are extensive and enable us to demystify and characterize the main activities occurring within political groups on WhatsApp.

Another limitation is the set of keywords used to identify political public groups. New public groups emerge daily, and discussions in society evolve due to events and changing situations. Additionally, groups change, and users may lose interest in older groups or leave because they are no longer relevant. Therefore, we continuously search for and join new public groups to keep the data up to date with current trends. We can also add new keywords to the list to monitor recent events or emerging topics. Furthermore, the data collection relies on physical smartphones, and to scale the number of groups, additional smartphones are needed to access and join the groups. Since groups receive many messages per day, having a single smartphone manage all the groups can significantly slow down the process and even cause crashes, which makes collection more difficult.

Despite these limitations, the data collection presented in this work represents a large dataset that observes important recent political events in Brazil. To the best of our knowledge, this is one of the largest recent WhatsApp datasets. While it may not be fully representative, it offers valuable insights and transparency into this closed network.

Chapter 4

The Role of Mobilized Attacks in WhatsApp's Ecosystem

The rise of messaging applications has significantly transformed how people communicate and interact. The immense popularity of WhatsApp, coupled with the nature of the communication it facilitates, has created a highly convoluted and fertile environment for the propagation of misinformation campaigns. The environment created by messaging apps like WhatsApp is inherently complex. While these platforms offer a variety of tools to facilitate the rapid dissemination of messages, they also maintain a level of anonymity that conceals the authors of these messages.

The public space within the WhatsApp platform has emerged as a hub of communication and organization, enabling the seamless coordination of activists. These public groups connected hundreds of very active users dedicated to spreading information to participants and groups, creating a backbone for information propagation within WhatsApp [102]. Misinformation campaigns feed these groups of activists, who are moved by loyalty to the preferred candidate and tend to amplify the reach of the messages received, regardless of their truthfulness. At the same time, given the polarized nature of political discussions, groups of activists organize themselves into digital groups to fight with each other and to promote hostile interactions towards opponents. The public nature of these groups means that both supporters and users with opposing political views can engage in the same group. This public space also allows malicious users to infiltrate, disrupting the dynamics of these groups and enabling attacks. This no man's land created within WhatsApp by digital militias is nearly unexplored by the research community.

This Chapter presents a comprehensive study that analyzes the strategies and attacks employed by activist groups operating in public political WhatsApp groups. By examining the dynamics and tactics used by these groups, this chapter sheds light on the complex landscape of online political engagement and the role played by these activist groups in dismantling and attacking the opposing side's groups. To address this question, we explore the available data (Chapter 3), to investigate the attacks and the dynamics of WhatsApp. Thus, Section 4.1 describe the flooding attack, a commonly employed tactic to disrupt the activity of the opponent group. This attack involves overwhelming the

group with a high volume of messages. Last, Section 4.2 presents the hijacking attack, which involves the unauthorized takeover of a WhatsApp group by a malicious user, who aims to disrupt and dismantle the group. The hijacker gains control over the group, often exploiting vulnerabilities in the group's administration and then taking destructive actions, such as removing all members or spreading harmful content.

4.1 Flooding Attack

Flooding attacks are denial-of-service (DoS) attacks that aim to overwhelm a server and cause network disruption by creating network congestion [165]. Flooding attacks are not only limited to computer networks, it is also a popular type of attack and can also affect other communication channels, like SMS [67] and chat messages on online messaging platforms. On messaging platforms like WhatsApp, attackers can infiltrate a group and send a large volume of messages quickly, disrupting the group's regular operation and making it difficult for benign users to interact and chat in the WhatsApp group. Motivated by this, we aim to identify and characterize these attacks, understanding how they are carried out and analyzing their impact on targeted groups.

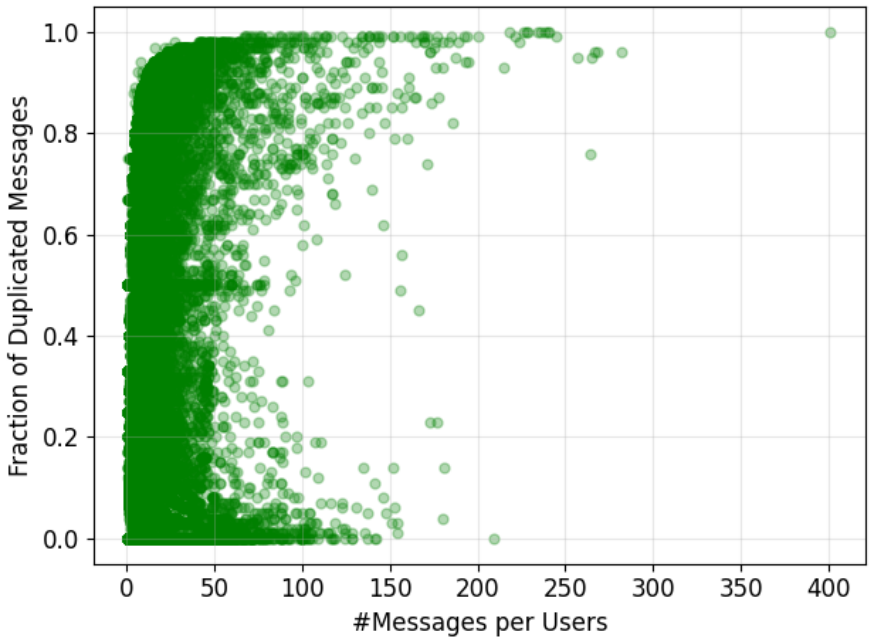
Our analysis of flooding attacks focuses on the period between July 2022 and December 2022, which includes data from 1,267 groups and 12,167,529 messages (see Chapter 3 for details on data collection). We focus on this period for some reasons. First, this is the most active period of our dataset, and second, this period in our data collection included all activity related to sticker messages, which, as we will see later, are important for detecting flooding attacks. Moreover, this period encompasses important political events, such as the Brazilian presidential elections [124] and misinformation campaigns targeting the electoral process and protests urging for military intervention [38].

4.1.1 Identifying Flooding Attacks

The flooding attack on WhatsApp group occurs when an attacker sends a large volume of messages, usually containing identical content, within a short period. To identify flooding attacks on WhatsApp groups, we devise the following methodology. First, we split the group's message-sharing activity into *sessions*, each comprising one minute of the group's activity. Then, for each session, we calculate: 1) the average number of

messages per user; 2) the fraction of duplicated messages (i.e., sharing the same text, image, audio, video, sticker).

Figure 4.1: Aggregate user-activity and fraction of duplicate messages per session.



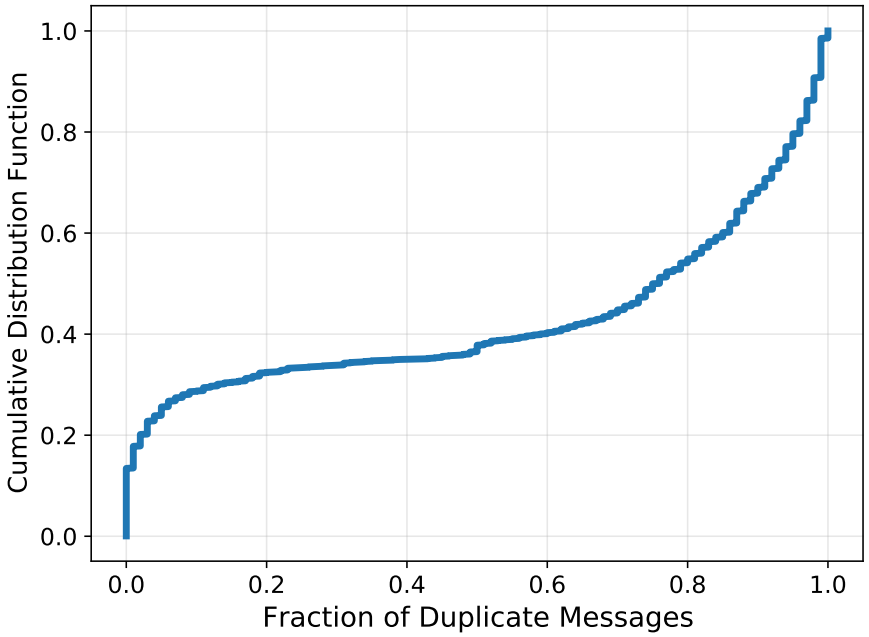
Source: The Author.

Figure 4.1 shows a scatter plot of these two metrics for each 1-minute session; we observe that the majority of the sessions have less than 60 messages per user, which is expected given that in most of the sessions, we expect to have benign conversations where many users share messages with relatively low frequency. Also, we observe that for a low average number of messages per user (less than 60), we have many sessions with a fraction of duplicated messages across the entire range of 0 and 1. On the other hand, when considering sessions with more than 60 messages per user, we observe that the fraction of duplicate messages is concentrated mainly on the limits.

This is evident by looking at Figure 4.2, which shows the Cumulative Distribution Function (CDF) of the fraction of duplicated messages for all sessions with 60 messages per user or more. We observe that 60% of sessions with 60 messages per user have at least 60% of the messages shared within the session as duplicates (i.e., users sharing messages with identical content). Based on this session-based characterization, we assume that a group is under a flooding attack when there is an average number of messages of 60 messages or more and at least 60% of all the session messages are duplicates.

Using the above-mentioned methodology, we identify 893 flooding sessions in 95 WhatsApp groups (7,04% of all active groups from July 2022 to December 2022). Then, we aggregate the flooding sessions into flooding attacks. Since we create 1-minute sessions, flooding attacks may span multiple consecutive flooding sessions. Therefore, we combine

Figure 4.2: Distribution of duplicate messages and user-activity in the 1-minute sessions.



Source: The Author.

all consecutive flooding sessions happening in the same group and treat them as part of the same flooding attack. Overall, we find 580 flooding attacks in 95 WhatsApp groups.

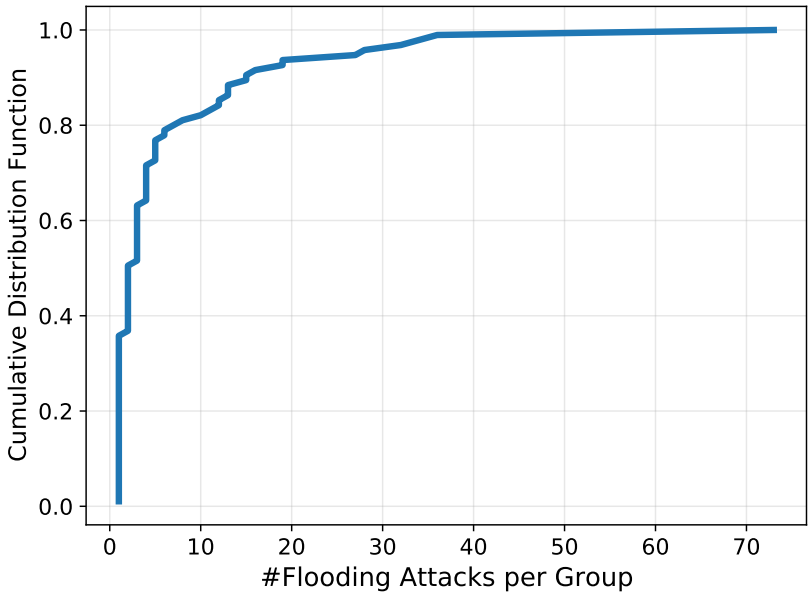
4.1.2 Characterizing Flooding Attacks

Having identified a set of flooding attacks, we aim to characterize these attacks, focusing on understanding how these attacks are executed in WhatsApp groups. We start our characterization by looking into the groups that are the recipients of the flooding attacks. Figure 4.3 shows the CDF of the number of flooding attacks received per group (Figure 4.4(a)), as well as the CDF of the number of flooding attacks per group per day (Figure 4.4(b)). Almost half of the groups experience only one flooding attack throughout our dataset.

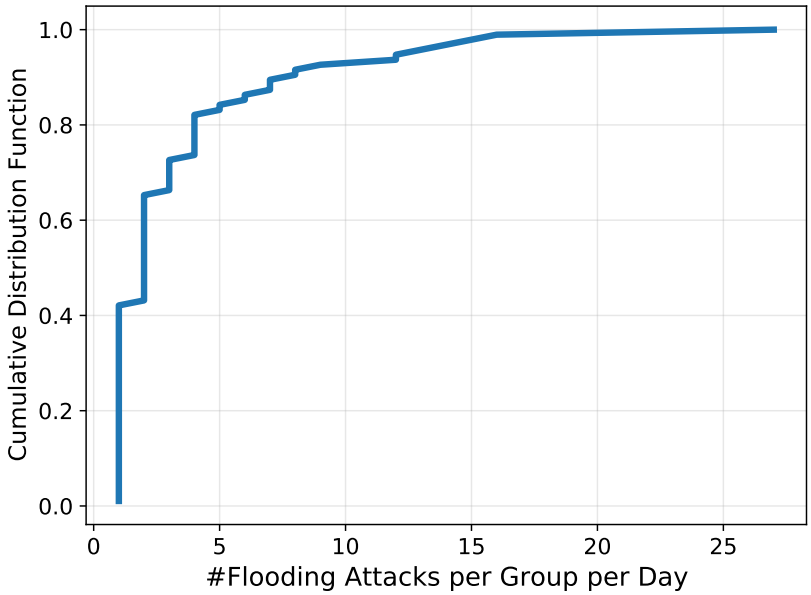
At the same time, we observe that many groups receive flooding attacks; e.g., 20% of the groups receive more than seven flooding attacks throughout our dataset (see Figure 4.4(a)). More worrying is the finding that groups receive multiple flooding attacks within the same day. We find that 57.89% of the groups receive more than one flooding attack within the same day (see Figure 4.4(b)), highlighting the prevalence and gravity of these attacks, especially in political groups.

To better illustrate this phenomenon, we present a case study of a single WhatsApp

Figure 4.3: CDF of the number of flooding attacks per group: a)for the entire period of our dataset; b) per group per day. We focus on the groups that received at least one flooding attack during our dataset.



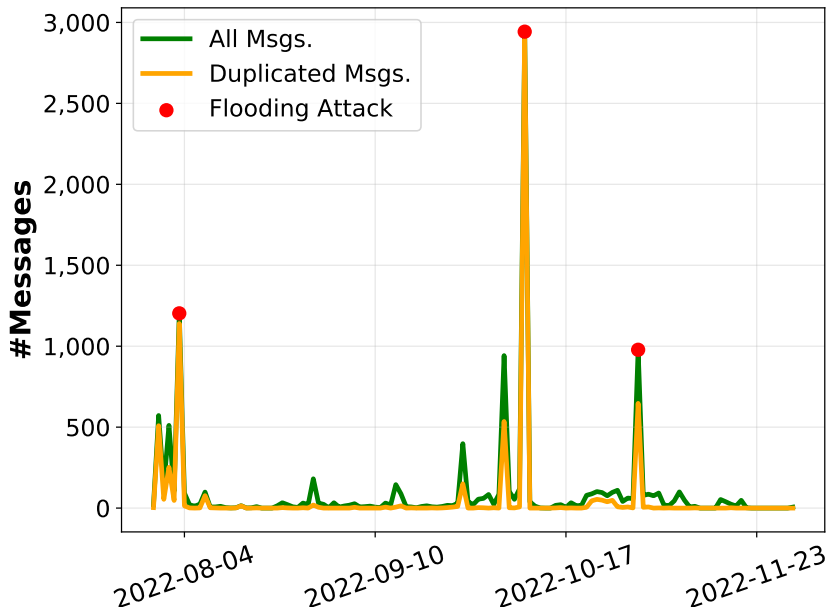
(a) Per group



(b) Per group per day

Source: The Author.

Figure 4.4: Group targeted by multiple flooding attacks.



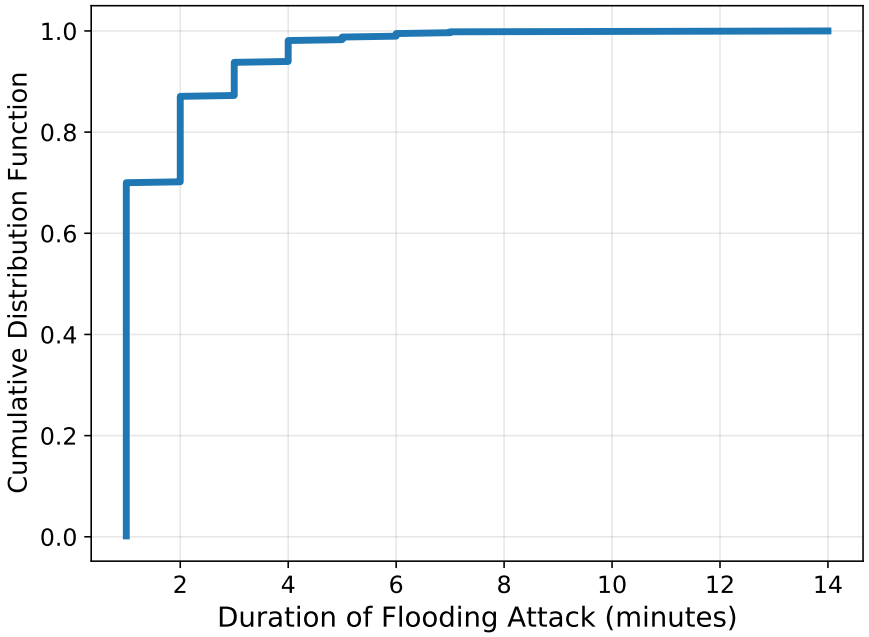
Source: The Author.

group that received multiple flooding attacks throughout our dataset in Figure 4.4. This specific group received in total four flooding attacks, with the first three increasing in intensity, as observed by the increasing number of duplicate messages shared during the attacks. Overall, the finding that WhatsApp groups are the recipients of multiple flooding attacks, and sometimes within the same day, indicates that the group's administrators can not prevent or moderate these attacks effectively. This is likely due to the absence of effective moderation tools that can assist group administrators in tackling attackers that share many duplicate messages within a short period of time [102].

Next, we look into the duration of flooding attacks. Given that flooding attacks may consist of multiple 1-minute flooding sessions, we calculate each attack's duration by summing all the consecutive 1-minute flooding sessions. Figure 4.5 shows the CDF of the duration (in minutes) of the flooding attacks observed in our dataset. We observe that, in general, flooding attacks are short-lived; 70% of the flooding attacks have a duration of up to one minute, and 98.1% of the flooding attacks have a duration of up to four minutes.

Given that flooding attacks are short-lived, we then turn our attention to looking into the type of messages that are disseminated during the flooding attacks. We expect that attackers are sending media or types of messages that can send en-masse in a short period. To shed some light on the modus operandi of the attackers, for each flooding attack, we identify the types of messages that are disseminated during the flooding attack. Figure 4.6 shows the prevalence of the flooding attacks across the various message types. Most attacks are carried out using exclusively stickers (54.13%), text (22.06%), or a

Figure 4.5: CDF of the duration of flooding attacks.



Source: The Author.

