-pattern design (Kowald & Bruns, 2020). Features like no-reply options, single-answer buttons, and synonymous multiple-choice buttons restricted users from expressing views or raising other concerns, highlighting asymmetric and information-hiding dark patterns.

Stage 3—Activation

The third stage, *activation*, involves the chatbot directly asking users to perform specific tasks. Unlike traditional social engineering focused on system penetration, as Gehl and Lawson (2022) note, where "the humans they control and manipulate are not the end goal: penetrating the system itself is" (p. 145), the Bibi-bot targets individuals. It aims to influence users' thoughts—convincing them Netanyahu is the only viable candidate—and actions—prompting them to vote for him and persuade others. Compliance is rewarded with encouragement and promises of prizes, leveraging Netanyahu's likability and authority (Workman, 2007, 2008). It uses foot-in-the-door techniques to guide users to specific tasks. Additionally, the chatbot transforms into a canvassing system, turning the end-user into a "botified" agent expected to perform microlabor tasks for Netanyahu.

The chatbot initially engages the user with prescripted conversations, trains her to comply with these scripts, and then provides scripts to engage others—essentially turning the user into a bot herself. This process includes sharing personal contact details extracted by the Likud party from a back-end database to pressure individuals to vote for Netanyahu. Users were also asked to perform quality assurance, reporting whether the canvassing was successful. This repetitive botification reflects Mathur and colleagues' (2021) concerns about dark patterns, specifically interference with regulatory objectives and diminishing collective welfare and individual autonomy.

Finally, the Bibi-bot employed rhythmedia to shape users' experiences (Carmi, 2020b). Our analysis shows that each stage had distinctive order, timing, rhythm, and specific rhetorical and interface tempo. The single-answer button quizzes in the training stage, followed by the canvassing loops in the activation stage, reinforced learning through repetition (Cacioppo & Petty, 1979). As Election Day approached, nudging

rhythms intensified, using rhetoric to instill urgency and emphasize the importance of actions at that moment. Additionally, the bot dictated when it was not the right time to act. Thus, rhythmedia functioned as a dark pattern—structuring urgency and timing to pressure users into action.

Conclusion: The Rise of Automated Personal Persuasion

This article contributes to the literature on computational propaganda, social engineering, and dark patterns by analyzing a case study showing how these elements combine within political chatbots to manipulate users. Although the Bibi-bot is a distinctive case, it may represent a broader trend as AI technologies advance, highlighting the importance of studying such cases for their increasing relevance in the political sphere.

Based on our findings, we conceptualized *dark cycles* as a political communication tool converging social engineering, dark patterns, and conversational agents. Such tools also converge with public and private communication channels in ways that give rise to the automation of personal persuasion techniques. The Walkthrough Method allowed for interpolating the political chatbot's vision and desired uses. We showed how the Bibi-bot's dark cycles combined specific rhetoric borrowed from social engineers and propaganda, dark patterns, and modalities to shape citizens to think in prescribed scripts and act on requests from their leader.

The use of the *dark cycles* extended beyond the techniques that the literature describes concerning political campaigns' use of social bots to shape opinions, create a buzz, or increase the volume of social media conversations (Keller & Klinger, 2019). Instead, the political chatbot was designed to impersonate a political leader and lure, manipulate, and mobilize individual Likud supporters into performing specific tasks, from changing their profile pictures to providing friends' personal data and reporting on their political views. The campaign trained and activated users to act as volunteers performing crowdsourced canvassing tasks without pay, building on their affective willingness to engage in "aspirational labor" for their beloved politician (Ben-David, 2023; Irani, 2015). Thus, *dark cycles* aim to produce, control, and manage the individual's political agency, engineering what, how, and when they should operate in their political context.

Netanyahu's chatbot campaigns and the Cambridge Analytica scandal have a shared premise that voters' behavior can be engineered through behavioral data, targeted messages, and conversational dark patterns that appear as choice architectures. Netanyahu's chatbot campaigns relied heavily on behavioral economics, borrowing from principles outlining when and how choice architectures induce desired action (Thaler et al., 2013). Conducting these in under-the-radar communication channels meant it was easier to avoid scrutiny of the propaganda delivered in these spaces.

Consequently, the potential use of dark cycles as a tool for disseminating individual propaganda and social engineering en masse, coupled with a back-end data extraction and profiling system, further accentuates the asymmetric power relations that social media and computational tools create between political parties, social media platforms, and citizens (Zuboff, 2015). Following Tufekci (2014), such new relationships between political chatbots and the end-user break publics into individuals based on surveillance and compliance, wrapped in mimicry and deception (Natale, 2021). The chatbot mimics the politician but

is, in fact, an automated software; the buttons mimic interactivity but preclude symmetric conversation; the rhetoric is informal and needy while personal data are extracted.

