CENTRE FOR
STRATEGIC AND
INTERNATIONAL
STUDIES

RESEARCH REPORT

CYBERTROOPS AND PUBLIC OPINION MANIPULATION THROUGH SOCIAL MEDIA IN INDONESIA

Wijayanto & Ward Berenschot

CYBERTROOPS AND PUBLIC OPINION MANIPULATION THROUGH SOCIAL MEDIA IN INDONESIA

CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES

A Research Report by CSIS Indonesia

Wijayanto
Ward Berenschot

The CSIS Research Report is a means by which members of the Centre for Strategic and International Studies (CSIS) research community can quickly disseminate their research findings and encourage exchanges of ideas.

The author(s) welcome comments on the present form of this Research Report. The views expressed here are those of the author(s) and are not intended to be attributed to CSIS Indonesia

© 2024 CSIS Indonesia
All rights reserved

Cybertroops and Public Opinion Manipulation through Social Media in Indonesia

Wijayanto[1], Ward Berenschot[2]

Editor: Ross Tapsell[3]

I. Introduction

Social media were once considered a boon for democracy. That enthusiasm has faded. A growing body of research is showing that social media are increasingly being used to hamper public debate and influence election outcomes. A recent overview-study has shown that cyber troops and public opinion manipulation is taking place in at least 82 countries in the world, including among others: European countries like United Kingdom, Sweden, the Netherlands and Russia, Asian countries like China, Thailand and Indonesia, as well as the United States (Bradshaw, Bailey, and Howard, 2020). While this phenomenon is referred to with different terms – from 'organized social media manipulation', 'networked disinformation' and 'digital disinformation' to 'underground campaigning' and 'disinformation campaign production'[4] – the commonality among observers is a considerable concern about the ways in which paid social media campaigns are not just distorting public debate but also weakening democracy.

Indonesia has emerged as a prime example of how social media can be used to manipulate public opinion and, in doing so, affect democratic processes. A small but growing number of studies have been documenting how paid social media operations have been 'engineering consent'. This has involved spreading disinformation and slander during election campaigns[5], the harassment of dissident voices and opposition politicians[6], as well as influence operations to generate support for government policies[7]. These studies suggest that Indonesia's political and economic elites are increasingly willing to fund social media campaigns to bend public opinion in their favour.

What is the character of these campaigns that use social media to manipulate public opinion? How are these campaigns organized, who is behind them, and how should Indonesia's government and civil society address the threats posed by these campaigns? These are the questions this report addresses. Combining a computational analysis of public debates on twitter with material from interviews with 52 individuals involved in these campaigns executed between January and

[1] Diponegoro University
[2] University of Amsterdam
[3] Australian National University

[4] The following studies employ these different terms to describe public opinion manipulation through social media: Howard and Bradshaw, 2017; 2019; Ong and Cabanes, 2018; Cabañes, 2020); Tapsell, 2020; Ong and Tapsell, 2022; Sastramidjaja and Wijayanto; 2022.

[5] On influence operations and election campaigns, see Rakhmani and Saraswati 2021 and Tapsell 2020

[6] On 'cyber terror', see Wijayanto, Suwana and Sardini 2022

[7] For example, on the role of social media campaigns to generate support for its attempt to curtail Indonesia's anti-corruption commission, see Wijayanto, Suwana and Sardini 2022.

December 2021, this report dives into the organization, everyday functioning and financing of the networks engaged in these social media campaigns. We all these networks 'cybertroops', which we define as networks of secretly paid actors using mostly anonymous social media accounts to engage in coordinated public opinion manipulation[8].

We argue in this report that the emergence of 'cybertroops' constitutes a threat to Indonesia's already embattled[9] democracy, as cyber troops undermine public debate, weaken oppositional forces and further deepen the dominance of economic elites. We show that – with some exceptions – cybertroopers operate as online mercenary in the sense that they are willing to be hired by wealthy actors for a wide range of online campaigns. In this way the emergence of cyber troops has provided Indonesia's economic elites with yet another instrument to cement their political and economic power.