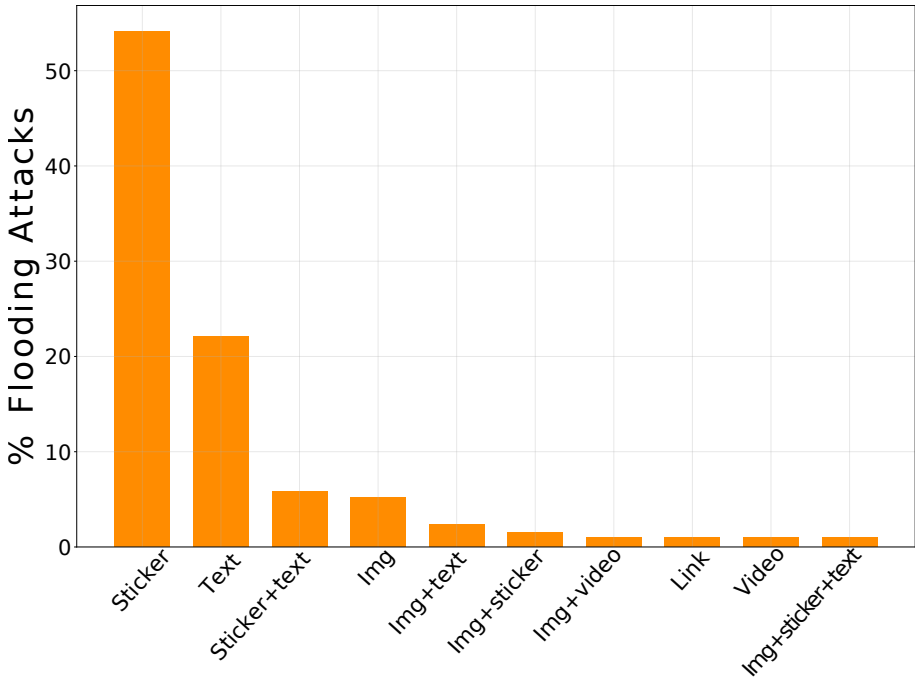
combination of both text and stickers (5.86%). Stickers are small images and can even be animated. They serve multiple purposes, like sharing emojis and memes that can be easily and quickly shared in a group. Given that stickers are also customizable, and group participants can create new stickers, attackers may create some offensive stickers and then disseminate them in the group to undertake a more severe attack.

4.1.3 Characterizing stickers used in Flooding Attacks

Thus far, we have observed that stickers are one of the most popular message types for undertaking flooding attacks. To better understand flooding attacks, here, we characterize the content of the stickers by undertaking a qualitative analysis to better understand the domains. To do this, we extracted a random sample of 100 stickers used during flooding attacks. We constructed a codebook after two researchers went through the stickers, created initial codes, discussed them together, and refined them iteratively until no more changes were made, reaching as result ten codes:

- **Political Agenda**: Promotion of political views or ridicule/criticism of the opposite political side.
- **Meme:** Non-political memes and animated content.
- **Porn:** Explicit sexual content, nudity, and pornography.

Figure 4.6: Percentage of flooding attacks for each different type of message in our dataset.



Source: The Author.

- **Abstract:** Random stickers and miscellaneous topics.
- **Disgusting:** Repulsive and disgusting content, usually involving bodily waste.
- **Religious Attack:** Employing religious symbols and irony to mock or satirize religion.
- **Violence:** Content that promotes violence.
- **LGBTQ+ Attack:** Content attacking LGBTQ+ people.
- **Antisemitism:** Promoting nazism or attacking Jewish.
- **Racism:** Content promoting racist views.

Having constructed the codebook, two researchers independently coded another sample of 100 messages; we find a Cohen's Kappa coefficient of 0.936, indicating high agreement between them, hence the rest of the stickers are coded from a single annotator. Overall, we coded all 1,667 stickers used in flooding attacks. We find that almost 60% have a Political Agenda, which shows that the attacks also aim to provoke the opposite side and sometimes promote their ideologies. Memes (17.87%) are frequently employed to inundate the group. Abstract (8.62%) stickers are readily accessible, with some being standard stickers commonly found on many phones, indicating that users choose random stickers to inundate the group.

More worrying is the fact that we find a substantial percentage of stickers containing harmful content like Porn (12.34%), Violence (1.12%), and Disgusting (2.79%), including repulsive content and offensive imagery. The attacker's goal extends beyond merely targeting the group; it also involves creating discomfort by disseminating offensive and repugnant content. Other instances of hate content include Religious Attacks

(1.18%), LGBTQ+ Attacks (0.87%), Antisemitism (0.81%), and Racism (0.50%). The substantial degree of harmful stickers used in flooding attacks highlights the gravity and potential impact of such attacks on WhatsApp users.

4.1.4 Characterizing text used in Flooding Attacks

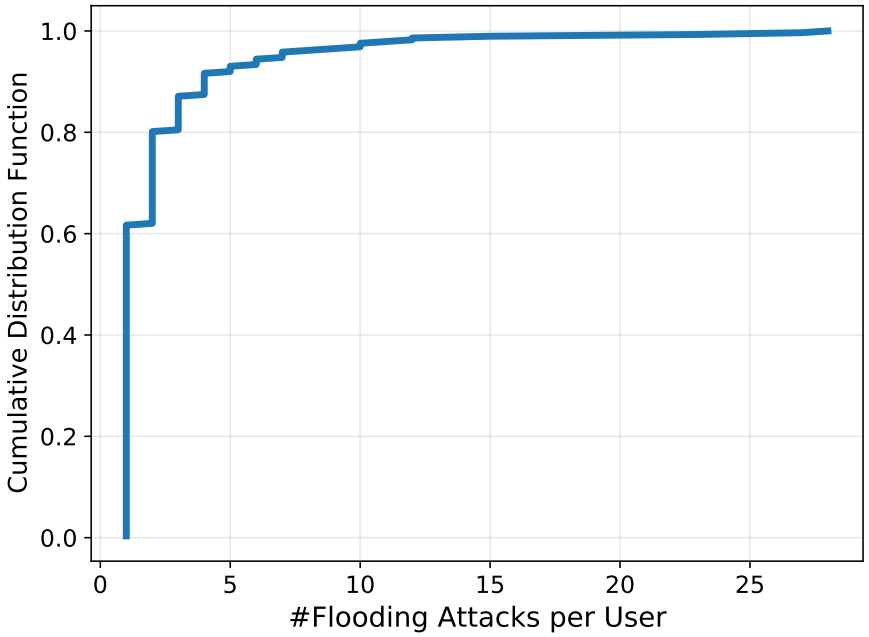
Text messages are also popular for flooding groups; 31.3% of flooding attacks used text messages. Here, we aim to characterize the text content shared during flooding attacks. To do this, we categorize 20% of all flooding text messages. Initially, two human evaluators examined 30% of these messages and established the five codes:

- **Overload Attack Message**: A long message with many characters designed to slow down the phone.
- **Political**: Messages strengthen their own political stance.
- **Meaningless**: Laughter or random characters with no specific meaning.
- **Accusation/Attack**: Messages to provoke or incite political reactions.
- **Word/Phrase**: Words or phrases lacking a particular discernible purpose.

Subsequently, all text messages in the sample were labeled. Within this set of messages, 54.88% were identified as Overload Attack. This shows the malicious intent of the attacker, who not only floods the group but also attempts to slow down users' phones. Furthermore, an additional 25.61% Meaningless messages, characterized by random characters seemingly typed on the keyboard without any discernible meaning. Another 14.64% contained Political and Accusations/Attacks designed to provoke the opposing political group. Finally, 4.88% consisted of random Words/Phrases lacking a specific meaning.

To conclude our characterization of the flooding attacks, we look into the users who participate in flooding attacks (i.e., attackers). To identify attackers, we extract the most active users in each flooding attack and we treat the user as an attacker if the number of messages they shared during the attack period is 20% or more of the entire session activity. Figure 4.7 shows the CDF of the number of flooding attacks per user, as well as how many users are participating in the same flooding attack. We find that 38.3% of the users that participated in flooding attacks participated in more than one attack throughout our dataset (see Figure 4.7). Also, we find that most of the flooding attacks are executed by a single attacker (90%, see Figure 4.8).

Figure 4.7: CDF with flooding attacks per user.



Source: The Author.

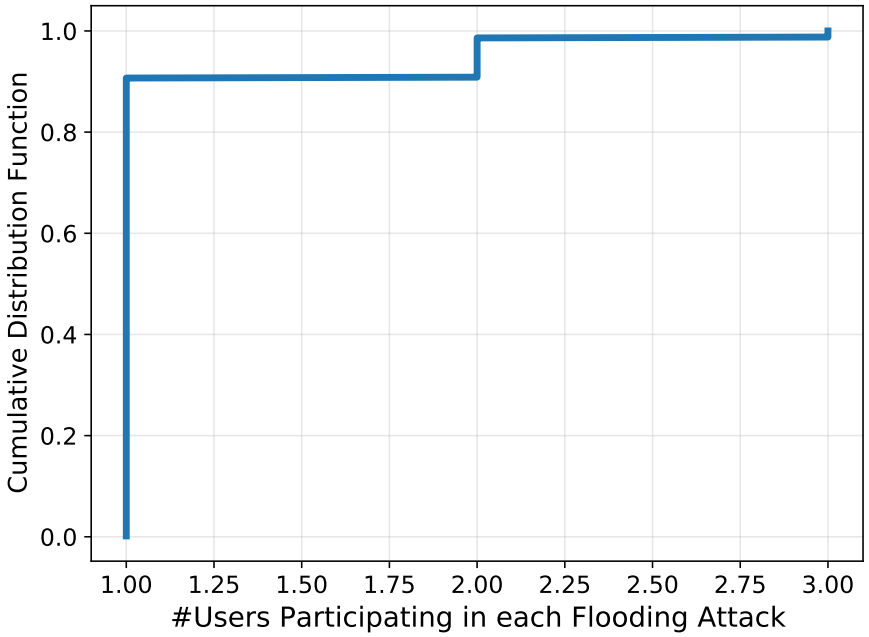
4.1.5 Impact of Flooding Attacks

Having characterized flooding attacks, here, we aim to analyze the impact of these attacks on WhatsApp groups. To achieve this, we compare the activity within the group before and after each flooding attack. Given that we already showed that flooding attacks are short-lived, we focus on 24 hours before and after the attack. Then, we calculate the hourly number of messages and active users and present the results in Figure 4.9 and in Figure 4.10. We focus here on cases where we only have one flooding attack within 48 hours (corresponds to 21.03% of all flooding attacks), as subsequent flooding attacks will affect the WhatsApp group activity.

We observe a substantial increase in both metrics (number of messages and active users) during the flooding attack. This result is expected for the number of messages, given that the attack itself is based on the creation of a large number of messages. On the other hand, the increase in the number of active users is likely due to benign users enquiring about the attack. After the attack, we observe that the group is restored to its regular activity three hours following the flooding attack; on aggregate, we have a similar number of messages and active users before and after the flooding attacks. Overall, these results highlight that flooding attacks can potentially disrupt the groups' activity, however, their impact appears limited to only a few hours.

To conclude our analysis of the impact of the flooding attacks, we perform a small-

Figure 4.8: CDF with users per flooding attacks.



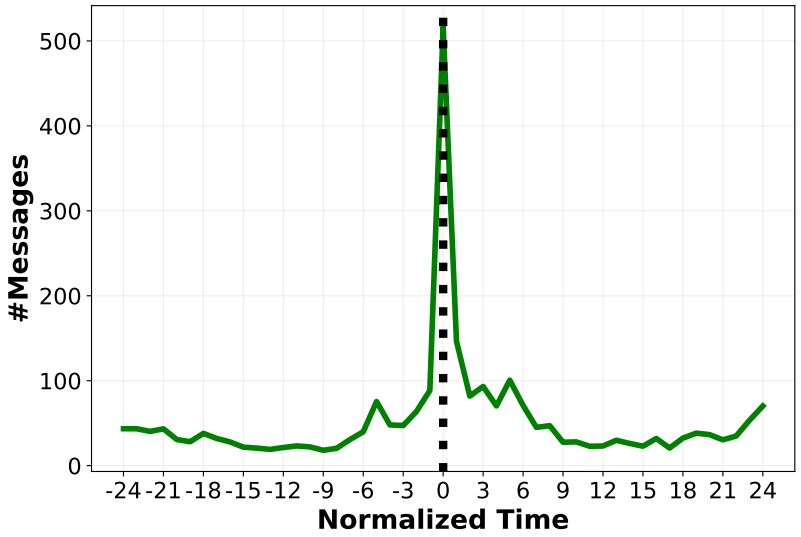
Source: The Author.

scale qualitative analysis of text messages sent by benign users to shed some light on the impact on WhatsApp users. In this direction, we labeled 20% of all text messages sent by benign during the flooding attack, corresponding to 243 messages. Initially, 30% of messages were labeled to find these five codes:

- **Complaining/Cursing**: Users express dissatisfaction or use profanity to describe flooding attacks.
- **Requesting Moderation**: Users request the administrator to take action and eliminate the attacks.
- **News**: Political news or new media forwarded.
- **Interaction**: Users engage with one another.
- **Miscellaneous**: Laughing, meaningless content or message that we could not identify.

Next, all other messages were labeled by two human evaluators, reaching a kappa coefficient agreement of 0.70 [26]. Among all the messages, 31.28% specifically pertain to Complaining/Cursing about the ongoing attack, while 13.17% of messages were out of a lack of Moderation and requested the administrator's intervention to remove the attacker. For instance, some examples we observed during flooding attacks from benign users are: *"Where is the admin?"*, *"Hey admin ban the attacker"*, *"What is it?"*, *"my cell phone is crashing"*(translated messages from Portuguese). Furthermore, 25.93% of the messages involve users interacting with each other or responding, while 16.05% consist of News content shared during the attack. Lastly, 13.58% constitute Miscellaneous, which could not be clearly identified or categorized.

Figure 4.9: Number of messages before and after flooding attacks. We normalize the time and we focus on 24 hours before and after each attack (time 0 corresponds to the flooding attack).

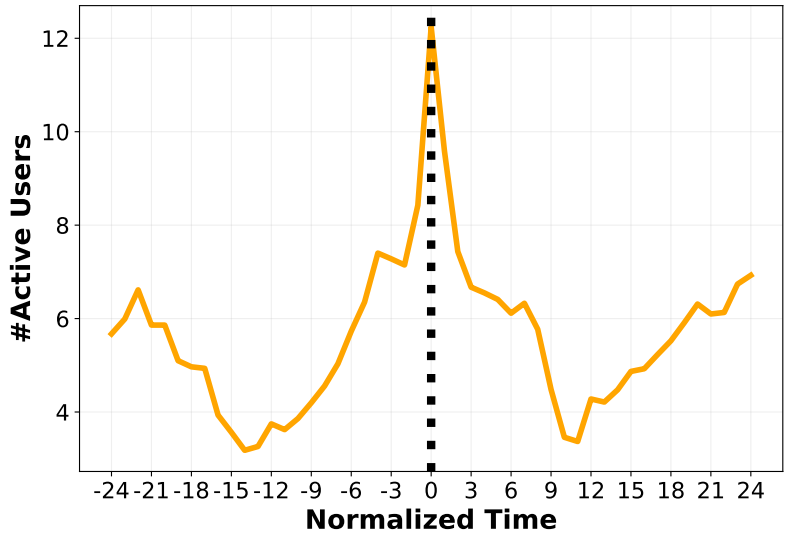


Source: The Author.

4.1.6 Flooding takeaways

- Flooding attacks are not a rare phenomenon on WhatsApp when considering Brazilian groups related to politics. We find that 7.04% of all monitored WhatsApp groups experienced at least one flooding attack throughout our dataset.
- Flooding attacks are short-lived (70% of the flooding attacks have a duration of up to one minute), and they are usually undertaken by a lone wolf (i.e., 90% of all flooding attacks consist of a single attacker).
- We find that WhatsApp groups are the recipients of multiple flooding attacks (even within the same day), which indicates that the moderators or group administrators cannot proactively prevent flooding attacks.
- Many flooding attacks are made using the large dissemination of stickers; 62.57% of all flooding attacks in our dataset use stickers. In addition, based on our manual annotations, we find flooding attacks that use offensive stickers including pornography, violence, and provocative messages.
- By analyzing the impact of flooding attacks, we find that the irregularities in the group activity due to the attacks last for only a few hours (usually three hours), which indicates that both the attack and its impact are short-lived.

Figure 4.10: Number of active users before and after flooding attacks. We normalize the time and we focus on 24 hours before and after each attack (time 0 corresponds to the flooding attack).



Source: The Author.

4.2 Group Hijacking Attack

In the previous section, we investigated flooding attacks on WhatsApp groups and observed that WhatsApp groups tend to return to regular operation/activity after the flooding attacks. Here, we investigate a more severe attack, the Group Hijacking Attack, where an attacker aims to obtain complete control of the group and potentially make drastic or catastrophic changes. The attack is initiated when an attacker obtains administrator rights in the group either via unauthorized means (e.g., by compromising the account of an administrator or the group creator) or by enticing other administrators to promote the attacker to an administrator, or by identifying groups where the creator left the group. Having obtained administrator rights, an attacker can make important changes in the group, such as removing group participants, repurposing the group by changing group metadata, or even archiving/deleting/privatizing the group.

The group hijacking attack is analogous to attacks aiming to compromise accounts on social media platforms [37] to either repurpose it [39], steal personal information, or share misleading information. Here, we focus on understanding and characterizing this phenomenon through the lens of political groups from Brazil on WhatsApp. In political groups, hijacking attacks can be used to disrupt the discussions of supporters from the other party or attack them by sharing provoking content within their group. Overall, there is a pressing need to understand this phenomenon, as it has the potential to increase

online political polarization in the WhatsApp ecosystem. Our analysis of hijacking attacks focuses on the entire collected dataset, including messages collected between March 2020 and December 2022, with 189k active users.

To identify potential group hijacking attacks, we focus on groups that had at least one change in the group's name throughout the period of our dataset. We find that 563 groups (34.28% of all groups) had at least one name change; not all name changes pertain to attacks. To identify potential attacks, we then manually annotate all the 563 groups and their respective name changes to identify whether the name change is suspicious (e.g., the group's name before and after the change substantially differ semantically) by two evaluators with a 0.7 kappa coefficient. We find a total of 33 groups with substantial semantic differences in the two group names, which corresponds to 5.86% of all groups with at least one name change in our dataset.