Our research has two limitations. First, because of the closed nature of Facebook and the chatbot, our access and capacity to fully comprehend their operations are restricted. Consequently, our analysis is confined to the choice architectures available for observation. Second, we could not estimate the number of people who engaged with the chatbot, trace their conversation flows, or measure its influence. Similarly, we lack information about the outcomes when users chose to disengage from the bot after initial interaction.

Gehl and Lawson's analysis of masspersonal social engineering by Cambridge Analytica and the IRA illustrates the difficulty in measuring campaign success. They note:

> None of this means that masspersonal social engineering or other forms of social engineering don't have effects . . . Just because they might not do what was intended, that doesn't mean they do nothing at all and that the effects they do have aren't potentially negative. (Gehl & Lawson, 2022, p. 206)

This highlights that even unintended outcomes can lead to harmful effects, necessitating scrutiny in future research.

Importantly, similar to other political campaigns, isolating campaigns from many other factors influencing people's opinions and behaviors is challenging and probably impossible. Nevertheless, we believe there is value in analyzing the user interface, even if partial and incomplete, to understand better the computational tools political parties develop and use on citizens.

Besides the potential implications of automated influence on citizens' agency, the rise of political peer-to-peer chatbots raises pertinent questions about public scrutiny, oversight, and regulation. As regulators are currently seeking solutions for preventing deception related to influencer marketing in many-to-many channels, the difficulty in detecting deceptive personal automated influencing is a new threat to the democratic process that leaves citizens vulnerable to various types of harm.

References

Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets, 31*(2), 427–445. doi:10.1007/s12525-020-00414-7

Adamopoulou, E., & Moussiades, L. (2020). Chatbots: History, technology, and applications. *Machine Learning with Applications, 2*, 1–18. doi:10.1016/j.mlwa.2020.100006

Ben-David, A. (2020). Counter-archiving Facebook. *European Journal of Communication, 35*(3), 249–264. doi:10.1177/0267323120922069

Ben-David, A. (2023). Little Samaritan brothers: Crowdsourcing voter surveillance. *The Law & Ethics of Human Rights, 17*(2), 127–165. doi:10.1515/lehr-2023-2008

Ben-Porat, C. S., & Lehman-Wilzig, S. (2020). Political discourse through artificial intelligence: Parliamentary practices and public perceptions of chatbot communication in social media. In O. Feldman (Ed.), *The rhetoric of political leadership* (pp. 230–245). Cheltenham, UK: Edward Elgar Publishing. doi:10.4337/9781789904581.00022

Bronstein, J., Aharony, N., & Bar-Ilan, J. (2018). Politicians' use of Facebook during elections: Use of emotionally-based discourse, personalization, social media engagement, and vividness. *Aslib Journal of Information Management, 70*(5), 551–572. doi:10.1108/AJIM-03-2018-0067

Cacioppo, J. T., & Petty, R. E. (1979). Effects of message repetition and position on cognitive response, recall, and persuasion. *Journal of Personality and Social Psychology, 37*(1), 97–109. doi:10.1037/0022-3514.37.1.97

Caldarelli, G., De Nicola, R., Del Vigna, F., Petrocchi, M., & Saracco, F. (2020). The role of bot squads in the political propaganda on Twitter. *Communications Physics, 3*(81), 1–18. doi:10.1038/s42005-020-0340-4

Campbell-Smith, U., & Bradshaw, S. (2019). *Global cyber troops country profile: India*. Oxford Internet Institute. Retrieved from https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/05/India-Profile.pdf

Carmi, E. (2020a). *Media distortions: Understanding the power behind spam, noise, and other deviant media*. New York, NY: Peter Lang.

Carmi, E. (2020b). Rhythmedia: A study of Facebook immune system. *Theory, Culture & Society, 37*(5), 119–138. doi:10.1177/0263276420917466

DiResta, R., Grossman, S., & Siegel, A. (2022). In-house vs. outsourced trolls: How digital mercenaries shape state influence strategies. *Political Communication, 39*(2), 222–253. doi:10.1080/10584609.2021.1994065

Dubois, E., & McKelvey, F. (2019). Political bots: Disrupting Canada's democracy. *Canadian Journal of Communication, 44*(2), 27–33. doi:10.22230/cjc.2019v44n2a3511

Facebook. (2019a). *Identity information*. Retrieved December 20, 2024, from https://web.archive.org/web/20190227075921/https:/developers.facebook.com/docs/messenger-platform/identity

Facebook. (2019b). *Sending messages*. Retrieved from
        https://web.archive.org/web/20190302055246/https:/developers.facebook.com/docs/messenger
        -platform/send-messages/