This report on the involvement of cyber troops in public opinion manipulation in Indonesia has three main parts. After a brief discussion of our methods, we start by employing our computational analysis of twitter debates to discuss indications of involvement of cyber troops in Twitter debates about three issues: the presidential election of 2019, the revision on the law on Indonesian anti-corruption body 2019, and the controversial omnibus law of 2020. In the second part we employ our interview material to provide insights into the organization, financing and everyday functioning of the cyber troops behind these campaigns. In the third and final part of the report we provide our recommendations for dealing with the threats posed by cyber troops to Indonesia's democracy. Among other things we argue for more thorough efforts to ban fake accounts, media literacy classes in schools, and we propose that Indonesia's politicians embrace a code regarding online ethics.

II. Research Method

To write this report, we have made use of an interdisciplinary and mixed-method research project in which the authors participate[10]. Employing material generated by this project, we combine social media analysis and in-depth interview with 52 informants. The social media analysis is conducted to identify the ongoing social media propaganda as well as suspicious accounts involved as cyber troops. We employed Drone Emprit Academy system (discussed below) to analyse twitter debates. Our analysis of this material focused on three indicators of manipulation of online communications through social media: (1) the sudden emergence of a particular (trending) narrative; (2) the dissemination of a variation of photos, memes and videos accompanied by a very similar narrative; and (3) the lack of followers and/or other interactions on social media of the accounts spreading those pictures, memes and videos. This propaganda often involves fake robot alias accounts. To identify such robot accounts, we use botometer. This is a software application that analyses their online behavior, in particular on Twitter. This assessment

[8] For a more elaborate discussion on this definition, see Wijayanto et al. forthcoming.
[9] Indonesia's democratic decline is a recurring topic in recent political analysis, see for example Power 2018, Wijayanto et al 2019, Power and Waburton, 2020; Wijayanto et al 2021.
[10] See https://www.kitlv.nl/cyber-troops-and-computational-propaganda-in-southeast-asia/

is based on the fact that humans usually post various tweets in a random time span, whereas robots post similar tweets in a patterned time span. In this regard, we first investigated the cluster of conversation around the aforementioned topic.

For the analysis in the first part of the report, we employed Drone Emprit's Academic system. This is a big data system that enables the capturing and monitoring of social media conversations as well as news sites. The Drone Emprit Academy system employs the Twitter's application program interface (API) to collect conversations in real time. Employing search terms associated with the public debates we were tracing – related to the presential elections, the KPK revision law and the Omnibus law - we mined hundred of thousands of tweets. We subsequently analyse these posts by a. using retweets to map the social networks involving online conversations and then b. manually identified suspicious accounts based on the three criteria outlined above – participation in sudden dissemination of a particular narrative, sharing of content similar to other accounts and a lack of meaningful interaction with other accounts. In this way we identified accounts likely employed by cybertroopers.

To test whether or not those suspicious accounts were cybertroopers, we worked with a team of researchers, consisting 5 fieldworkers, of which three were ex-cybertroopers who themselves were familiar with cyber troops and had some prior knowledge about the accounts. This started when one of the authors (Wijayanto) of this report recruited a colleague researcher for the field research who happened to have been an active cybertrooper. Through this first recruit, Wijayanto was able to use his social network to draw other (ex) cybertroopers into the research project. After receiving elaborate training and employing elaborate interview templates these researchers set out to contact and interview the cybertroopers we identified through the above-mentioned social network analysis of twitter postings. Thanks to their good connections, they succeeded in interviewing 52 cybertroopers - 23 buzzers, 22 influencers, 2 content creators and 5 coordinators. This research was executed between January and December 2021. Some of our findings have first been published in a special issue of Inside Indonesia[11].

III. Cases and Patterns of Online Cybertroops Campaigns

What forms does this public opinion manipulation through social media take? In this section we will employ the above-mentioned social network analysis of twitter posts through Drone Emprit Academic to examine three instances of cybertroops involvement in online public debates: the presidential election of 2019, revision on the law on Indonesian anti corruption body 2019, and the debates surround the adoption of the omnibus law in 2020.