4.2.1 Characterizing groups with name changes.

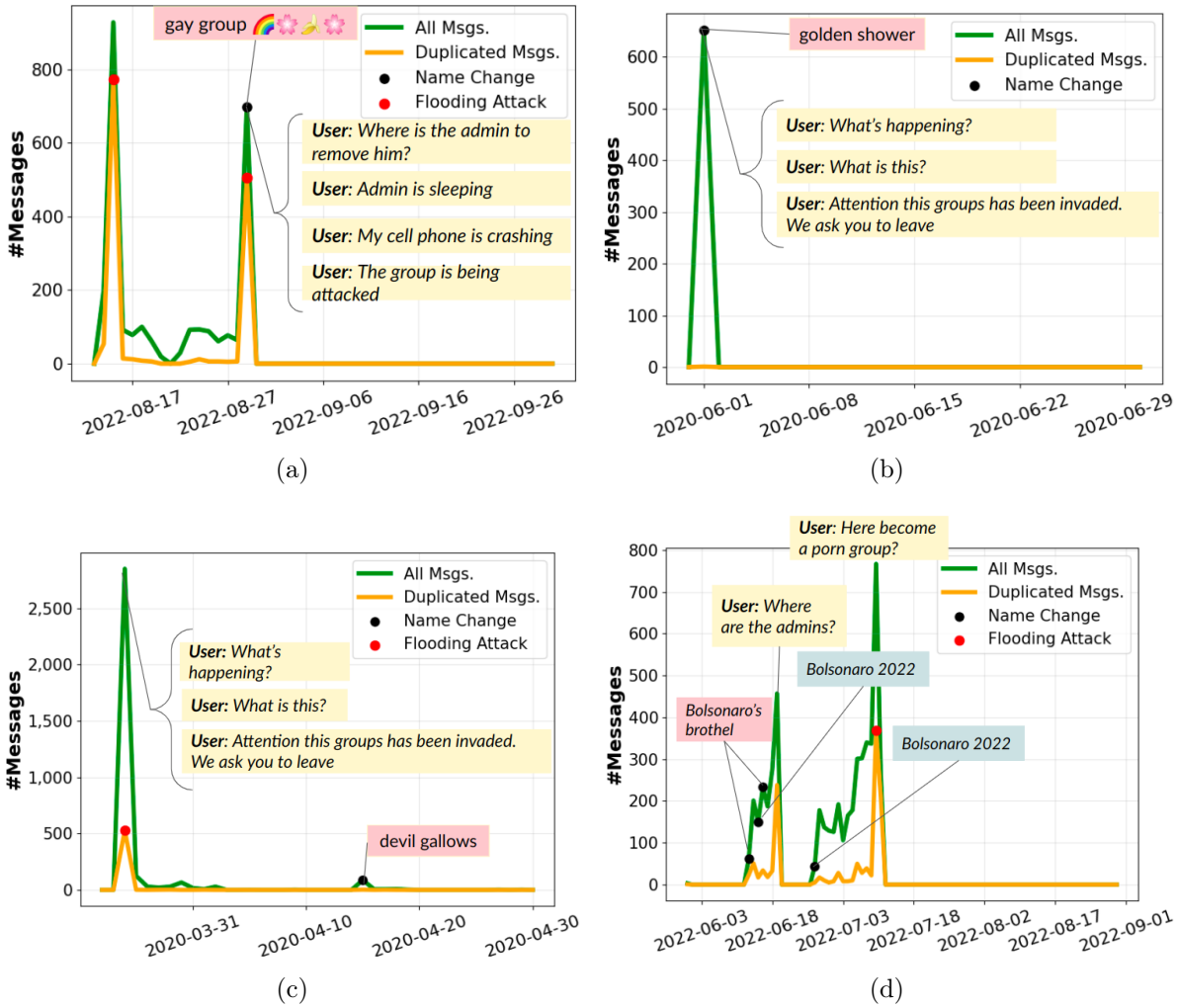
Based on our manual annotations, we categorize these 33 groups into four high-level categories (see Table 4.1).

- **Conflicting:** These are groups that, after the group name change, a contradiction emerges in the political ideology when comparing the period before and after the change in the group's name. We find four cases of groups in our dataset with conflicting political leanings. For instance, a group named "Bolsonaro reigns" was renamed to "Left Reigns," indicating the substantial shift in the group's ideology, likely because of a group hijacking attack.
- **Offensive:** Groups where the group's name became more offensive or toxic after the name change. We find in total five such cases of groups in our dataset. For instance, we find a group that was changed from "Bolsonaro 2022" to "Gay Group" and a group changed from "Patriots and the Captain" to "bordel bozo" (Bolsonaro's brothel).
- **Explicit:** These are groups where the name change indicates that there was an attack on the group. We find four such cases; some examples include a group initially named "Alliance for Brazil" and then "Hacked" and a group renamed "Archived by apocalipse."
- **Context Switch:** Refers to groups where the name change indicates a substantial shift in the group's context and topic of discussion. We found 15 groups with context switching. For instance, a group called "We with Bolsonaro" was renamed to "Grandma's recipe," a topic that has nothing to do with political discussions.

Categories	Original Name	Changed Name
Conflicting	*Bolsonaro's slogan*	*Lula 2022*
	Evangelic & Lula	*100% Bolsonaro*
	Brazil Patriot	*Antifa Action*
	Bolsonaro the myth	*Arthur King*
	Bolsonaro Reigns	*Left Reigns*
	Bolsonaro's Slogan	*Brazil is Lula*
	Lula vs Bolsonaro the Myth	*Lula big vs Bolsonaro*
	*Haddah is a sh***	*Antifascist*
Offensive	*Bolsonaro 2022*	*Gay Group*
	Alliance for Brazil	*Golden Shower*
	Captain gallows	*Devil Gallows*
	Just patriots	*Bozo the shit*
	22	*Prostitution Group*
	Bolsonaro 2022	*Bolsonaro's Brothel*
Explicit	*Entourage PT*	*157 by: lagxzada*
	Alliance for Brazil	*Hacked*
	Anything goes!	*Archived by Apocalypse*
	Itu antifascism	**bot.py**
Context Switch	*We with Bolsonaro*	*Grandma's recipe*
	Antifascist Alliance	*Banana Cake*
	Beloved Brazil	*Birthday Uncle Dudu*
	Strategic Right	*Cake Recipes*
	Brazil-CE	*Yoga Group*
	Bolsonaro President	*Play the Siri*
	Brazilian patriots generation	*New/used online business*
	Bolsonaro's power 20 years	*Zumbussiness your future*
	Civil Resistance!	*Coconut Water*
	Anti Communists	*Groups of Friends*
	Bolsonaro News	*Max iptv and netflix*
	Politics Revealed Youtube	*Free Consultancy*
	300% Bolsonaro patriots	*Happy Family*
	United Right	*Grandma's Recipe*

Table 4.1: Groups with suspicious name changes (translated names from Portuguese).

Figure 4.11: Examples of hijacking attacks (offensive name changes). Figures (a), (b), (c), and (d) show examples of offensive name changes.



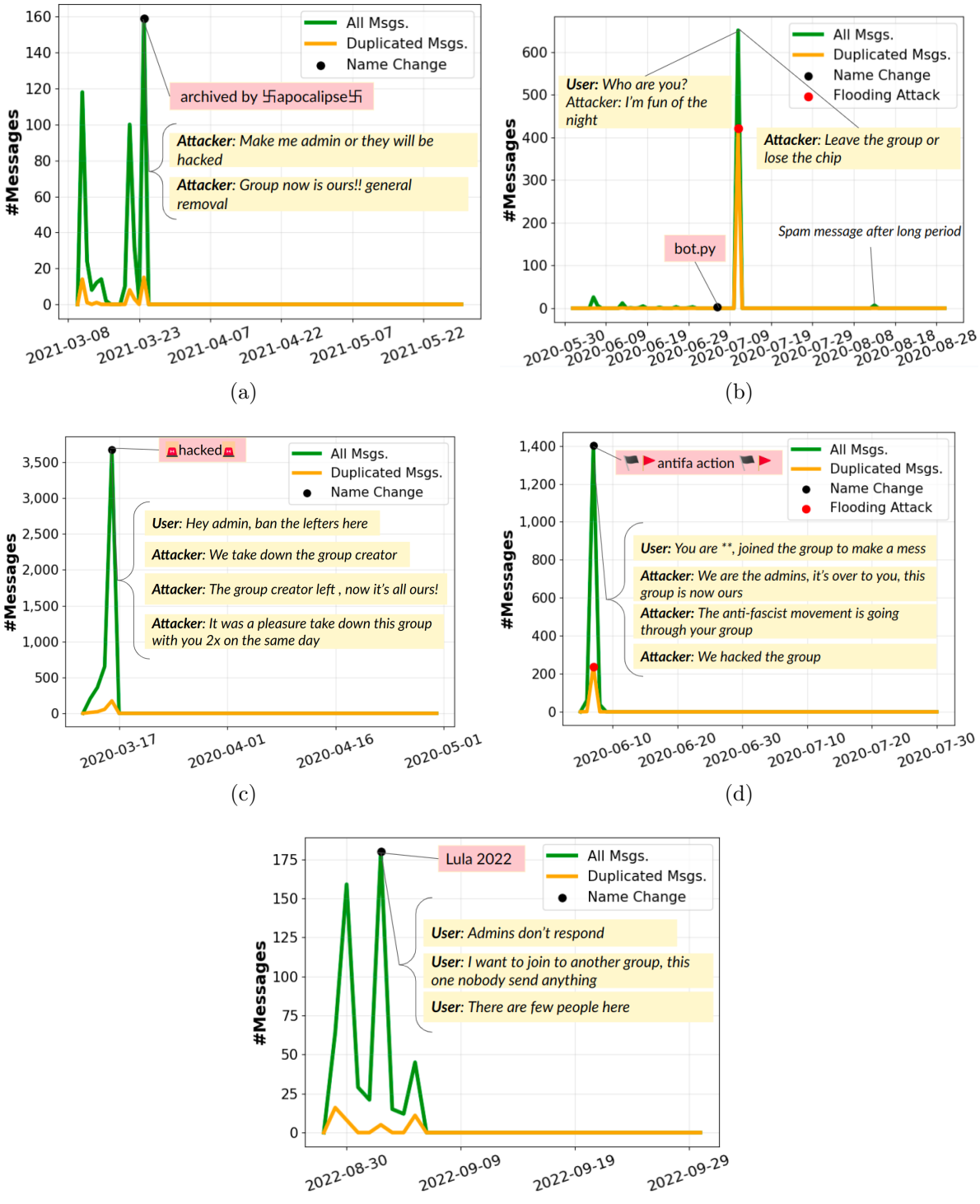
Source: The Author.

4.2.2 Identifying and annotating Hijacking Attacks.

Just because some WhatsApp groups have suspicious changes in their metadata does not necessarily mean they are the victims of hijacking attacks. Therefore, to detect hijacking attacks, it is paramount to analyze and understand what happened in the WhatsApp groups after the name changes and what messages were shared (if any) after the name change. To do this, we performed a manual annotation on the 33 WhatsApp groups that had suspicious name changes based on our previous annotations. In particular, for each group, we plot and evaluate the message activity (i.e., number of messages shared per day, before and after the name change) and manually read messages before and after the name change.

Our analysis yields several interesting observations. First, we find that 15 out

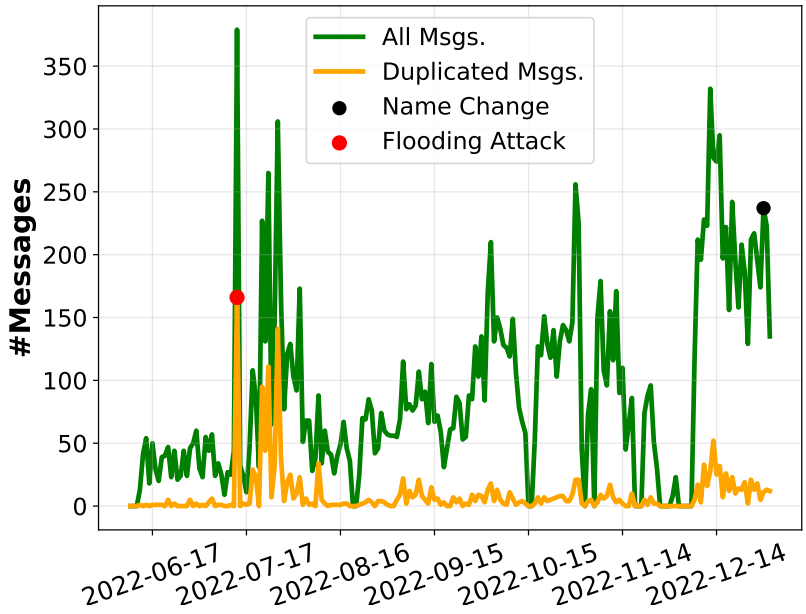
Figure 4.12: Figures (a), (b), and (c) show examples of explicit name changes, and (d) and (e) show examples of conflicting name changes.



(a) (b) (c) (d) (e)

Source: The Author.

Figure 4.13: Switch Context Example.



Source: The Author.

of the 33 groups that had suspicious name changes pertain to a group hijacking attack. For 15 of the groups, we observe that after the hijacking attack, the activity (in terms of messages shared) of the group becomes zero and we find messages that indicate that indeed an attack occurred. For instance, Fig. 4.13(c) shows an example of a group that received a hijacking attack, and shortly thereafter the group is destroyed and has no further activity.

In addition, the attacker provokes the participants who complain and say that the group was overthrown, in addition to celebrating the success of the action (see yellow box in Fig. 4.13(c)). The rest of the groups (all part of the Context Switch category), we observe that are not the victims of group hijacking attacks, but rather, the group had a name change in an attempt to obfuscate the political nature of the group. Below, we present some examples of hijacking attacks and examples of context switching.

4.2.3 Characterizing Hijacking Attacks.

Figure 4.11 and Figure 4.12 shows 9 out of the 15 groups that were the recipients of hijacking attacks (others omitted due to space). For these suspicious names, we have read all messages on the days before and after the group name change. The messages sent on the attack day help us understand what happens in the group. Looking at Fig-

ure 4.12(c), 4.13(c), 4.13(a) and 4.13(d), we realize that the attacker sometimes interacts with the participants, threatening them *"make me admin or they will be hacked"*, sending messages that the group was taken down *"it's over for you, this group is now ours"*, or even celebrating successful group destruction, *"It was a pleasure to take down this group with you 2x on the same day"*. In other cases, the attacker does not interact, but messages from participants indicate that an attack is taking place. Figure 4.12(a) shows an example where some users ask the admin's support to moderate and remove the attacker because the group is under attack. In Figure 4.12(b), the last message was sent by a user informing the group was attacked and the participants needed to leave.

Upon careful observation, we have identified a pattern in hijack attacks: most groups had an attack shortly after we joined the group, typically within a maximum of 10-20 days from its initial creation, 11 of 15 hijacking groups. Moreover, 9 out of the 15 hijacked groups ceased their activities within a maximum of 5 days. In Figure 4.13(c), we see an example of a group that suffered an attack on the same day of its creation, and the group was destroyed. This pattern suggests that attackers are specifically targeting recently formed groups. The public group is shared on social networks, and many users join, even malicious users, who take advantage of the recently created group to ask for help with group moderation and gain admin privileges. Each group contains at least one admin responsible for moderating the group, but others can also be added to help organize the group. The attacker can gain the confidence of the moderator by assuming the role of an admin within the group, once a malicious user obtains admin privileges, the group becomes vulnerable to destruction. In some cases, the group has vulnerabilities and, by default, allows users to join with administrator privileges.

Moreover, the attacker can intimidate group members and foster a hostile environment. In Figure 4.12(c), we can observe how the attackers orchestrate a flooding attack toward the admin's private chat. This can coerce the admin into either leaving the group or adding the attackers as additional admins. In Figure 4.13(c), the attackers also flooded the group and sent a message stating that the group's original creator had been removed and that the group now belonged to the attackers. In two other groups, the attacks did not occur immediately after their creation, but within days of joining the groups. This suggests a scenario where the group admin re-shared the invite link to attract new users, and attackers discovered a new group to infiltrate.

Out of the 15 groups that were targeted in the attacks, one group managed to avoid complete destruction because the admin promptly took action by renaming the group and removing the attacker's presence. This case shows that quick administrator action can help mitigate the damage caused by an attack. In practice, we realized that the attacked groups did not have an active and engaged administrator, which facilitates the action of the attackers. In Figure 4.12(d) and 4.13(e), we show how users are complaining about admin action: *"where are the admins?"*. In Figure 4.12(a), the user goes so far as to say

that the administrator is sleeping.

Finally, among the hijacked groups, we found that 4 also had a flooding attack on the day the group was renamed. This suggests a strategy employed by the attackers: hijacking and flooding attacks are used to gain control and disrupt the group. By flooding the group, the attackers create chaos and confusion, facilitating their hijacking actions. Flooding attacks are not just random messages; sometimes they are selected to evoke fear or intimidation among the group's users. In Figure 4.12(d), the attackers flood the group with pornographic messages and stickers.

4.2.4 Characterizing context switching.

Looking for cases that had significant name changes but were not identified as an attack, we find context-switching groups. We noticed that 11 out of 15 cases occurred on specific days, coinciding with either the second round of the Brazilian presidential election or the final days of 2022 when Bolsonaro exited the Brazilian government. During that period, the Superior Electoral Court (TSE) issued numerous court orders to shut down several WhatsApp and Telegram groups used to coordinate protests alleging election fraud [100], which resulted in the invasion of the Brazilian Congress, Supreme Court, and presidential offices [111].

These groups argue that there may be prosecution and therefore they need to camouflage to avoid censorship by the next government. Upon examining the activity within these groups, it becomes evident that despite the name change, they sustained a consistent level of message exchange and active user participation (see Figure 4.13). The change in group names serves as camouflage, offering participants a sense of confidence and security to express their thoughts and opinions freely. By adopting new names, these groups seek to preserve a level of anonymity and protect themselves from potential sanctions [100].

4.2.5 Hijacking takeaways

- The hijacking attack targets recently formed groups, 11 out of the 15 hijacked groups being compromised shortly after we joined the group, either within a few days or 10-20 days of the group's creation.

- The hijacking attack goes further than flooding attacks, taking control of the group and disrupting the overall interaction. In 9 of 15 hijacking attacks, the group activity stops within a maximum of 5 days.
- 11 of 15 of the groups classified as context switch did this on presidential election day or the last day of Bolsonaro's presidency. These groups are from Bolsonaro supporters, and by adopting new names, aim to maintain a certain level of anonymity and shield themselves from possible sanctions [100].
- Among the hijacked groups, 4 also had a flooding attack on the same day as the group renaming, indicating a connected strategy to disrupt and gain control over groups.

4.3 Summary

In this Chapter, we explored two kinds of attacks that can disrupt the activity of WhatsApp groups, particularly flooding attacks that aim to disseminate many messages within a short period and hijacking attacks that aim to take control of the group and drastically change its purpose. We collected a large-scale dataset of 1.6K WhatsApp groups related to Brazilian politics between March 2020 and December 2022, including 19 million messages. Then, we propose a methodology to identify and characterize flooding attacks and investigate hijacking attacks by focusing on WhatsApp groups.

The analysis shows that flooding attacks are not rare when considering political groups in Brazil. It is likely a way for people from one party to attack people from another party, aiming to disrupt their conversations. We find that flooding attacks are usually short-lived, and most flooding attacks are made by one attacker. Also, we find that WhatsApp groups are the recipients of multiple flooding attacks, even within the same day, which likely highlights the lack of effective tools that assist the group moderators and administrators who aim to maintain the group's harmony. Regarding hijacking attacks, we find many such attacks in our dataset, and we find that in most cases, the attacker's goal is to close or remove the group. Finally, we find that WhatsApp groups can be the recipients of both flooding and hijacking; the attackers first flood the group and then hijack the group entirely.

Overall, the study is a significant leap towards demystifying the dark side of WhatsApp groups, particularly hostile intergroup interactions across the political spectrum. This study highlights the prevalence and gravity of these attacks, identifying that they are not rare in Brazilian political WhatsApp groups. Additionally, our qualitative analysis highlights that a significant portion of these attacks contains harmful content, such

as hateful or offensive stickers, as well as overly long messages to disrupt WhatsApp's regular operation on users' phones. Taken together, these findings show that these attacks are an important problem, and our work has the potential to raise awareness about these attacks among both WhatsApp users and operators of messaging platforms. For WhatsApp users, raising awareness of these attacks is important as it allows them to be more prepared when the attack is underway and try to protect themselves. For messaging platforms, our work and findings can be used to raise awareness about how these attacks are performed on their platforms, which is vital for designing effective moderation tools.