Facebook Ad Library. (2019). *Benjamin Netanyahu – בנימין נתניהו* [Benjamin Netanyahu]. Retrieved from
        https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=IL&q=%D7%9E
        %D7%96%D7%9E%D7%99%D7%9F&view_all_page_id=268108602075&search_type=page&m
        edia_type=all

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots.
        Communications of the ACM, 59(7), 96–104. doi:10.1145/2818717

Forelle, M., Howard, P., Monroy-Hernández, A., & Savage, S. (2015). *Political bots and the manipulation of
        public opinion in Venezuela*. ArXiv preprint. Retrieved from https://arxiv.org/abs/1507.07109

Gehl, R. W., & Bakardjieva, M. (Eds.). (2016). *Socialbots and their friends: Digital media and the
        automation of sociality*. New York, NY: Routledge.

Gehl, R. W., & Lawson, S. T. (2022). *Social engineering: How crowdmasters, phreaks, hackers, and trolls
        created a new form of manipulative communication*. Cambridge, MA: MIT Press.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX
        design. In *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing
        Systems* (Paper No. 534, pp. 1–14). New York, NY: ACM. doi:10.1145/3173574.3174108

Haaretz Editorial. (2019, September 10). The Likud's little red booklet. *Haaretz*. Retrieved from
        https://www.haaretz.com/opinion/editorial/2019-09-10/ty-article/the-likuds-little-red-
        booklet/0000017f-e4e6-d568-ad7f-f7ef943e0000

Bergmen, R. (2019, March 31). Twitter network uses fake accounts to promote Netanyahu, Israel
        watchdog finds. *The New York Times*. Retrieved from
        https://www.nytimes.com/2019/03/31/world/middleeast/netanyahu-fake-twitter.html

Haleva-Amir, S. (2022). The 2019–20 Israeli electoral digital campaigns: Algorithmic campaigns' slippery
        slope. *Israel Affairs, 28*(6), 940–955. doi:10.1080/13537121.2022.2134397

Hill, C. E., Knox, S., Thompson, B. J., Williams, E. N., Hess, S. A., & Ladany, N. (2005). Consensual
        qualitative research: An update. *Journal of Counseling Psychology, 52*(2), 196–205.
        doi:10.1037/0022-0167.52.2.196

Irani, L. (2015). The cultural work of microwork. *New Media & Society, 17*(5), 720–739.
        doi:10.1177/1461444813511926

Kahneman, D., Slovic, S. P., & Slovic, P. (Eds.). (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge, UK: Cambridge University Press.

Keller, T. R., & Klinger, U. (2019). Social bots in election campaigns: Theoretical, empirical, and methodological implications. *Political Communication, 36*(1), 171–189. doi:10.1080/10584609.2018.152623

Keren, M. (2022). Benjamin Netanyahu and online campaigning in Israel's 2019 and 2020 elections. In R. Davis & D. Taras (Eds.), *Electoral campaigns, media, and the new world of digital politics* (pp. 163–178). Ann Arbor: University of Michigan Press. doi:10.3998/mpub.12013603

Kershner, I. (2019, September 12). Facebook suspends Netanyahu campaign bot over hate speech. *The New York Times*. Retrieved from https://www.nytimes.com/2019/09/12/world/middleeast/facebook-netanyahu-bot.html

Kim, Y., & Lee, H. (2023). The rise of chatbots in political campaigns: The effects of conversational agents on voting intention. *International Journal of Human–Computer Interaction, 39*(20), 3984–3995. doi:10.1080/10447318.2022.2108669

Kowald, C., & Bruns, B. (2020). Chatbot Kim: A digital tutor on AI. How advanced dialog design creates better conversational learning experiences. *International Journal of Advanced Corporate Learning, 13*(3), 26–34. doi:10.3991/ijac.v13i3.17017

Lavi, M. (2018). Evil nudges. *Vanderbilt Journal of Entertainment and Technology Law, 21*(1), 1–94. Retrieved from https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss1/1

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society, 20*(3), 881–900. doi:10.1177/1461444816675438

Mann, C. B. (2021). Can conversing with a computer increase turnout? Mobilization using chatbot communication. *Journal of Experimental Political Science, 8*(1), 51–62. doi:10.1017/XPS.2020.5

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 31–32. doi:10.1145/3359183

Mathur, A., Kshirsagar, M., & Mayer, J. (2021, May). What makes a dark pattern . . . dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–18). New York, NY: ACM. doi:10.1145/3411764.3445610

Milan, S., & van der Velden, L. (2018). Reversing data politics: An introduction to the special issue. *Krisis | Journal for Contemporary Philosophy, 38*(1), 1–3. Retrieved from https://www.proquest.com/scholarly-journals/reversing-data-politics-introduction-special/docview/2291068828/se-2

Mitnick, K., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. New York, NY: Wiley.