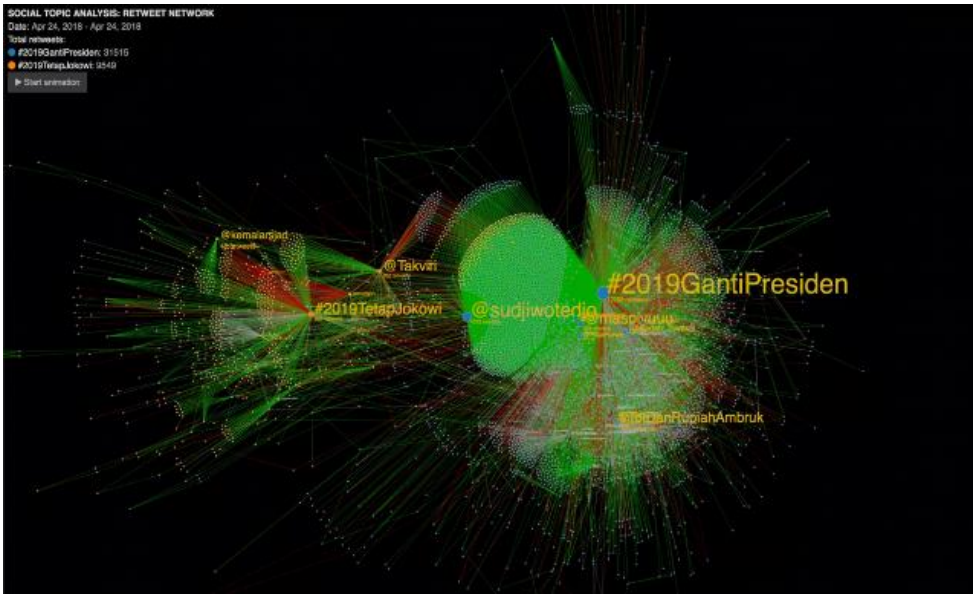
The 2019 Presidential Elections

In the 2019 election, incumbent President Joko Widodo competed with Prabowo Subianto for the second time. On social media a 'war of hashtags' erupted, with the two camps pushing hashtags

[11] https://www.insideindonesia.org/editions/edition-146-oct-dec-2021/the-threat-of-cyber-troops

like #2019GantiPresiden (2019ChangethePresident) vs #2019TetapJokowi (2109StayWithJokowi). Through analyzing the conversation in social media, the retweet activity can be visualized in the following manner:

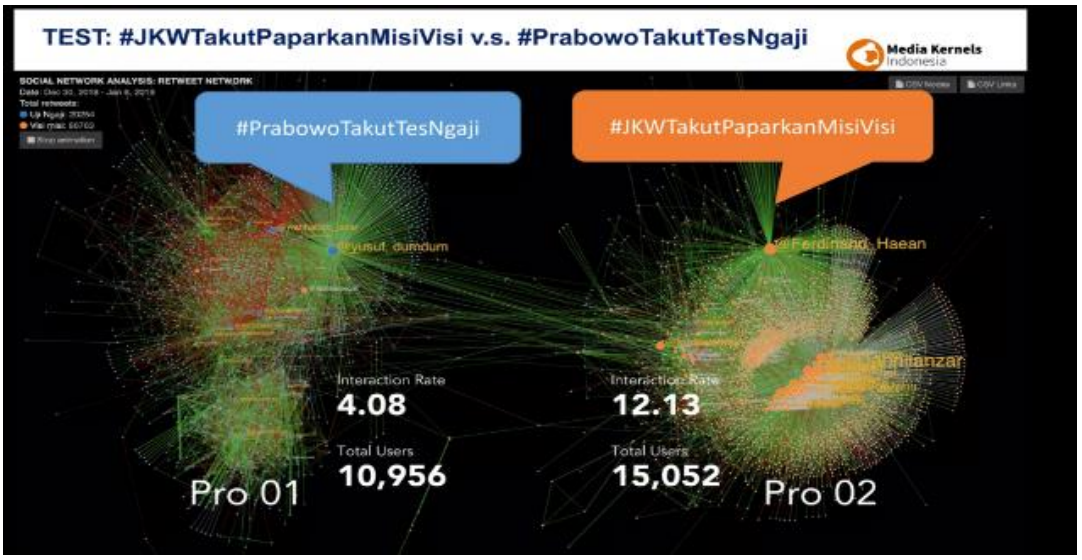
Figure 1 #2019GantiPresiden vs #2019TetapJokowi