Chapter 5

Understanding the Use and Abuse of Stickers

In the Chapter 4, we unveiled how malicious users exploit stickers as an attack form in public WhatsApp groups, particularly during flooding attacks. Stickers have emerged not only as a popular media type for interaction but also as a potent tool in the dissemination of harmful, offensive, and politically provocative content. Our findings revealed that more than half of the flooding attacks in our dataset employed stickers, many of which conveyed political propaganda, hate speech, or explicit imagery intended to provoke, harass, or destabilize target groups.

Building on these findings, this chapter presents a deeper and systematic characterization of sticker usage on WhatsApp. Rather than focusing solely on attack dynamics, we now turn to a broader analysis that examines stickers as a distinct form of media, exploring their structural, visual, and behavioral patterns. Our goal is to understand how stickers differ from other media formats, how they are created, shared, and collected, and how their content and visual features reflect broader sociopolitical dynamics within the messaging platform.

WhatsApp introduced stickers on the platform referring to them as something to "*help you share your feelings in a way that you cannot always express with words*".[1] The platform enables users to create custom stickers on any subject or occasion, allowing them to be quickly integrated into various contexts. This flexibility has made stickers particularly prominent in political discussions, which is a widely popular topic on WhatsApp [126]. This becomes even more relevant considering that WhatsApp has frequently been associated with the rapid spread of misinformation [11] and has played a central role in political disinformation campaigns [16, 103].

In Brazil, the popularity of stickers has increased considerably. Brazilians hold the record for the highest number of stickers sent [21], transcending their role as a mere form of humor to become a key element of political strategy. The 2022 Brazilian presidential election marked the first major political event in which stickers were massively deployed, with political actors using them to disseminate campaign messages from a visual and

[1] https://blog.whatsapp.com/introducing-stickers

emotional perspective [28]. Their influence has grown so significantly that the Brazilian Electoral Court has released an official sticker pack to aid in fact-checking news [143]. In this direction, stickers have even been weaponized in political activism campaigns, with supporters of one political party using flooding and hijack attacks to spam and undermine their opponents within WhatsApp groups during elections, as shown in Chapter 4. This open and permissive environment, in which users are free to create and share custom stickers, has also led to serious abuses. Some users have produced offensive and hateful stickers that threaten group members, including child sexual abuse material [43] and Nazi propaganda [136], creating an unsafe environment for users. As stickers have become increasingly popular among users, we have observed a rise in their misuse on WhatsApp, ranging from misinformation campaigns to hateful harassment content. However, we still lack a comprehensive analysis of their usage on a broader scale within the messaging platform ecosystem, due to the closed, private, and encrypted architecture of instant messaging platforms.

To address this gap, this chapter aims to provide a comprehensive perspective on the dual nature of stickers: both as tools for enriching digital expression and as vectors of abuse in politically charged environments. Through this analysis, we seek to answer the following questions: How are stickers shared in public WhatsApp groups? How is political content visually encoded in these artifacts? And how do users exploit stickers to propagate offensive or harmful content?. To this end, we focus on messages shared during the 2022 Brazilian presidential election period, identifying over 650,000 sticker messages encompassing 57,031 unique stickers.

We begin by analyzing sticker usage patterns and volume across our dataset, identifying peaks in activity during major political events such as the 2022 presidential election (Section 5.1). We then present a visual content analysis by clustering stickers based on perceptual similarity and dominant color, uncovering visual trends associated with political campaigns and expressive conventions (Section 5.2). Next, we investigate the political attacks made with Stickers (Section 5.3). Finally, we explore how these stickers encode ideological messages and are strategically propagating offensive or harmful content (Section 5.4).

5.1 Stickers as a Distinctive Form of Media

Multimedia messages are very popular on WhatsApp [66]. While text messages remain the majority, users often share different kinds of media using images, videos, audio, and stickers. Although images and stickers are both visual media, some key changes

distinguish them. Stickers may display animated images in chats. They are smaller than actual images and are stored in a different format by the app. Unlike regular images, stickers are usually displayed directly within the text, similar to emojis.

Stickers are usually described as emoticons in the form of colored images [24], as both can be used as visual reaction messages or determine the feeling of the interlocutor during the conversation, but differ from in-line emojis in diversity, complexity, and usage [86], providing a richer communication [154]. Also, they differ from simple static images as they can be short animated movies. Stickers are also closely related to memes [155], which often present a combination of a picture and a statement, typically with sarcastic or humorous intention [32]. Usually, there is a template-based image that people modify, edit, and publish their version while keeping some key aspects so that the meme template is still recognizable.

Both memes and stickers can be created based on personal experiences, but inspiration can be obtained from popular cultural products such as television shows and video games [55]. Additionally, users publish memes on the Web to create an incentive for others to share by replicating the original [87]. The origin of these stickers dates back to 2011, when LINE, a popular messaging app in Japan, mixed cartoons and "emojis" [130]. This tool allowed users to express socio-cultural differences in a more specific way, inspiring other applications to adopt stickers as well. In 2013, Facebook added stickers to its platform, but still with a limited set of pre-created images. This media was adopted by WhatsApp only in 2018.

Although they share similarities, stickers also diverge from GIFs in many ways. WhatsApp distinguishes between reaction GIFs and stickers by incorporating both separately in its interface, highlighting important differences in their nature and use. Reaction GIFs, a popular form of internet communication [9], are integrated into WhatsApp via Tenor,[2] an online GIF library owned by Google. When a user searches for a GIF in WhatsApp, they are searching in this database. The selected GIF from the cloud is then embedded in the message and sent. Stickers, on the other hand, are not hosted externally. Instead, they are static or animated WebP image files stored in the user's private sticker collection on WhatsApp and also in their devices. As a result, users can prohibit the download of any kind of media file except for stickers [81]. Users can create their own stickers using WhatsApp's built-in tool or third-party apps, or they can save stickers received in chats to their collections. Because of that, stickers on WhatsApp offer a much greater degree of flexibility, as they can be modified (gaining new details, texts, clippings), saved, and used in different ways, promoting a more personalized and creative expression in chats. That sticker will always be available to the user in their collection unless they choose to delete it.

Finally, while other image media formats have a typical rectangle format, stickers

[2] https://tenor.com/pt-BR/

appear in much more diverse forms, with their edges often shaping the outline of the image they represent and without the need to click to enlarge the content. Unlike images, which users can choose not to show on chat directly, stickers are automatically downloaded and displayed to users in WhatsApp chats [81], making them even more susceptible to abuse by malicious actors. These characteristics make stickers a powerful visual media format, easy to use, and more invasive than others, which may explain why they are being used for attacks within WhatsApp, as reported in Chapter 4.

5.1.1 Stickers Usage Patterns

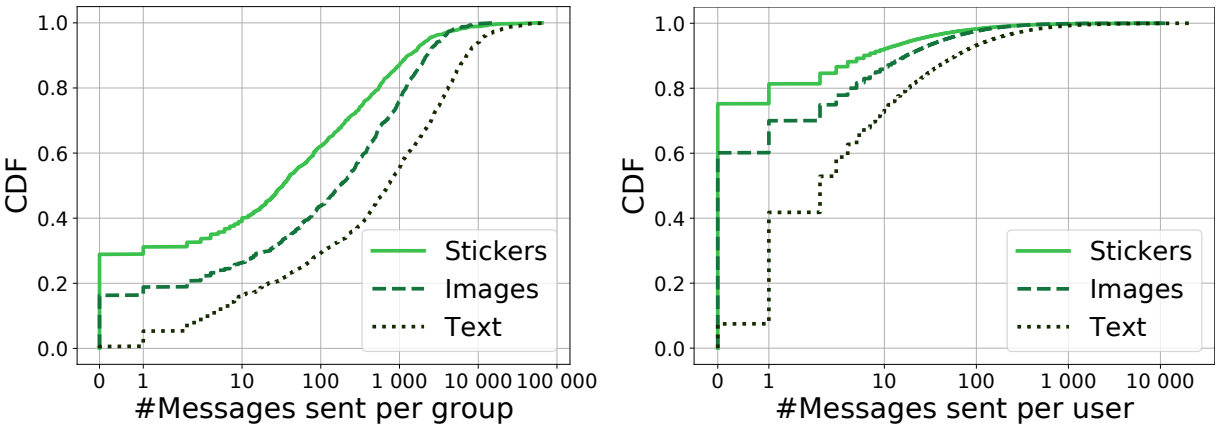
These characteristics, however, refer to the structure and format of the sticker media and not to their usage. We do not know whether the thought process employed by users when sending a sticker is similar to or not from other kinds of media. In this section, we evaluate some aspects of the stickers to investigate how members of the groups use this media.

In Figure 5.1, we compare stickers with images and texts regarding the volume of media sent per group and user. In the cumulative distribution function (CDF) of the messages per group (Fig. 5.2(a)), we observe that sticker messages were less popular in the groups than images. About 30% of the groups did not send any stickers in the chat, images were absent in less than 20% of them, and all groups had text messages. Moreover, 60% of groups sent no more than 100 stickers in total. On the other hand, we note that some groups have more than 10,000 stickers. The less frequent use of stickers may be explained by the political nature of the groups monitored in this study, since some groups expect a more formal communication for the debate while stickers are often associated with a more casual or funny context. In contrast, not all political groups are made only of serious discussions, which can reflect a higher number of stickers.

In the distribution of messages per user (Fig. 5.2(b)), we have similar curves, with stickers being the least common media. Here, even more, users do not send any stickers (75%), but we also have users who individually sent around 10,000 stickers. Hence, we can observe that, as expected, in a messaging app, text format is much more commonly used than other types of media. However, it is interesting to note that users prefer to send images than stickers on the groups, even though both media are widely spread on WhatsApp, especially when considering that stickers are generally easier to send, as they do not need to select a file from the gallery and are more incorporated into the WhatsApp interface.

As we processed and merged stickers, we measured the number of shares each

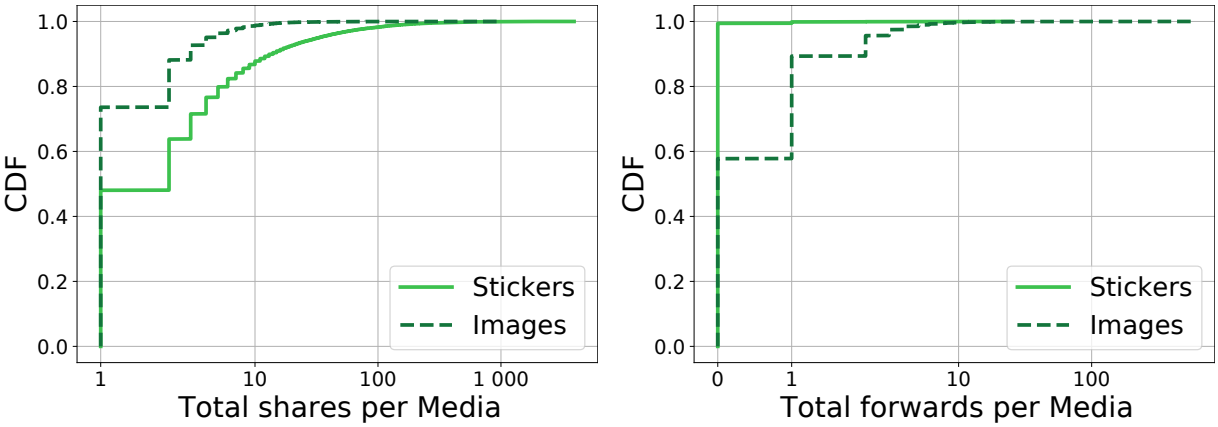
Figure 5.1: Cumulative Distribution Function (CDF) of stickers sent per group and user, compared with image and text.



(a) Groups (b) Users

Source: The Author.

Figure 5.2: Cumulative Distribution Function (CDF) of total shares and forwarding per sticker and image media.



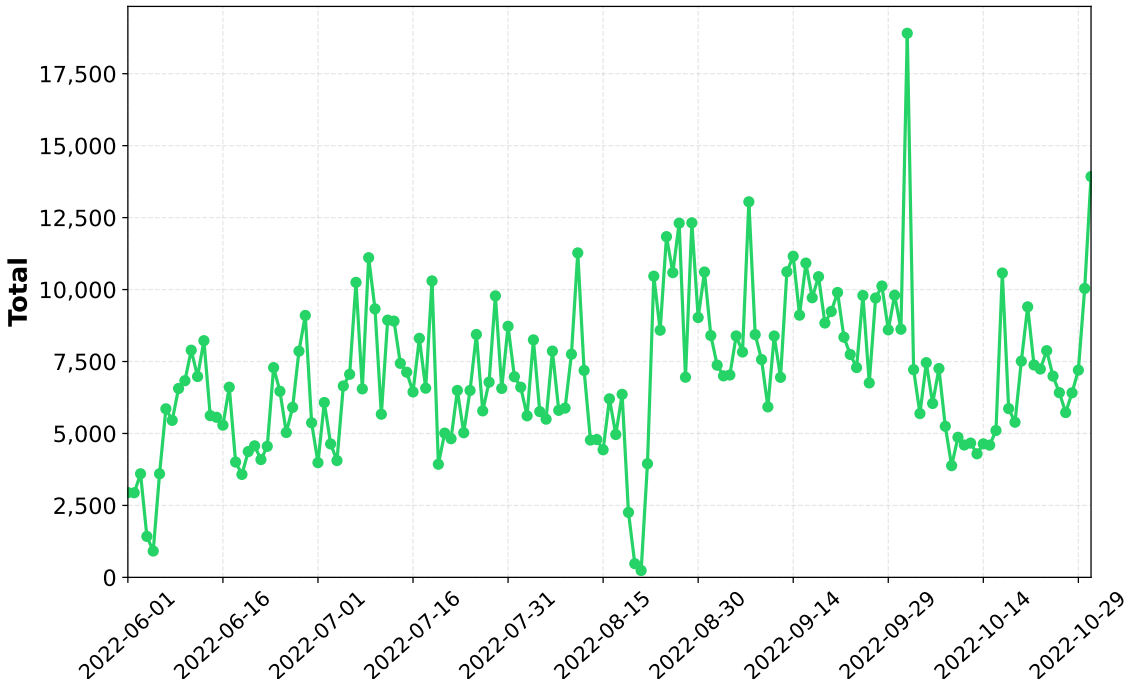
(a) Shares (b) Forwards

Source: The Author.

sticker has within our dataset. In Figure 5.3(a), we evaluate the distribution of total shares per media by comparing images and stickers. Even though we observed more unique image messages in the data, when looking at the total shares per unique media, we note that stickers, in general, have more individual shares than images. About half of the stickers appeared more than once, many of which were shared more than a thousand times. In contrast, about 75% of images have only a single appearance.

Another attribute we obtained for each message is whether it was forwarded or not. Forwarding is an essential tool in the WhatsApp ecosystem, in which users quickly share content with their contacts [102]. A recent study shows that about a quarter of all messages in WhatsApp groups are forwarded [103]. By analyzing forwarded content on our dataset, we found that images are much more frequently forwarded than stickers. Almost none of the collected stickers were found in the forwarded messages, meaning that

Figure 5.3: Stickers sent per day in the WhatsApp dataset.



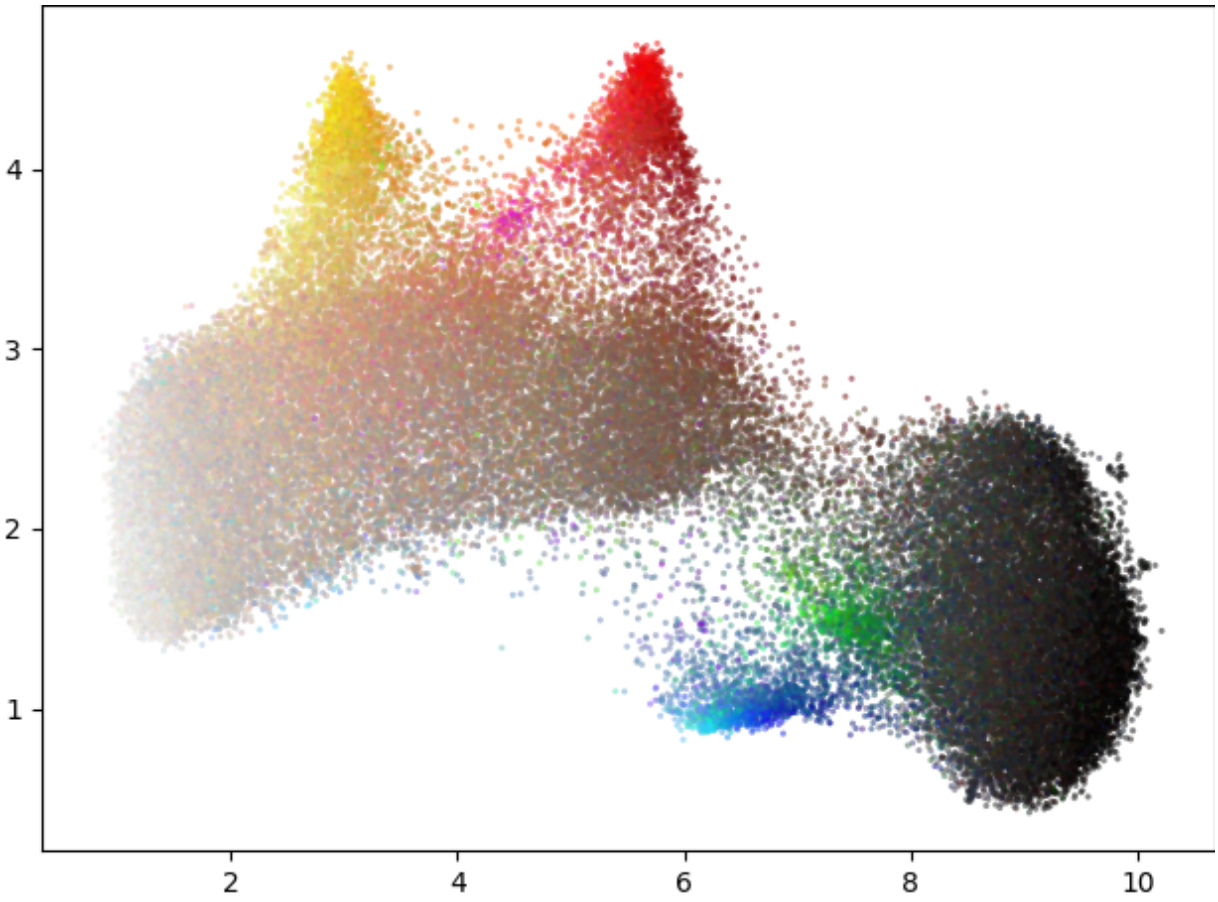
Source: The Author.

nearly all of them were sent directly from the users associated with a group. On the other hand, for images, we observe that 40% have been shared as a forward at least once. This reveals a key difference between these multimedia formats.

Stickers differ from images not only structurally but also in their usage patterns. While there are fewer stickers in total compared to other media types in WhatsApp groups, individual stickers are shared more frequently and directly (not using forwarding) by users in chats. This behavior suggests that stickers may present a collectible quality [170], in which users prefer to curate a collection of stickers that can be readily used in specific situations or as a form of self-expression [154]. To understand this, it is crucial to examine how stickers work on WhatsApp. Without the forwarding mechanism, users need to save them to their collection by marking them as favorite stickers. This process, described in detail by [81], involves selecting a received sticker and choosing the "mark as favorite" option, which adds it to the user's favorites menu. WhatsApp interface reinforces this collection-based experience by providing a dedicated section for users to access their favorite stickers, enabling quick use in chats.