Natale, S. (2021). *Deceitful media: Artificial intelligence and social life after the Turing test*. New York, NY: Oxford University Press.

Netanyahu, B. [@netanyahu]. (2019, March 24). *Ma ha-nose she-hachi chashuv lecha ba-bechirot* מה הנושא שהכי חשוב לך בבחירות; [What is the most important issue for you in the elections; Facebook ad]. Facebook. Retrieved from https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=IL&media_type=all&q=%22%D7%9E%D7%94%20%D7%94%D7%A0%D7%95%D7%A9%D7%90%20%D7%A9%D7%94%D7%9B%D7%99%20%D7%97%D7%A9%D7%95%D7%91%20%D7%9C%D7%9A%20%D7%91%D7%91%D7%97%D7%99%D7%A8%D7%95%D7%AA%22&search_type=keyword_exact_phrase

Neyazi, T. A. (2020). Digital propaganda, political bots, and polarized politics in India. *Asian Journal of Communication, 30*(1), 39–57. doi:10.1080/01292986.2019.1699938

Nye, J. S., Jr. (2004). *Soft power*. New York, NY: Public Affairs.

Patel, M. S., Volpp, K. G., & Asch, D. A. (2018). Nudge units to improve the delivery of health care. *The New England Journal of Medicine, 378*(3), 214–216. doi:10.1056/NEJMp1712984

Pybus, J. (2019). Trump, the first Facebook president: Why politicians need our data too. In C. Happer, A. Hoskins, & W. Merrin (Eds.), *Trump's media war* (pp. 227–240). Basingstoke, UK: Palgrave Macmillan.

Rogenhofer, J. M., & Panievsky, A. (2020). Antidemocratic populism in power: Comparing Erdoğan's Turkey with Modi's India and Netanyahu's Israel. *Democratization, 27*(8), 1394–1412. doi:10.1080/13510347.2020.1795135

Santini, R. M., Salles, D., & Tucci, G. (2021). Comparative approaches to mis/disinformation| When machine behavior targets future voters: The use of social bots to test narratives for political campaigns in Brazil. *International Journal of Communication, 15*, 1220–1243. Retrieved from https://ijoc.org/index.php/ijoc/article/view/14803

Schäfer, F., Evert, S., & Heinrich, P. (2017). Japan's 2014 general election: Political bots, right-wing Internet activism, and Prime Minister Shinzō Abe's hidden nationalist agenda. *Big Data, 5*(4), 294–309. doi:10.1089/big.2017.0049

Silva, G. R. S., & Canedo, E. D. (2024). Towards user-centric guidelines for chatbot conversational design. *International Journal of Human–Computer Interaction, 40*(2), 98–120. doi:10.1080/10447318.2022.2118244

Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2017). Detecting bots on Russian political Twitter. *Big Data, 5*(4), 310–324. doi:10.1089/big.2017.0038

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New York, NY: Penguin.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2013). Choice architecture. In E. Shafir (Ed.), *The behavioral foundations of public policy* (pp. 428–439). Princeton, NJ: Princeton University Press.

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the Dark Web: Leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science, 48*, 43–63. doi:10.1007/s11747-019-00704-3

Tufekci, Z. (2014). Engineering the public: Big data, surveillance, and computational politics. *First Monday, 19*(7). doi:10.5210/fm.v19i7.4901

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday, 21*(4). doi:10.5210/fm.v21i4.6161

Woolley, S. C., & Howard, P. N. (2016). Automation, algorithms, and politics: Political communication, computational propaganda, and autonomous agents—Introduction. *International Journal of Communication, 10*, 4882–4890. Retrieved from http://ijoc.org/index.php/ijoc/article/view/6298/1809

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security, 16*(6), 315–331. doi:10.1080/10658980701788165

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674. doi:10.1002/asi.20779

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In J. Abawajy, S. Mukherjea, S. Thampi, & A. Ruiz-Martínez (Eds.), *Security in computing and communications* (Vol. 536, pp. 438–449). Cham, Switzerland: Springer. doi:10.1007/978-3-319-22915-7_40

Yavetz, G. (2022). Bibi and Mr. Prime Minister: Do different Facebook identities imply different messages for political leaders? *Online Information Review, 46*(3), 464–482. doi:10.1108/OIR-01-2021-0004

Yeung, K. (2017). "Hypernudge": Big data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136. doi:10.1080/1369118X.2016.1186713

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. doi:10.1057/jit.2015.5