Source: Drone Emprit, 8 May 2018

The above picture – where one 'dot' represents a Twitter user. The green color signifies the positive sentiment while the red signifies negative sentiment - visualizes how thousands of accounts used various hashtags to both oppose and support President Jokowi's bid for a second term.

Figure 2 #JKWTakutPaparkanVisiMisi vs #PrabowoTakutTesNgaji

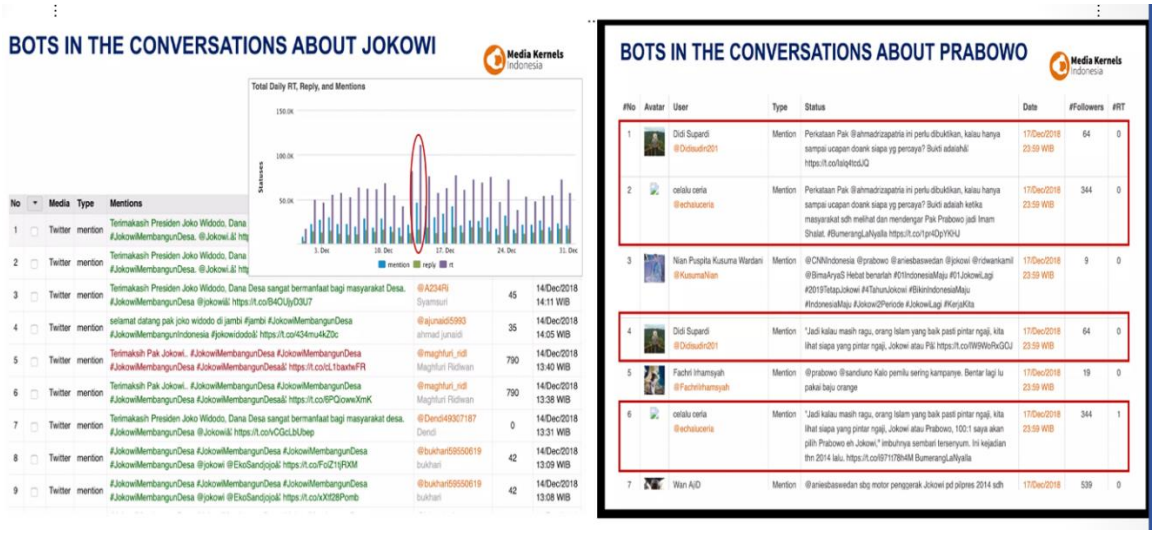


Source: Drone Emprit, 6 January 2019

From the picture above, we can see in the hashtag #JkwTakutPaparkanVisiMisi (Jokowi fears to share his vision and mission) that this hashtag dominated discussion, while for Prabowo and the hashtag #PrabowoTakutTesNgaji (Prabowo fears to perform reading Qur'an test) also dominated the Twittersphere on [State date].

What interesting was that the further investigation found that both hashtags involved bots accounts in its spread as can be seen in the following picture:

Figure 3



Source: Drone Emprit, 6 January 2019

The picture above is the result of accounts detection using botometer i.e. a web based program to used to measure how likely a Twitter account is a bot account. This assessment uses machine learning to classify twitter account as bot or human by looking at features of profile including friends, social network structure, temporal activities, language and sentiments. It is based on the fact that humans usually post various tweets in a random time span, have various friends and networks of followers, and are able to generate organic content. On the contrary, robots post similar tweets in a patterned time span, have no followers, and, in many case, only re-twit posts of other account or simply sharing journalism content without giving any comment[12]. These results

[12] Chen, C. F., Shi, W., Yang, J., & Fu, H. H. (2021). Social bots' role in climate change discussion on Twitter: Measuring standpoints, topics, and interaction strategies. *Advances in Climate Change Research*, 12(6), 913-923.

of the botometer software suggests that automated (bot) accounts were used to push the attacks on both candidate, which helped to make these hashtags go viral and gain public attention.