Last, we observed in Figure 5.3 the large volume of stickers posted per day within the public groups monitored from our dataset. Users send over 5,000 stickers per day on average within the groups analyzed, but three significant peaks stand out. The largest occurred on October 6, coinciding with the Brazilian presidential elections, when sticker usage surged to over 17,500, while the second peak was on October 30, during the second round of the elections, with over 13,000 stickers. The third was around September 7,

Figure 5.4: UMAP visualization of all stickers from the WhatsApp dataset.



Source: The Author.

Brazil's Independence Day, an important date in the country's political calendar. It is also interesting to note the gradual increase in the number of stickers as the election period approaches and the sharp drop right after voting day. These spikes underscore the political nature of the dataset and the strong connection between sticker activity and major political events.

5.2 Sticker Content Characterization

In this section, we evaluate sticker content, grouping them by visual similarity, and creating a graph of stickers according to the groups in which they were posted to evaluate.

A visual representation of all stickers collected is shown in Figure 5.4. We created a representation using both the pHash binary vector and each sticker's dominant color. Then, we employed dimensionality reduction via uniform manifold approximation and projection (UMAP) to plot the sticker representations in a 2D space [98]. Each point is

Figure 5.5: Cluster of grouped stickers representing emojis.

(a) (b) (c) (d)

Source: The Author.

associated with the representation of a single sticker, and its color is the dominant color of the actual sticker. It is visible that there is a concentration of red stickers and also green and blue ones, which are related to the context we captured, and related to political campaigns for the 2022 Brazilian elections. The leading left-wing party in Brazil employs red colors associated with the party's branding, while the leading nationalist right-wing party mostly uses green, blue, and yellow colors derived from the Brazilian flag. The stickers in our dataset reflect the partisan nature of the branding of the competing parties. A thorough manual investigation of the yellow chunk of stickers revealed the presence of many "emoji" stickers, which are faces drawn in emoji style representing existing emoji characters. The gray area in the plot encompasses many different sticker styles, and we do not point to a single characteristic of them.

5.2.1 Exploring Visual Similarity

To explore the similarity of these stickers, we leverage image features to cluster and investigate the patterns and characteristics of the stickers. A similar methodology has been employed to study memes in Web communities [167], annotating and mapping them to clusters. Since the perceptual hash (pHash) provides a comparable fingerprint of stickers, we can use it to cluster the stickers through the density-based spatial clustering of applications with noise (DBSCAN) algorithm [35], merging them into visually similar groups of content shared on WhatsApp. Using DBSCAN allows us to investigate the popularity and diversity of stickers and gain insights into their content.

The pHash-grouped sticker clusters reveal sets with variations of images, emojis, or memes, evidencing the dynamics of sticker usage. Some clusters highlight a key characteristic of stickers: their role as both meme-like content and emoji substitutes, as seen in Figures 5.5 and 5.6. Emojis, which are pictorial representations of emotions or objects,

Figure 5.6: Example of the cluster with meme sticker template with small variations.

(a) (b) (c) (d)

Source: The Author.

often take the form of simple, round yellow faces [170]. In the case of stickers, these are frequently more elaborated versions, with some evolving into animated versions. Like emojis, these stickers are commonly used as emotional reactions to messages, providing users with a more visually nuanced way to express themselves in conversations [155].

The meme-associated clusters, on the other hand, consist of a set of analogous images that follow a recognizable template, differentiated only by minor text changes or visual details to express humor or satire. This aligns with the typical behavior of memes, where a base well-known image is edited and remixed across the Internet, maintaining its core template while being adapted to various contexts [55]. This practice of remixing, transforming, and altering base images is central to the meme ecosystem on the Web, where visual elements are modified to reflect cultural or situational humor [86, 87]. Stickers, in this context, also extend this behavior, serving not only as images but as part of a broader visual conversation that blends both expressive and cultural elements.

It is interesting to note that within certain clusters, very visually similar stickers may also portray opposing ideas. In the context of the public political groups encompassed in this work, many clusters are directly related to the poll-leading politicians in the Brazilian 2022 elections and contain advertising/provocative material associated with their campaigns. Here, we can find examples of corresponding stickers that carry drastically opposing partisan content, as shown in Figure 5.7. This cluster grouped two visually analogous stickers, but they are shared in different contexts. The stickers portray an edited image of opposing candidates of the left and right-wing parties in a criminal photo, suggesting that stickers are co-opted by adversary groups and used with opposing semantics but adopted with the same visual aesthetics. These results alert us to the implications of grouping stickers (or any image content) exclusively based on their visual appearance. Small details often imply drastic changes in the semantic value of the sticker.

Figure 5.7: Examples of visually similar stickers used by opposing political leanings.

(a) (b)

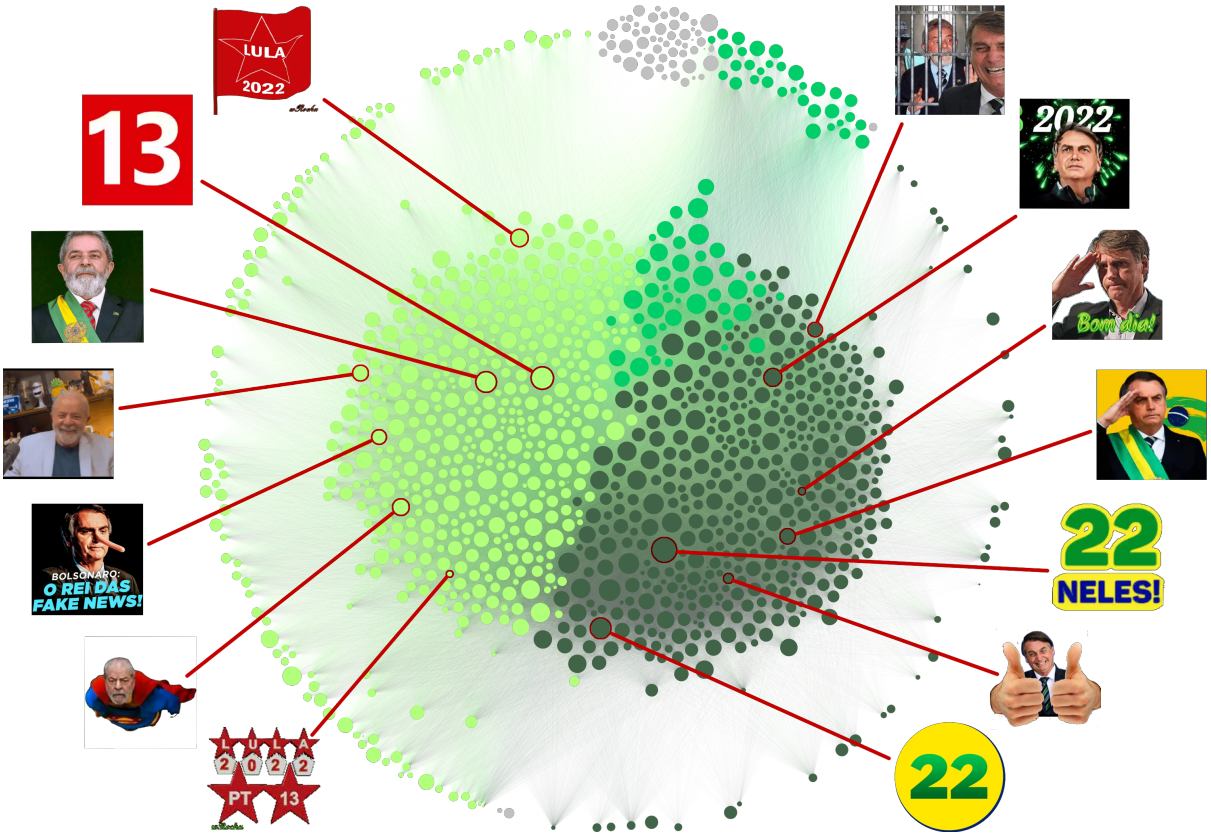
Source: The Author.

5.2.2 Political Alignment of Stickers

As exemplified in the previous section, visually similar stickers can convey drastically different ideas and be used in entirely different contexts. Since groups analyzed in our dataset expose differences in political alignment, activism level, or even in goals or topics discussed, besides the visual appearance of stickers, we also evaluate their similarity based on the context in which they are used. To evaluate the content of stickers from this perspective, and check whether stickers sent in similar groups express similar ideas, we build a graph of stickers shared within the same chats to create a network of stickers based on the groups in which they were shared. Figure 5.8 offers a graph visualization of this network assembled with the most popular stickers in our WhatsApp data. In this graph, each node is a sticker, and they are linked with an edge if both appear in the same group. We also applied a community detection algorithm based on modularity optimization [12] to identify sticker communities within the network. For visualization clarity, we used only stickers shared more than 100 times in the observed groups and edges with at least 10 groups in common.

Even with a very dense network (density measured at 0.698), we could identify two main larger communities and a smaller one. These two main communities reflect the dataset's polarization, featuring very similar stickers from both political leanings. There were two major candidates for the Brazilian 2022 presidential elections (Bolsonaro, a right-wing candidate, and Lula, a left-wing candidate). Most of the stickers found in the monitored public groups represent both sides of this dispute. While some stickers are symbols, numbers, draws, and colors associated with each political party, others portray both candidates as being in a position of leadership as president or in a position of defeat.

Figure 5.8: Stickers network.



Source: The Author.

Numerous stickers aim to criticize or anger members of the opposing political leaning. Together, these sticker archetypes form a unique and connected political community. In contrast, the smaller third community features more diverse content, including sexual content and generic stickers. To analyze the partisan leaning of stickers, we label each monitored group as left-wing, right-wing, or undefined, based on the political stance indicated in the group's name and, when needed, its description. The group annotation shows that most groups support the right-wing candidate Bolsonaro (666 groups), while only 126 groups support a left-wing agenda. The remaining 617 groups were tagged as undefined, as their political alignment could not be determined (e.g., general debate groups or support for other political positions).

Next, we analyze each sticker to determine its political leaning based on the groups that shared it. Then, using the labels of these groups, we calculate the proportion linked to each political side and assign the sticker a label based on the side with the highest proportion. This label indicates whether the sticker is primarily used in right-wing or left-wing contexts. Note that some stickers may be used equally by both sides of the political spectrum or predominantly by groups without a clear political alignment. To prevent mislabeling in such cases, we introduced the third category, "undefined", for stickers without at least 60% majority on either side. This approach allows us to better

	Right	Left	Undefined
Total Groups	666	126	617
Total Stickers	18,158	6,704	32,169

Table 5.1: Political alignment of groups and sticker context.

identify stickers that are closely linked to a political alignment. Through this annotation, we found that 18,000 stickers are strong biased towards usage in right-wing groups and 6,000 towards the left, as shown in Table 5.1. Note that the difference could be explained by the fact that, in Brazil, the right-wing movement is seen to be actively mobilized on WhatsApp [16].

5.3 Political Attacks with Stickers

Given the potential for stickers to convey strong partisan sentiments, our analysis delves into the scenarios in which political stickers serve as tools for provocation or even direct attacks against opposing political groups using our methodology. In the Chapter 4, we analyzed political activism on WhatsApp in Brazil, revealing common types of attacks performed by partisan public groups towards opponent campaigns on WhatsApp. The public nature of these political groups easily allows individuals from adversarial political positions to join, establishing a channel for launching targeted assaults against individuals aligned with opposing ideologies. The ease of one-click sticker sharing may explain why these initiatives are particularly conducive to flooding group chats with divisive content. By identifying the political leaning of stickers, we can examine whether they are being misused in public groups by political campaigns to harass opposing users. To investigate this, we analyze whether stickers predominantly associated with a specific political alignment appear in groups aligned with the opposing spectrum.

Our analysis shows that most politically annotated stickers were used exclusively within their respective ideological groups. However, we also found cases where political stickers transcended party boundaries, appearing in groups with opposing leanings, suggesting politically motivated attacks. Based on these criteria, we identified 869 partisan stickers, with a notable majority (794) exhibiting right-wing bias and being shared in leftist groups. In contrast, only 75 left-wing biased stickers appeared in right-wing groups. A manual evaluation revealed that many of these stickers are either political propaganda supporting the opposing candidate or "humorous" memes intended to provoke group members. We also observed stickers portraying both candidates in derogatory and

humiliating ways, including edited images with sexual connotations, highlighting the offensive nature of some attacks. Notably, creating WhatsApp stickers using a person's face without permission, particularly when intended to insult, harass, or damage their reputation, is already considered illegal in countries like Indonesia [84]. In Brazil, this issue is regulated by broader defamation laws, and there is no specific regulation for WhatsApp. Nonetheless, the Superior Electoral Court has criminalized the massive spread of political content through message applications.[3] In Germany, police reported that child sexual abuse stickers were shared in a climate activism group, putting all members at risk of having illegal content on their devices [81].

Figure 5.9 shows examples of these "political attack" stickers, which promote a partisan candidate in rival environments. The presence of such stickers in politically opposing groups suggests a deliberate act of confrontation by users, trying to cause reactions and distress among individuals holding contrasting political views. For instance, Figures 5.10(a), 5.10(b), 5.10(c), and 5.10(d) depict stickers featuring the right-wing presidential candidate Bolsonaro, perceived as provocative within leftist groups. One sticker even includes the text "Leftists will infarct with hate", tailored to instigate distress. Similarly, leftist stickers depicted in Figures 5.10(g) and 5.10(h) endorse Lula and are also incongruous with right-wing ideologies. Of particular concern are images such as those in Figure 5.10(e), depicting Bolsonaro wielding a firearm, and Figure 5.10(f), featuring heavy boots crushing a red star with the words *"This is our fight. Communism, not here!"*. These images evoke menacing connotations, thereby exacerbating tensions within a polarized online political discourse.

Our findings reveal that clustering stickers based on their image pHashes, which denotes visual similarity, enables the identification of image sets exhibiting even minor variations. However, this may not capture the subtle political context carried with them and may also inadvertently put together stickers with opposite political messages. On the other hand, examining stickers through the perspective of the groups in which they are shared, and thus their political alignment, exhibits a strong association with the contextual environment rather than solely relying on visual resemblances of the images. This highlights the importance of considering the broader sociopolitical context in understanding sticker usage patterns. Furthermore, we observed that stickers often demonstrate remarkably partisan alignments and are frequently utilized as tools for provocation and abuse within political public groups on WhatsApp. This highlights the pivotal role of stickers in expressing and perpetuating political ideologies and tensions within this network.

Moreover, the asymmetric distribution of stickers aligned with right-wing ideologies may reinforce echo chambers and polarization within WhatsApp groups. Users who predominantly encounter content aligned with their own political beliefs may become

[3] https://folha.com/zdu068gh

Figure 5.9: Example of stickers used to "provoke" or "attack" opposing political groups.

(a) (b) (c) (d)

(e) (f) (g) (h)

Source: The Author.

further entrenched in their viewpoints, hindering dialogue and deepening division in online communities. Sharing biased stickers also raises important questions about political engagement and manipulation on social media platforms. The deliberate dissemination of partisan content, particularly in the form of stickers designed to provoke or attack opposing political groups, shows a strategic use of digital media for political propaganda.

5.4 Abusive and Hate Stickers on WhatsApp

Although politically motivated attacks are one form of sticker abuse, others involve offensive and inappropriate content on WhatsApp. In this section, we delve deeper into these pathways, shedding light on the various forms of abusive behavior facilitated by stickers on the platform, including the spread of hate speech. We use the NSFW Yahoo model [91] to measure information on how "explicit" each sticker is. We also use SafeSearch detection with Google Vision API[4] to get complementary data about potentially harmful content being posted on WhatsApp through the stickers.

On WhatsApp, users can freely create customized stickers based on any image they want. However, this model is not unanimous among all messaging apps. Most

[4] https://cloud.google.com/vision/docs/detecting-safe-search

of them have only predetermined and limited sets of stickers that users can use during conversations. Facebook and its messaging system "Messenger" do not allow any users to add their own creations as stickers [44]. The mobile messaging app LINE even sells millions of curated sticker packs per month, and stickers have long been one of LINE's key revenue drivers [131]. Despite Meta restricting stickers on its other platforms and selling stickers can be a highly profitable economic model, for WhatsApp, particularly, Meta chose to let users freely create and share their own stickers. However, this permissive model has some challenges, as it opens the way for the dissemination of offensive and inappropriate content. Not surprisingly, stickers are used to distribute not only memes, but also illegal content such as child sexual abuse material [43] and Nazi propaganda [136]. Even worse, WhatsApp automatically saves every sticker received in a chat, hence users may have incriminating stickers on their devices without knowing or wanting to [81].

WhatsApp's terms of service, however, state that stickers created must be legal, authorized, and acceptable images. Furthermore, users are not allowed to use WhatsApp services in ways "*that are obscene, defamatory, threatening, intimidating, harassing, hateful, racially or ethnically offensive, or instigate or encourage conduct that would be illegal, such as promoting violent crimes*". Although WhatsApp's TOS does not allow for offensive stickers, a quick manual inspection of the top 5,000 most popular stickers shared within our dataset revealed clear examples of stickers that do not comply with these rules. There were instances of stickers depicting extreme violence, hate symbols, degrading pornography, and highly repulsive images.

Figure 5.10 presents hate stickers found in our dataset. Sticker 5.11(a) is an example of a homophobic image against LGBTQIA+ people; Sticker 5.11(b) depicts a swastika, symbolizing Nazism; Sticker 5.11(c) shows a black man holding a knife alongside the phrase "around blacks never relax", which is a recurring racist remark on the Web. Similarly, Sticker 5.11(d) portrays a derogatory caricature of a Jewish man, reflecting antisemitic stereotypes, which is also a widely known hate symbol.[5] These examples demonstrate that stickers, freely sent and shared between users on WhatsApp, can be used as media for targeted harassment and attacks against marginalized communities.

In our data, we also found a considerable presence of stickers with sexually explicit content. To evaluate this, we apply the convolutional neural network model for Not Safe for Work (NSFW) proposed by Yahoo Inc. [91] to identify adult-themed stickers. Images with a score greater than 80% are labeled as explicit. Figure 5.12(a) presents the volume of NSFW stickers. Compared to images, stickers are five times more likely to depict explicit content (0.5% of images and 2.3% of stickers are NSFW). In total, we discovered 33,335 messages containing NSFW stickers, accounting for 5.5% of all sticker messages. As shown in Figure 5.12(b), around 10% of users in the monitored groups shared NSFW sticker, and some individuals posted hundreds of NSFW stickers. There is even a peculiar

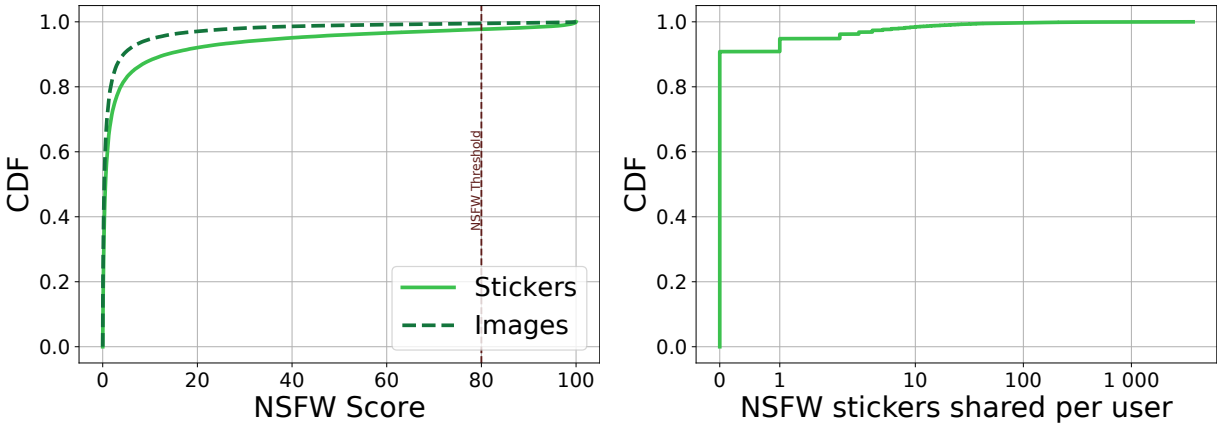
[5] https://www.adl.org/resources/hate-symbol/happy-merchant

Figure 5.10: Example of offensive stickers sent by users that violate WhatsApp's terms of use.

(a) (b) (c) (d)

Source: The Author.

Figure 5.11: Distribution of NSFW stickers sent.



(a) NSFW Score (b) NSFW per Users

Source: The Author.

user who shared more than 3,000 NSFW stickers. These findings suggest abusive behavior, particularly given that these public political groups are typically not intended for adult content, with some even explicitly forbidding it in their descriptions.

Furthermore, we evaluate other categories of NSFW content through the Safe Search detection from Google's Vision API.[6] This tool detects content within an image across five categories (adult, spoof, medical, violence, and racy) and returns the likelihood for each one of them. According to the API, Adult content encompasses elements such as nudity, pornographic images, cartoons, and activities of a sexual nature. The medical category accounts for the likelihood that the content is associated with medical imagery (e.g. wounds, surgeries, blood). Violence offers an estimation of the probability that the image portrays a violent action. Spoof is the likelihood that a modification was made to the image's canonical version to make it appear funny or offensive. Content deemed racy may include (but is not limited to) skimpy clothing and strategically covered nudity, lewd, provocative poses, and extreme close-ups of sensitive body areas. In Table 5.2, we aggre-

[6] https://cloud.google.com/vision

	Unique Stickers	Number of Shares
Yahoo_NSFW	1,322 (2.3%)	33,335 (5.05%)
Adult	1,423 (2.5%)	30,828 (4.6%)
Violence	416 (0.7%)	4,583 (0.7%)
Racy	4,503 (7.9%)	55,476 (8.4%)
Medical	735 (1.3%)	14,300 (2.1%)
Spoof	17,834 (31.2%)	150,351 (22.7%)

Table 5.2: "Not Safe" stickers categories on WhatsApp.

gated the results of Safe Search detection on our data collection of stickers, considering the likely and very likely labels for each category.

These findings underscore the urgent need for moderation and enforcement of content guidelines within WhatsApp's sticker ecosystem. While stickers enhance user engagement and communication [154], their misuse brings significant risks, including promoting hate speech, reinforcing harmful stereotypes, and creating unsafe environments within online communities. Our analysis suggests adopting strategies such as using automated tools to detect offensive, NSFW, or adult content and restrict potentially harmful stickers. Despite WhatsApp's encrypted ecosystem, studies have proposed system architectures for moderate content on the platform [77] without violating the privacy of its users [122]. Since these stickers are primarily derived from existing images, the platform could offer alternatives to restrict the creation of content that violates community standards.

5.5 Summary

In this chapter, we explored the multifaceted role of stickers in WhatsApp's political ecosystem, focusing both on their expressive potential and on their abuse during the 2022 Brazilian presidential election. Analyzing 650,000 sticker messages across 1,600 public groups, we characterized their usage patterns, visual features, political alignment, and potential for abuse. Our findings reveal some characteristics that suggest stickers are indeed a distinctive media format while also sharing similarities with others: stickers are less frequently sent compared to other media types, such as images within groups. However, a single sticker usually presents higher total shares, which means they exhibit a higher rate of recurrence within conversations, similar to an emoji. Moreover, stickers are rarely forwarded, suggesting that users often save and keep their collection of preferred stickers for future use instead of using the system's forwarding tools. This behavior highlights the collectible nature of stickers, in which individuals accumulate a personalized

repertoire of stickers to deploy on various occasions, like an emoji or a meme.

However, we also uncover instances where visually similar stickers convey entirely different meanings, emphasizing the importance of considering other aspects when grouping images by perceptual hashes. Particularly in political groups, where misinformation is a concerning issue, it is important to avoid merging distinct ideas within the same category, especially when minor alterations in images could propagate misleading narratives. Furthermore, we analyzed the political alignment of the stickers by building a network of co-occurrence in public groups. This network analysis resulted in two prominent communities of stickers, mirroring the polarized partisan landscape of our political WhatsApp dataset, and finding a strong association between stickers and political affiliations. Notably, we observe instances where political stickers are shared across ideologically opposing groups, often serving as tools for attacks and abuse on WhatsApp.

Our results reveal the urgent need for better moderation mechanisms to curb the dissemination of offensive stickers and safeguard users from encountering inappropriate content on WhatsApp. We identified a significant prevalence of potentially offensive sticker messages, including homophobia, hate symbols, racist stereotypes, and derogatory depictions of marginalized groups. We also observed that stickers are five times more likely to depict explicit (NSFW) content compared to images. Explicit content accounts for 2.3% of unique stickers and 5% of all sticker messages. Additionally, we identified a substantial volume of violent (0.7%), medical (2.1%), and racy (8.4%) stickers, which may be sensitive for certain audiences, especially in public groups. Given the visual immediacy of stickers, the unrestricted access to public groups, and the ease with which users can create and disseminate stickers from virtually any image, there are significant risks of offensive content spreading unchecked due to a lack of moderation. Despite WhatsApp's private and encrypted nature, our research provides valuable insights into how stickers are used within public political groups, bringing more understanding and transparency to the platform, particularly about the substantial abuse of stickers with offensive content disseminated on WhatsApp, which requires actions to bring more safety to users.

Chapter 6

From Fake News to Real Protests: Coordination in Public Groups

Upcoming elections in different countries come together with serious concerns about election integrity. Those concerns are mainly associated with the uncontrolled dissemination of misinformation in social media [60], the increasing polarization [27] and radicalization [129], the indiscriminate use of targeted advertising [137] and social bots [46], the increasingly personalized feed algorithms from social media platforms [129]. Those concerns are more worrisome as different AI models become readily accessible, simplifying the creation of misinformation [7].

Since 2018, misinformation campaigns in Brazil took place in a new digital space, yet poorly understood: messaging platforms such as WhatsApp [10]. After the 2018 elections in Brazil, WhatsApp acknowledged the existence of coordinated campaigns that spread massive amounts of messages during the 2018 presidential elections in Brazil [99]. To mitigate the problem, WhatsApp took steps to reduce its virality features by limiting how much content can be forwarded [102]. On the other hand, the Superior Electoral Court, responsible for Brazil's elections, has criminalized the massive spread of political content through message applications[1]

However, although those countermeasures are very welcome, they are still limited. First, bypassing the forwarding limit was quite simple and ineffective [103]. Second, WhatsApp introduced new features that increased virality and facilitated massive spreading. For example, WhatsApp introduced communities, which allow one to manage and post in multiple groups simultaneously.[2] Finally, although a coordinated campaign for sharing political content in WhatsApp can be considered an electoral crime in Brazil, auditing any activity in WhatsApp is very difficult, given the closed nature of the application [120].

In this chapter, we aim to investigate the existence of coordinated campaigns. Specifically, we will examine whether there is evidence of coordinated accounts actively spreading messages on the platform. Furthermore, we will explore the content and goals of the coordinated messages and analyze how they relate to recent Brazilian political events.

[1] https://folha.com/zdu068gh
[2] https://faq.whatsapp.com/495856382464992

Despite there are works studying coordination on WhatsApp [114, 115], they bring a definition of coordination at the group level, using network structure and backbone extraction to identify coordination by the similarity of the content posted. In contrast, our paper presents a different and more restrictive definition, rapid coordination, adapted from [118]. This approach considers the content similarity and the synchronous posting behavior to identify coordinated accounts. This brings a completely different perspective on coordination in WhatsApp, which has not been explored before. Here, we focus on identifying consistent and synchronous coordination efforts on WhatsApp that leverage the instantaneous nature of the platform to boost and amplify messages. Furthermore, to the best of our knowledge, this is the first large-scale study to explore rapid coordination on WhatsApp using a large dataset of more than 13M messages collected over seven months, covering recent important events in Brazil. We gathered an extensive messaging collection of Brazilian political public groups, considering seven months of data from July 2022 until January 2023. This period captures significant Brazilian events such as the 2022 presidential election, attacks on the electoral process, and riots that ended with an attack on Brazil's federal government buildings on 8 January[3]. In total, this study analyzes 13,452,039 million messages shared in 1,444 groups from 100 thousand users. The huge data volume allows us to observe a different perspective by incorporating temporal similarity to identify synchronous coordination actions. By including a similarity of time posting, we can identify more consistent cooperation between accounts [58]. Additionally, we aim to investigate different coordination formats, including text, images, and videos.

This chapter is organized as follows: First, we define rapid coordination and present the modeling approach used to identify such coordination (Section 6.1). Next, we apply this approach to detect coordination activity (Section 6.2) and analyze coordination messages (Section 6.3), characterizing the text (Section 6.3.1), URLs (Section 6.3.2), and images (Section 6.3.3) involved. Finally, we explore the content of these coordination messages to better understand the goals behind the coordinated efforts (Section 6.4).

6.1 Rapid Coordination

Coordinated activity is a well-known phenomenon on various social networks, where users employ it for various purposes, such as sharing beliefs, marketing, mobilizing people, shaping public opinion, and spreading misinformation [112]. In WhatsApp, the main messaging app in Brazil, particularly for political purposes, coordinated accounts can take advantage of the platform to amplify engagement in specific activities.

[3] https://en.wikipedia.org/wiki/2023_Brazilian_Congress_attack

These groups of users often replicate similar behaviors over time, such as endorsing certain messages and amplifying specific content.

Due to the widespread use of WhatsApp for content spreading, our goal is to identify networks of accounts that share the same content rapidly, simultaneously, and repeatedly in a coordinated way. Although there are works studying coordination on WhatsApp [114, 115], they bring a definition of coordination to the group level, using network structure and backbone extraction to identify coordination by the similarity of posted content. In contrast, our goal represents a different and more restrictive definition, rapid coordination. This approach considers the content similarity and the synchronous posting behavior to identify coordinated accounts. This brings a completely different perspective on coordination in WhatsApp, which has not been explored before. Here, we focus on identifying consistent and synchronous coordination efforts on WhatsApp that leverage the instantaneous nature of the platform to amplify messages.

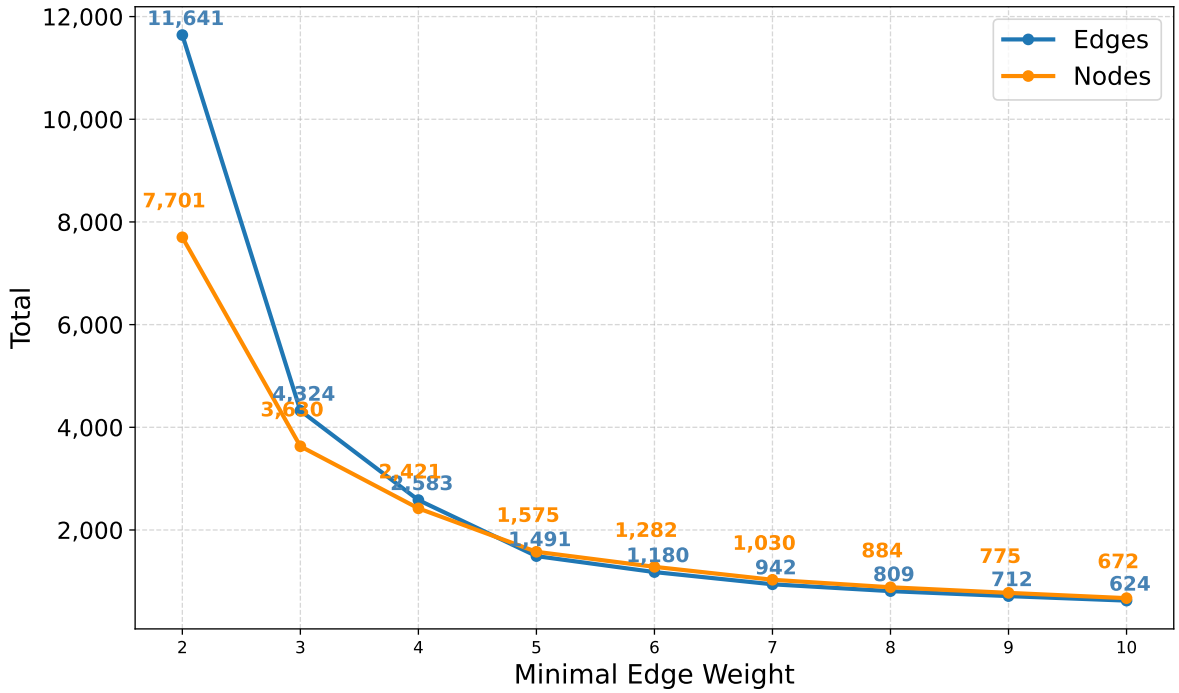
6.1.1 Rapid Spread Network Modeling

To achieve this, we adapted the Rapid Retweet Network proposed by [118], which was originally applied to the Twitter ecosystem, focusing on retweet actions. This approach is particularly effective for identifying groups of accounts that consistently retweet the same source. On WhatsApp, there are no retweets like on Twitter. Instead, users typically receive content and share it in two main ways: directly forwarding the message to another group or copying and pasting the content into a different group.

We define the Rapid Spread Network based on the simultaneous sharing of similar messages within a specific time window. To analyze content similarity within WhatsApp data, we adopted the MD5 hash algorithm to detect identical messages and identify shares of the same content. This method assigns a unique identifier to each unique message, where two messages are considered identical only if they have the same hash. Any modification results in a different hash. With these definitions, we build a weighted network where users are connected if they post the same message in the same time window. In the network $G(V, E)$, a node $v \in V$ corresponds to users who post messages on WhatsApp. The undirected weighted edge $e = (v_i, v_j)$ is included in the users v_i and v_j if they posted the same message in the same time interval. The edge weight of w_{ij} represents the total number of messages they have shared in common during the time window.

On WhatsApp, the private nature of the platform prevents the identification of the source or promoters of a message. Consequently, the network analyzed in this study is composed of users who disseminate identical content simultaneously, highlighting the

Figure 6.1: Coordinated users by alterations in parameters.



Source: The Author.

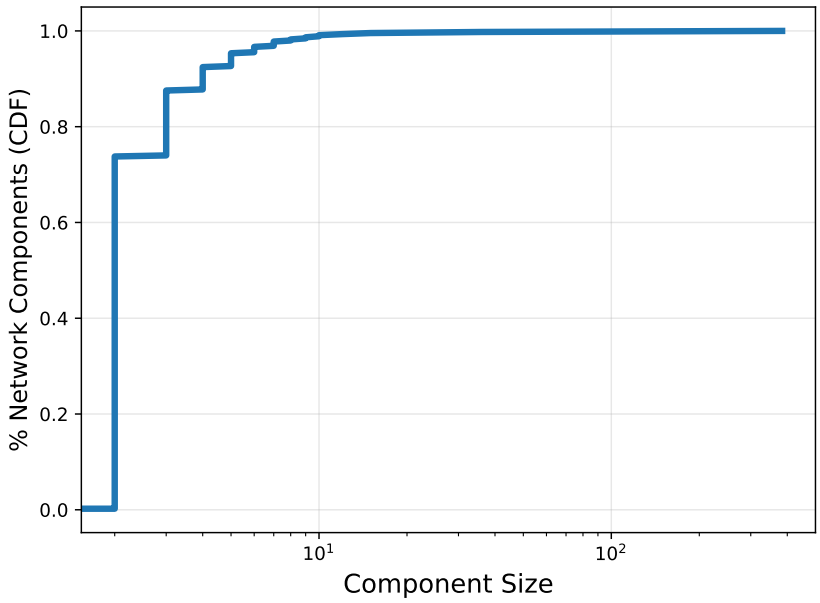
accounts and messages propagated concurrently across the network.

6.2 Identifying Coordinated Activity

Before applying the Rapid Spread Network to model the propagation of coordinated messages, we implemented a series of restrictive adjustments and parameter selections to ensure that we would only capture orchestrated actions by coordinated accounts. First, we selected a 60-second time window[4] to define rapid actions, allowing us to identify potential coordination by users acting simultaneously [78]. To avoid misclassifying common messages frequently shared on WhatsApp (e.g., "good morning", "hello") as coordinated actions, we also filtered out short messages with less than two words. Given the message flow and the large period observed, we tested various threshold values, as shown in Figure 6.1. Using the elbow method, we determined the optimal threshold by identifying the inflection point on the curve. Consequently, we filtered out edges with weights below five to build the final graph. The resulting coordination network comprises 1,575 nodes and 1,491 edges, with an average degree of 1.89.

[4]We performed a sensitivity analysis with varying thresholds to determine whether 60 seconds is a suitable threshold. Please see Appendix B for more details.

Figure 6.2: Component size distribution.

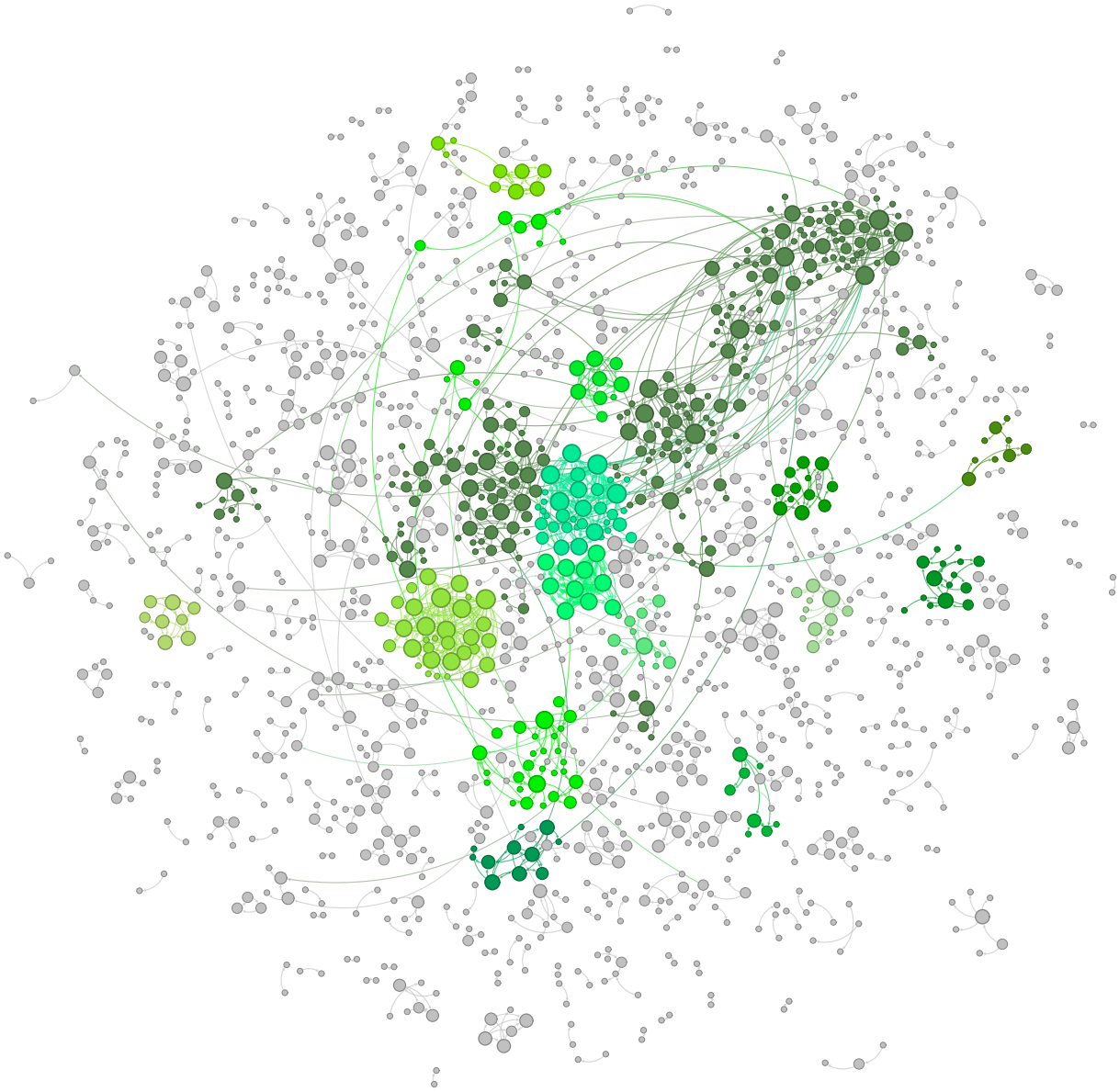


Source: The Author.

Although we are only examining a subset of the WhatsApp ecosystem, we can still observe a clear structure in the propagation of messages. One notable feature of this network is the presence of 450 unique components, which suggests that the network is not densely connected. This fragmentation is significant because it reveals the existence of many isolated pairs or small groups of accounts acting independently to coordinate messages. This high number of unique components suggests a decentralized coordination effort on WhatsApp, where many accounts operate separately to amplify their content rather than a single cohesive group controlling the flow of information. Figure 6.2 presents the cumulative distribution function (CDF) of component sizes, showing that the majority of coordinated components consist of two accounts (73.7%).

Furthermore, we identified a large connected component comprising 332 nodes (21% of the total network). This more connected group demonstrates that while much of the network consists of isolated actors, there is another aspect of coordination, with a substantial cluster of coordinated accounts operating together. This large component suggests a more organized structure within the WhatsApp ecosystem, in which many accounts are coordinated to propagate messages quickly and efficiently. Given WhatsApp's closed and encrypted architecture, it may be challenging for authentic users to differentiate this coordinated activity, making it even more concerning. Using the Louvain community detection algorithm [13], we further identified some communities within the large connected component, highlighting the coordinated nature of these accounts, as shown in Figure 6.3. The presence of multiple communities suggests that coordination on WhatsApp can extend beyond pairs of synchronized accounts, allowing them to reach a wider

Figure 6.3: Rapid Coordination Network.

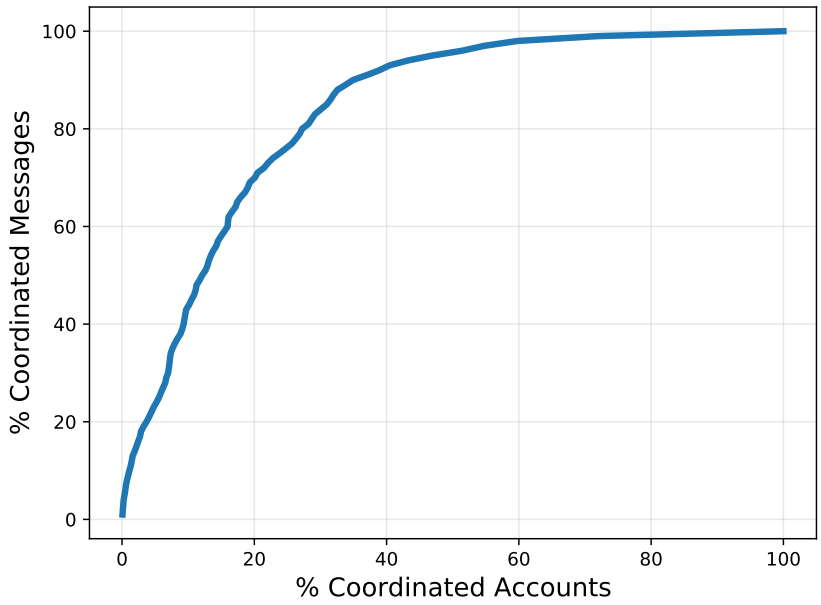


Source: The Author.

audience. These communities could be used to amplify specific narratives or target particular themes within political discussions. We observed that the three largest identified communities contribute significantly to the flow of message propagation on WhatsApp. These communities consist of 301 accounts (19% of all coordinated accounts) and together posted 4,982 messages (34.5% of all coordinated messages). Coordinated accounts in these communities reached 664 groups (45.9% of all groups observed). This scenario helps us understand the impact of coordination and how the WhatsApp environment is conducive to coordinated actions, in which some users can affect a representative part of the group ecosystem.

After we identified the coordinated accounts, we analyzed their messages. Ac-

Figure 6.4: Coordinated messages by coordinated accounts.



Source: The Author.

cording to our definition, messages are considered coordinated only if they are posted simultaneously by two or more coordinated accounts in the same time window. Considering these synchronous coordinated messages, we evaluated the portion of messages posted by the coordinated accounts within our dataset. We identified a concentration of coordinated activity, in which we observed that 80% of the coordinated messages are generated by 27.2% of the accounts, as shown in Figure 6.4. This suggests that, while many users are involved in sending messages, a relatively small subset of coordinated accounts is responsible for most of the messaging campaigns within the political public groups. This indicates a structured and orchestrated use of WhatsApp for coordinated political activity, with some actors playing a key role in shaping the network dynamics. However, this remains largely hidden from public view due to the platform's design.

Takeaways The main takeaways from this section are:

- Our methodology has identified more than 1,575 coordinated accounts actively disseminating political messages.
- There are decentralized coordination efforts in which accounts operate separately to amplify their messages, totaling 450 components.
- A small part of coordinated accounts (27.2%) are responsible for most of the flow of coordinated messages (80%).

6.3 Analyzing Coordinated Messages

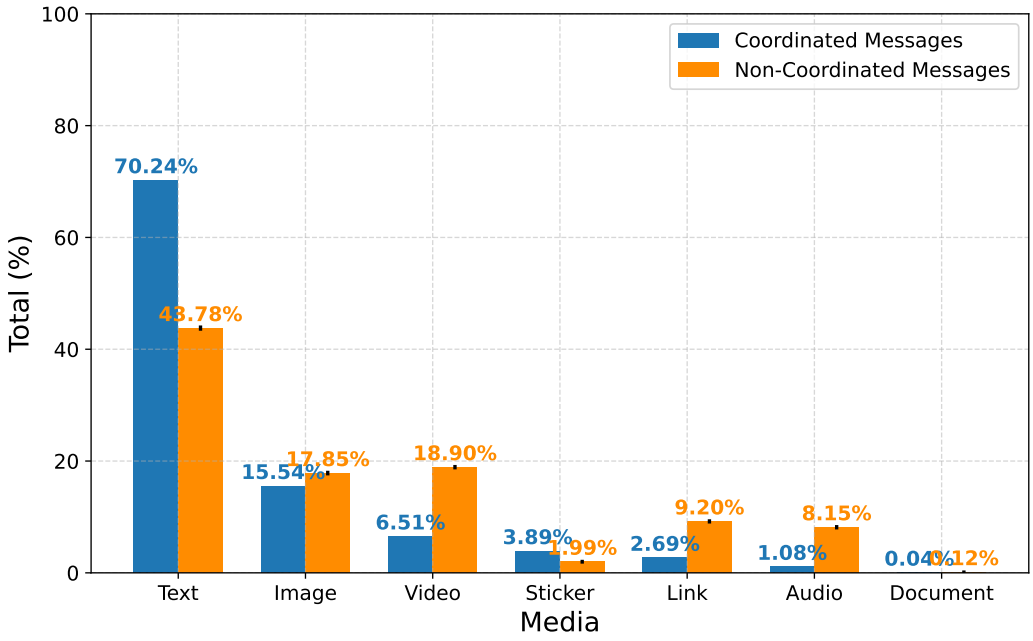
To delve even further into coordinated accounts, we examined their activities, focusing on understanding the messages they shared and their underlying motivations. Since we identified the coordinated accounts, we identified their posted coordinated messages, totaling 14,414 messages. It is important to remember that based on our coordination definition, a coordinated message is posted simultaneously by two or more accounts.

To provide a more contextualized analysis, we created 35 random samples of non-coordinated messages, each matched in size to the coordinated messages. This allowed us to perform a comparative analysis to identify distinctive patterns between coordinated and non-coordinated messages, while ensuring the robustness of our findings with a 95% confidence interval. Similarly to rapid network construction, this sample only includes text messages with more than two words. Figure 6.5 compares the types of media found in these two groups of messages. Text messages are the most common form of communication in coordinated messages, comprising 70.24% (10,124 messages) of the total 14,414 coordinated messages, compared to 43.78% ($\pm$0.1702) in non-coordinated. This significant difference highlights the efficiency of text messages, which are easily shared and forwarded without access to external media files or galleries. Images appeared in 15.54% of coordinated messages, aligning with 17.85% ($\pm$0.1145) in non-coordinated messages. Notably, videos, links, audio, and documents are rarely used in coordinated messages.

Another notable observation is that stickers are more common in coordinated content. While stickers are generally used as a spontaneous form of communication, their use among coordinated users suggests that they can serve as a resource to a flooding attack in a group [74]. A flooding attack occurs when one or more users overwhelm a group with a high volume of duplicate messages in a short period, intending to disrupt the flow of conversation or even crash the group, and usually use stickers [74]. When we applied this definition to observe one of the most popular right-wing groups in our dataset, we identified a flooding attack in which three coordinated users sent over 1,200 duplicate sticker messages within seven minutes. These stickers were primarily composed of provocative content and political attacks. This suggests that, although stickers are less commonly used than text messages, coordinated users can significantly amplify the impact of a sticker flooding attack, making it more effective in achieving its disruptive goals.

When analyzing coordination efforts, it becomes clear that the main goal is to spread messages among as many groups as possible. Text messages are particularly well-suited for this purpose, as they are easy to share and read. Unlike other media formats that require downloads or additional actions, text messages allow for direct and easy communication. This simplicity makes them an ideal choice for disseminating coordinated

Figure 6.5: Messages media type differences from coordinated and non-coordinated messages.



Source: The Author.

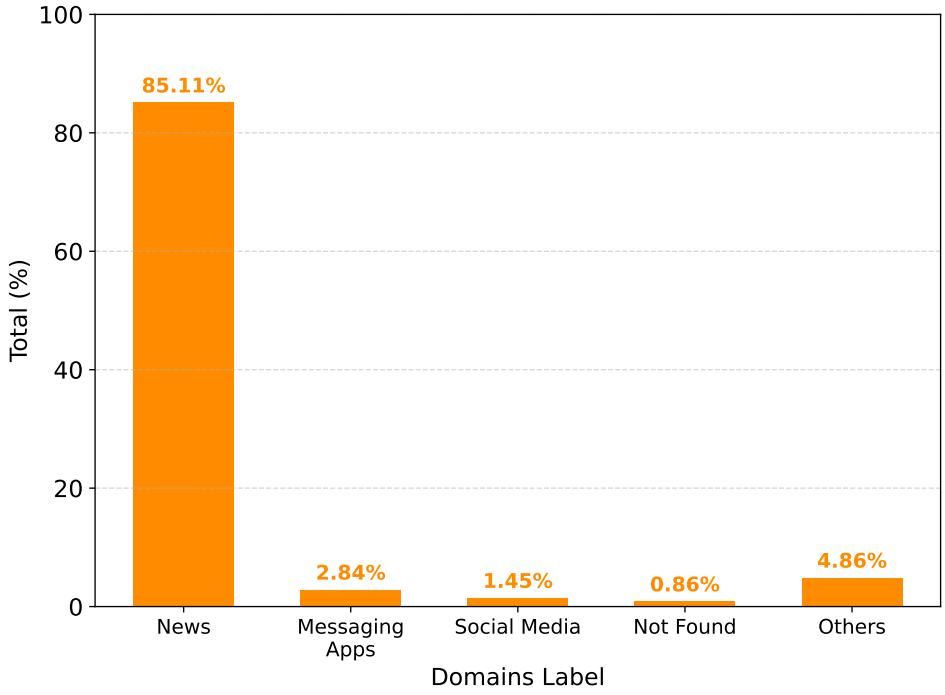
content.

Additionally, we found that 58.9% of coordinated messages were not forwarded. This suggests that most coordinated message sharing is not done through WhatsApp's forwarding mechanism, indicating a deliberate effort to share messages directly, as this mechanism is not widely used. WhatsApp has introduced this feature to combat misinformation and virality by labeling popular forwarded messages with the "forwarded many times" tag [103]. However, our findings suggest that this measure is ineffective in limiting the mass spread of coordinated accounts.

6.3.1 Characterizing Text Messages

Looking at the structure of coordinated text messages, we note an average length of 17.93 words with a standard deviation of 24.19. In contrast, non-coordinated messages are longer, with an average of 24.68 words (±0.4659), but show a much higher standard deviation of 106.07 (±26.74), suggesting significant variation in length. While coordinated messages are generally shorter than the average, the low standard deviation suggests they have a more consistent length than non-coordinated messages, which show greater vari-

Figure 6.6: Category of URLs found in coordinated text messages.



Source: The Author.

ability. This suggests that coordinated messages are not random but contain consistent information to engage users effectively.

6.3.2 Characterizing URLs

Upon closer inspection of the 10,124 coordinated text messages, we observe that 97.31% contain embedded URLs, reflecting the widespread use of hyperlinks by coordinated accounts. These URLs are seamlessly integrated into the text, suggesting that these textual messages not only inform but also direct users to external web resources. Compared with the sample of non-coordinated texts, we find that only 16.91% ($\pm$0.0009) contain links, highlighting a distinct difference between coordinated and non-coordinated messages.

Further analysis of URLs within coordinated messages involved an extraction and manual labeling process. By parsing the coordinated text messages, we found 11,725 links, of which 10,269 were unique. We extracted the domain of each URL from the coordinated text messages, resulting in a subset of 116 unique domains. This indicates that coordinated messages disseminate content from a small number of websites. Here, we characterize the content by undertaking a qualitative analysis to better understand

Domain	Category	Total URLs
pensandodireita*	news	2,403
portaltocanews	news	2,119
redebrasilnews	news	682
gazetabrasil	news	432
whatsapp	messaging apps	293
macajubaacontece	news	291
terrabrasilnoticias*	news	274
brazilnewsinforma	news	263
portalcidade	news	232
direitaonline	news	203

Table 6.1: TOP-10 URLs domains found in coordinated text messages. Domains in bold are sites that employed misinformation strategies during the 2022 electoral campaign, as reported by Aos Fatos Fact Checker

.

the nature of these domains. Initially, we compiled a list of all domains and created a codebook with preliminary codes, refining them iteratively until no further changes were necessary. Our codebook consists of five codes:

- **News**: Websites that host structured news content.
- **Messaging Apps:** Invitations to Telegram and WhatsApp groups/channels.
- **Social Media:** Links to social media platforms such as Facebook, Twitter, Instagram, YouTube, and TikTok.
- **Not Found:** Domains that do not exist or are currently unavailable.
- **Others:** Links that lead to product sales, app stores, or banking services, as well as websites that show characteristics of spam or fraudulent activities.

After building the codebook, we applied it to categorize all domains identified in the coordinated messages. This labeling process allowed us to determine the thematic focus of each shared URL. Figure 6.6 shows the distribution of the coordinated link category. Upon analyzing the results, we observed that 85.11% of all URLs within coordinated messages lead to news websites. Furthermore, messaging apps account for 2.84%, which is particularly interesting because coordinated accounts leverage public platforms to invite others to more exclusive private communities through group invitations. Typically, they share a message that includes an invitation link to other groups.

The significant prevalence of coordinated messages containing links to news websites provides valuable insight into the strategies employed by coordinated users. This suggests a deliberate focus among coordinated users on disseminating news-related content within WhatsApp groups to engage users in propagating specific narratives. By including news links, coordinated users attempt to bring a sense of formality and credibility to their messages. Moreover, including news links serves as a mechanism to drive

traffic to various news websites, thereby expanding the reach and influence of the disseminated information. Notably, websites hosting such coordinated news can generate revenue through advertisements, as shown by the Aos Fatos Fact-Checker.[5]

WhatsApp lacks mechanisms to verify information sources, and this is an ideal scenario in which coordinated users can exploit the platform's ecosystem to disseminate misinformation. This enables coordinated users to leverage WhatsApp as a tool for misinformation, potentially manipulating public opinion. Within political groups, individuals become deeply engaged with particular topics, facilitating the spread of news that aligns with specific narratives. As a result, these coordinated efforts can effectively spread messages that reinforce specific narratives in groups.

Upon analyzing the most frequently shared domains by coordinated users, we found the ten most shared domains in the messages in Table 6.1. Fact-checking agencies revealed that *pensandodireita (1º)* and *terrabrasilnoticias (7º)* domains spread fake news and misinformation. We adopt the definition of misinformation provided by the Aos Fatos fact-checking, which highlights that these websites employed misinformation strategies in their news coverage during the 2022 electoral campaign. According to Aos Fatos, these two websites promote their news across messaging app platforms to attract users to their platforms. These websites typically use multiple ads that eventually engage users who click on these ads, thereby generating additional revenue for the website owner. This discovery sheds light on the deliberate strategies employed to exploit misinformation content for financial gain. Notably, we found that 26% of all links identified in coordinated text messages are from these two misinformation websites, highlighting the role of coordinated accounts in the dissemination of misinformation.

6.3.3 Characterizing Images

Coordinated accounts also use image content to spread narratives, accounting for 15.54% of coordinated messages. Analyzing these images is crucial to understanding the similarities of media types shared in coordinated actions. Observing the ten most shared coordinated messages, we identified that five of these images are related to politics and presidential elections, including promoting candidates or attacking opponents. These images have a different impact on the user's perception, and the visual content can condense more information into a small piece of content. This makes images particularly effective for spreading misinformation, often by presenting events out of context or making old events appear recent. We observed that two of the ten most shared images were mis-

[5] https://aosfatos.org/s/w6gbyzq/

Figure 6.7: TOP-6 coordinated images based on total shares.

(a) (b) (c)

(d) (e) (f)

Source: The Author.

information. The figure 6.8(f), shared 396 times, is the sixth most shared coordinated image. The image is authentic, but the text puts it in the wrong context. Comprova's fact-checking team labeled this image misleading.[6] Another noteworthy example is the fifth most shared coordinated image, as shown in Figure 6.8(e), shared 427 times. This is an authentic picture, but the text puts this image in a different context, saying that one of the members present is a former Supreme Court justice. This image was classified as false by Aos Fatos Fact-checking organization.[7]

Furthermore, two of the analyzed images target the Supreme Federal Court and the electoral process, as shown in Figures 6.8(c) (shared 439 times) and 6.8(e). These two images aim to discredit the judicial decisions and accuse the court of political bias.

[6] https://projetocomprova.com.br/post/re_2B5W8XYjrLpY/
[7] https://aosfatos.org/s/r3i3wti/

This theme was particularly prominent in Brazil, as reflected in the identified topics presented in Table 6.2. A noteworthy aspect of the coordinated images is that some images encourage users to share the message, such as Figure 6.8(b), which has been shared 460 times. Additionally, three of the images are related to credit cards and financial topics. One example is Figure 6.8(d), which depicts a credit card and was shared 430 times.

Takeaways The main takeaways from this section are:

- Coordinated activities focus on news dissemination. 70.24% of coordinated messages consist of text, and 97.31% contain embedded links, with 85.11% of these links leading to political news.
- We found that 26% of all coordinated links are from news misinformation websites.
- Images are a key part of the content shared (15.54%) by coordinated accounts and also include misleading content. Notably, two of the ten most shared images were labeled as misleading content.

6.4 Topic Modeling

Going deeper into the content analysis, we conducted a topic modeling analysis to examine the content of coordinated messages, focusing on identifying their connections with political events. We characterized the topics discussed in coordinated textual messages shared by the coordinated accounts. For this purpose, we employed BERTopic, a topic modeling technique that generates dense clusters to produce interpretable topics. This method uses vector representation (embeddings) and the concept of c-TF-IDF to create coherent topics, preserving key terms in the topic descriptions that enhance the clarity and interpretation [61].

We start by converting coordinated WhatsApp messages into vector embeddings using the PTT5 transformer language model, which was trained on Portuguese Wikipedia data and contains 200 million parameters [20].[8] Next, we apply dimensionality reduction with the Uniform Manifold Approximation and Projection (UMAP) technique, which preserves both local and global structures of the embeddings. Then, we use a hierarchical clustering algorithm (HDBSCAN) to group the vector representations into clusters based on semantic similarities. Finally, we extract topics for each cluster using the Class Term Frequency-Inverse Document Frequency (c-TF-IDF), identifying the most relevant terms

[8] https://huggingface.co/unicamp-dl/ptt5-large-portuguese-vocab

given all documents in a cluster. Then, we refined the approach to balance the number of topics with the size of our dataset. Following the recommendations in the BERTopic documentation, we set the number of topics to 15. To further improve the results, we applied the outlier reduction method to reassign these outlier documents to the appropriate topics. UMAP was configured with ten neighbors, ten components, and a minimum distance of 0.05 for effective dimensionality reduction. Finally, we configured HDBSCAN with a minimum cluster size of 50 and a minimal sample of 50, specifying the minimum number of messages a topic can represent and ensuring that only significant topics are considered for analysis. Additionally, the epsilon parameter was set to 0.3, defining the maximum distance for points to be considered neighbors.

6.4.1 Topic Analyzes

Before analyzing the topics, it is important to understand the political scenario of Brazil during the period analyzed. In 2022, Brazil had a presidential election and, during this period, social networks and messaging apps were flooded with political discussions and campaigns. Furthermore, the analyzed period includes other important events, such as the intense protests marked by widespread fraud allegations about the results and the riots on January 8th. In addition, many protests were made against the decisions of the Supreme Federal Court and its ministers, which became a major topic in the news.

With that in mind, we can observe Table 6.2, which contains the discussed topics identified using the proposed framework. Initially, we can observe many political topics addressing different perspectives on the Brazilian elections. One major focus is the Supreme Court, which became the center of many protests, with several ministers' attacks (Topic 1). Additionally, many messages contain terms related to election fraud (Topic 5), as a large portion of the population refused to accept the results, claiming that it was rigged and asking for military intervention (Topic 15). We also observe discussions about journalists (Topic 6), political candidates (Topic 8), and political debate repercussions (Topic 10). Also, some topics reflect government arguments promoting the candidates' achievements (Topic 7), which relate to fuel and price reductions. Coordinated messages also include government assistance and subsidies for low-income individuals (Topic 14). Initially, we observed that the coordinated messages were related to the Brazilian political scenario, which gave us an idea of the interest of coordinated accounts in reinforcing specific narratives.

Furthermore, we identified topics unrelated to politics, such as messages about credit cards, bank loans, and financial resources (Topics 2 and 13). There is also content

Id	Label	Topic Terms
1	**Supreme Court of Justice - stf (42.9%)**	moraes, stf, pt, federal, minister, tse, round, whatsapp, police, pt supporter
2	**Credit Card (15%)**	thousand, card, credit, aid, cash, millions, bank, vacancies, request, receive
3	**Videos (8%)**	video, audio, activate, screen, husband, caught, wife, lover, videos, shows
4	**Social Networks (5.1%)**	telegram, whatsapp, twitter, network, social, facebook, instagram, follow, forget, follow us
5	**Election Fraud (4.6%)**	electoral court, electoral, crime, crimes, propaganda, fraud, operation, federal police, ballot boxes, elections
6	**Journalist Commentators (2.9%)**	shorts, amanda, klein, *toma, invertida, lapada*, guga, noblat, come through, live
7	**Economy and Fuel Price (3.5%)**	petrobras, price, gasoline, pf, seize, gas, reduction, tons, fuels, federal highway police (prf)
8	**Candidates (3.2%)**	candidate, candidates, presidency, candidacy, health, agenda, curses, covid-19, education, childish
9	**Health (2.4%)**	symptoms, cancer, know, hospital, disease, main, heart attack, treatment, signs, warning
10	**Political Debate (2.4%)**	debate, tv, criticize, band tv, knight, diego, globo tv, democracy, criticism, sbt tv
11	**Accident News (0.33%)**	death, dead, leaves, accident, found, dies, serious, deaths
12	**Pictures (1.8%)**	pictures, picture, images, body, globo tv, bikini, cameras, camera, happens, attention
13	**Money (1.8%)**	loan, aid, entrepreneurs, companies, payroll, beneficiaries, moraes, name, businessman, bank caixa
14	**Government Assistance (1.8%)**	family, families, scholarship, aid, receive, low, income, program, own
15	**Military (0.13%)**	military, military, police, defense, security, institutional security office, minister fachin, civil, organization, superior

Table 6.2: Discussion topics found in coordinated text messages. The topic terms are translated as the original in Brazilian Portuguese. The percentages in the labels represent the proportion of coordinated text messages for each topic.

that involves shared images, often featuring sexist themes (Topic 12). Videos are also popular, as seen in Topic 3, where many messages contain links to external websites hosting the videos. We also found health-related content that spreads tips on disease symptoms (Topic 9) and news about violence and accidents (Topic 11). As observed in domain analysis, many websites focus on increasing traffic and want to promote their content, often about curiosity or facts that intrigue people to know more, characteristics observed in these two identified topics.

The identified topics highlight the main discourses and narratives of the Brazilian political landscape during the period. WhatsApp plays a central role in Brazil's communication ecosystem, widely used for debates, gathering information, and tracking the repercussions of major events. Although WhatsApp is typically expected to be used to react and discuss real-world events, these coordinated actions suggest that, in some cases, it can be used as a strategy to organize, motivate, mobilize, and shape political narratives.

To better understand coordinated messages and their motivations, we focus on two key topics: the Supreme Federal Court (Topic 1) and Election Fraud (Topic 6). These topics were chosen because they were central to the Brazilian political discourse during the period covered by our dataset. The election is the most significant event, making these topics particularly relevant for analyzing how coordinated messages were used to influence the discussions. The Supreme Federal Court (Topic 1) became a focal point of political debates during the election, which was marked by widespread protests and many allegations of election fraud (Topic 6), making it a critical subject in public discourse.

6.4.2 Case Study 1

In this case, we identified a coordinated attack targeting the Brazilian Supreme Federal Court (STF), specifically aimed at doxxing the locations of the ministers. During the analyzed period captured by our dataset, the members of the Supreme Court became focal points of intense online discussions, which can be observed by Topic 1. To better understand this content, we analyzed the messages related to this topic and selected the most widely shared coordinated message about the ministers, which is shown as follows:

Message

"We have just discovered the hotel where the ministers of the Supreme Federal Court are staying in New York, please forward this to all Brazilians in the USA. xxxW xxth St, New York, NY xxxxx, United States" (translated and anonymized to not show address).

This message was shared 144 times within the entire dataset, with 29.2% of those shares coming from coordinated activity. The message reached 102 WhatsApp groups (7% of the total dataset), posted by 42 coordinated accounts.

Context. In November, following the Brazilian presidential election, there were tensions surrounding the decisions of the Supreme Court. When the ministers traveled to New York for a conference on November 13th, their hotel location was maliciously doxxed online, inciting an attack. This led to a flood of messages on WhatsApp, encouraging people to gather and confront the ministers.

Analysing the Impact. The dissemination of this message had a significant real-world impact. Protesters quickly mobilized to the location, gathering outside the hotel on the night of November 13. The ministers faced harassment and confrontations when entering and leaving the hotel.[9] The rapid spread of this information was crucial in organizing these protests, demonstrating how coordinated actions on WhatsApp can escalate from the digital ecosystem to a physical response. The incident highlights the power of doxxing, coordinated by some users, to endanger public figures by inciting hostile actions within hours.

6.4.3 Case Study 2

Here, we observed the Electoral Fraud (Topic 5). In this case, we analyzed the topic of Electoral Fraud. We searched for coordinated messages using the terms "fraud" and "ballot boxes". From the top three most relevant messages based on the total number of shares, we found the following message:

Message

"Our president said ALL PEACEFUL PROTESTS ARE WELCOME!!!! COME ON MY PEOPLE!! WE WILL NOT BACK DOWN! ALL THE RIGHT-WING IS GOING TO TAKE TO THE STREETS - THE ARMED FORCES ARE JUST WAITING TO REACH THE NUMBER TO HAVE THE NATIONAL AND INTERNATIONAL QUORUM THAT IS THE MASS OF THE POPULATION IN THE STREETS TO MEET THE DEMANDS OF THE PEOPLE" (translated).

[9] https://www.cnnbrasil.com.br/politica/manifestantes-hostilizam-ministros-do-stf-na-porta-de-h

This message was shared 83 times during the analyzed period, and 24% of these shares were in coordinated activities. It reached 74 different groups, and two coordinated accounts were involved in the coordinated actions of this message.

Context. After the election, former President Bolsonaro made his first public statement about the election. After that, messages like this one began to be shared, claiming that his pronouncement contained a subliminal message encouraging people to go to military posts and demand military intervention due to the alleged fraudulent election result.

Analysing the Impact. This coordinated message was widely shared after Bolsonaro's speech. After that, the protests intensified.[10] Many people took to the streets in front of military posts, demanding military intervention and alleging fraud in the polls. This coordinated message reinforced and motivated users to continue protesting and taking specific actions that had a real impact on society. This kind of message needs to be spread quickly, and the rapid coordinated actions work perfectly in this context, reaching more people quickly.

By examining these coordinated examples, we can reinforce that WhatsApp is an extremely politically relevant tool in Brazil, and coordinated activities can have a much greater influence, expanding discourse and reinforcing narratives. In our context, we observed that coordinated actions impacted orchestrating real-world events, such as protests and specific mobilizations. These coordinated actions aim to reach as many people as possible quickly, which is evident in both cases analyzed.

Takeaways. The main takeaways from this section are:

- The proposed topic analysis reveals that key Brazilian political events are highlighted in coordinated messages, particularly those that raise suspicions about electoral fraud and call for military intervention.
- We found evidence that the events discussed in the case studies (i.e., the mobilization of people against Supreme Court justices and protests over the election results) were also driven by coordinated accounts in WhatsApp groups.

[10] https://www.reuters.com/world/americas/bolsonaro-backers-call-brazil-military-intervene-after

6.5 Summary

This chapter provides valuable insights into the coordinated activities driving message propagation within WhatsApp. By examining 13M in public political groups from July 2022 to January 2023, we found a significant prevalence of coordinated accounts in disseminating messages on the platform. Our analysis reveals the presence of 1.5K coordinated accounts that work simultaneously to disseminate messages across multiple groups. These coordinated activities are focused on spreading news text messages that can easily shared across various groups. Our investigation showed that 26% of the links shared are from misinformation websites. This strategic news dissemination aims to engage audiences and promote specific political viewpoints. Furthermore, we observed that coordinated actions had a significant impact, as they were used to previously orchestrate protests and important political actions in the Brazilian political scenario.

Overall, this chapter sheds light on a frequent but little-explored phenomenon on WhatsApp. While the influence of misinformation and message apps on society is well recognized, the influence of coordinated activities is quite new. Our research reveals compelling evidence of coordinated efforts to disseminate misinformation on the platform and mobilize people to specific events. Importantly, even though we can not access the entire WhatsApp network, we identified many coordinated accounts that are working on spreading messages by public groups. This suggests that the problem is likely to be even larger than observed. Even with WhatsApp recognizing the existence of coordinated campaigns in the last Brazilian elections [99] and limiting forwarding per user to control virality [102], it was not enough to solve the problem, especially because coordinated accounts do not frequently use forwarding tool to spread their content. By observing the real impact employed by coordinated users, it is necessary to more notable strategies to mitigate the problem of controlling the influence of coordinated accounts. In 2018, WhatsApp already banned hundreds of thousands of accounts detected as spammers in Brazil.[11] Banning is a strategy that temporarily mitigates the problem, but it needs to be aligned with other control policies to keep the WhatsApp environment healthier. Even because new features were introduced facilitating massive spreading, such as increasing the number of participants per group and creating communities.

The methods to combat coordination misinformation should consider simultaneous posting patterns to mitigate coordination actions between multiple groups or accounts, since simultaneous posting activity is an important factor in the effectiveness of coordinated campaigns, such as protests or organized attacks. In this regard, effectively addressing coordinated misinformation is essential to foster collaboration between platforms

[11] https://wapo.st/3ZudkSD

and government authorities. This collaboration is particularly critical in high-impact contexts such as elections, where misinformation and coordinated accounts can directly and harmfully impact society. Increasing transparency from platforms is crucial, which should not only involve reporting on coordinated campaigns but also include measures to restrict the volume of messages during critical periods, improve content moderation algorithms, and ensure the detection and removal of harmful and inauthentic activity.

Chapter 7

Summary of Results and Next Steps

In this chapter, we provide an overview of the thesis, summarizing the key findings to date, and presenting the planned schedule to conclude this thesis.

7.1 General Outline

Given the open questions that guide this thesis, we have made partial progress in addressing the research goals presented in Chapter 1. In this section, we provide a general overview of the work completed so far, describing the methodology, and key findings, and outline the planned steps to finalize the thesis.

RG1 – Understanding attacks and hostile interactions in public groups.

In this research goal, we investigated the dynamics of WhatsApp groups and proposed a methodology that identified two distinct types of disruptive attacks. Particularly, while flooding attacks aim to disseminate many messages within a short period, hijacking attacks aim to take control of the group and wipe them out. After identifying the attacks, we analyze the occurrences and their impact. We identified that flooding attacks are not rare and groups are the recipients of multiple flooding attacks, even within the same day, which likely highlights the lack of effective tools that assist the group moderators. Subsequently, the messages used in these attacks were characterized. The analysis revealed a significant prevalence of stickers, as well as the presence of harmful content, including offensive, discriminatory, and violent material. This work contributes to understanding the negative aspects of WhatsApp group interactions, particularly hostile intergroup interactions across the political spectrum.

Publication: This work resulted in a published paper [74]:

- *Kansaon, D., de Freitas Melo, P., Zannettou, S., Feldmann, A., Benevenuto, F. (2024, May). Strategies and Attacks of Digital Militias in WhatsApp Political Groups. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 18, pp. 813-825).*

RG2 – Understanding stickers as a new form of spreading harmful content.

In this research goal, we explored how stickers have been appropriated as a mechanism for spreading harmful content within WhatsApp political groups. We proposed a methodology to detect sticker interactions and investigated their usage patterns. Our analysis revealed that stickers are not only widely adopted in political discourse but are also strategically used in coordinated attacks. In particular, we observed their role in flooding attacks, where stickers are employed to overwhelm conversations and disseminate offensive or misleading content in public groups, often without any form of moderation. Furthermore, we conducted a qualitative analysis of the most frequently shared stickers and identified the presence of abusive content, including offensive, provocative, and politically charged imagery. These findings demonstrate the structural uniqueness of sticker-based communication and reveal distinct usage patterns, including a darker side of sticker usage. Overall, our results show that stickers play a significant role in shaping political discourse on WhatsApp and underscore the importance of considering multimodal content in efforts to moderate harmful behavior on messaging platforms.

Publication: This work resulted in a published paper [34]:

- *de Freitas Melo, P., Kansaon, D., Couto, J. M., Reis, J. C., Benevenuto, F. (2025, June). A Sticker is Worth a Thousand Words: Characterizing the Use and Abuse of Stickers on WhatsApp Political Groups in Brazil. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 19, pp. 1210-1223).*

RG3 – Identifying and characterizing coordinated strategies employed for message spreading.

In this context, we proposed a rapid coordination network model designed to identify coordinated efforts that enable the quick spread of messages. The first step in this process is to detect coordinated users. To achieve this, we model all message interactions between groups and observe users who share similar messages at the same time. We analyzed 13M in public political groups from July 2022 to January 2023. Our findings revealed a significant prevalence of coordinated accounts in disseminating messages on the platform. Specifically, we identified 1.5K coordinated accounts that work simultaneously to disseminate messages across multiple groups. Our analysis showed that 26% of the links shared are from misinformation websites. Furthermore, we applied the BERTopic strategy to extract the topics of coordinated messages. We observed that coordinated messages addressed specific relevant political topics and were used to orchestrate protests and important political actions in the Brazilian political scenario.

Publication: This work resulted in a published paper [73]:

- *Kansaon, D., de Freitas Melo, P., Zannettou, S., Benevenuto, F. (2025, June). From Fake News to Real Protests: WhatsApp's Role in Brazilian Political Coordi-*

Table 7.1: Planned schedule for the conclusion of the project

	Month						
Activity	**Sep 25**	**Oct 25**	**Nov 25**	**Dec 25**	**Jan 25**	**Feb 25**	**Mar 25**
Create a dataset labeled with harmful text	•	•					
Qualitative and quantitative content analysis		•	•	•			
Survey of state-of-the-art approaches		•	•	•	•	•	
Thesis writing and refinement		•	•	•	•	•	
Final defense and submission							•

nation. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 19, pp. 1007-1020).

RG4 – Identifying subtle and harmful text-based discourse.

This research objective is still ongoing, and we are working to achieve significant progress. By the end of the thesis, we hope to better understand the WhatsApp political text message dataset, seeking to uncover recurring linguistic and narrative patterns and assess their role in the broader dynamics of abusive and manipulative discourse on the platform. Our focus is to analyze messages shared in groups to identify harmful textual content. Here, we concentrate on developing methods to identify linguistic and narrative patterns of harmful text. Our initial efforts have focused on analyzing stickers, revealing instances of harmful material such as Nazi, racist, and various forms of abusive content. Currently, we are shifting our focus to text-based content, specifically aiming to identify those that are particularly prevalent in political discussions.

7.2 Planned Scheduled

Table 7.1 presents the timeline for the final phase of this thesis. The planned activities include: (i) the construction of a labeled dataset with harmful text; (ii) qualitative and quantitative content analysis of the harmful messages; and (iii) the development of a systematic survey aimed at mapping the research area, consolidating the current state of the art, and identifying existing research gaps. Although many studies have addressed related topics, no comprehensive effort has been made to map these contributions and analyze their thematic scope. This survey will be conducted throughout the remainder of the thesis and will be incorporated into the related works section.