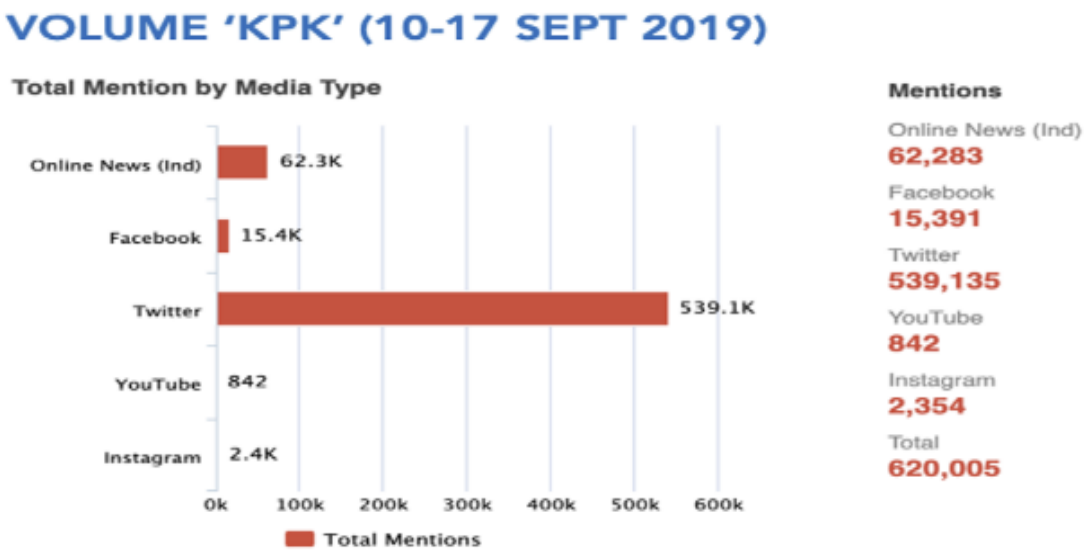
The KPK revision bill

The second case we analyzed concerned the bill on revising the law on corruption eradication commission (KPK) on September 17, 2019. This revision – which considerably weakened the independence and hence effectiveness of the KPK – immediately sparked public criticism, partly because the house of representatives spend little time discussing the bill. It was reported that the discussion took only 20 minutes, after which the legislative members to agreed to put the bill up for a vote.

This decision immediately sparked protest from many sides including civil society organisations, academics, students and even KPK members themselves, who expressed their concerns that the bill would weaken the anti-corruption body.

After news about this bill spread, it generated intense discussion on social media. However, this wave of conversations occurred only one week before the KPK Bill's ratification on September 17, 2019. The listening tool of Drone Emprit found that there was an unnatural spike in the number of tweets in the days leading up to the ratification of the revision of the KPK Law, reaching more than half-million tweets in just seven days. The sudden emergence of conversations about KPK can be seen in the Figure 4 below:

Figure 4

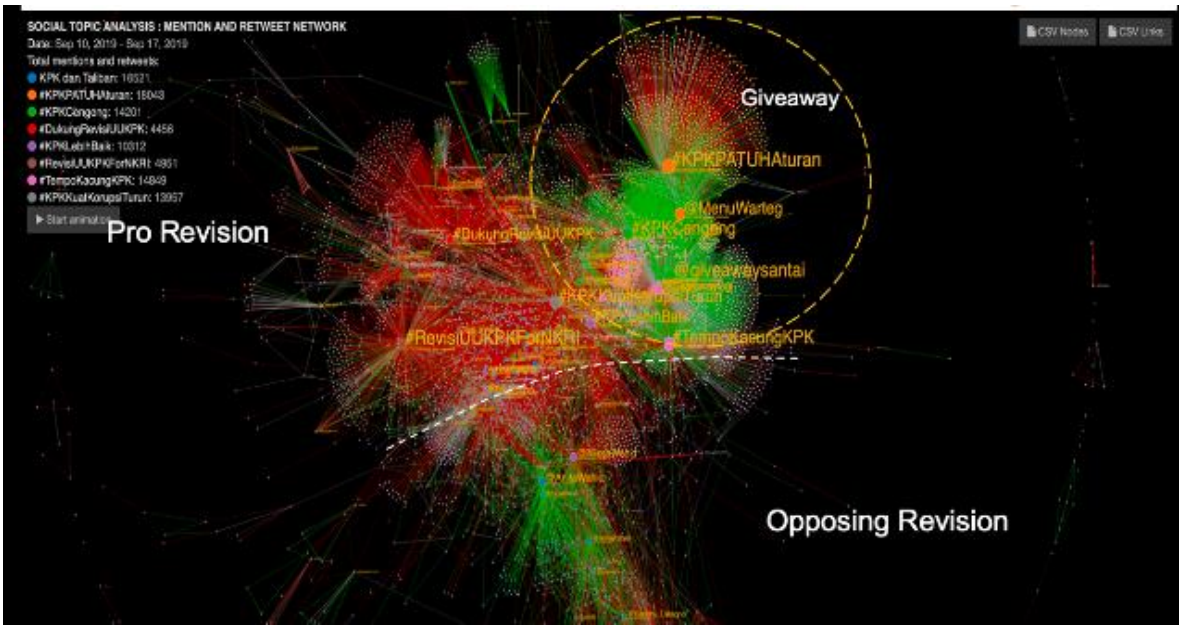


Source: Drone Emprit, 17 September 2019

The graph in Figure 4 shows that an enormous volume of conversations occurred on Twitter with more than 539,135 conversations. A volume of this size for one topic is not a frequent occurrence.

The conversation contained those who were pros and cons of the revision of the bill recorded in our SNA as follows:

Figure 5. Social Network Analysis (SNA) about revision of KPK law



Source: Drone Emprit, 17 September 2019

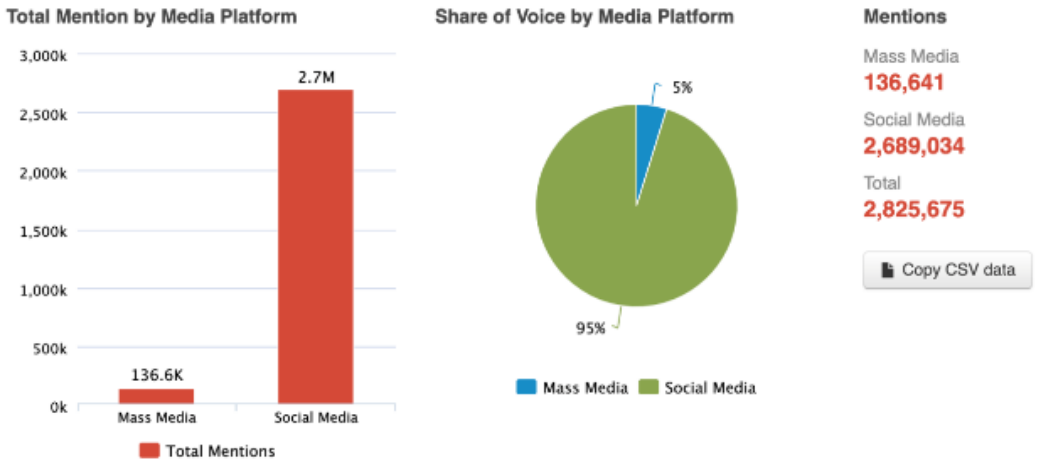
Figure 5 shows a visualisation of the social network analysis (SNA) of netizens who agree and reject the KPK Law revision. It can be seen in the visualization above that between 10 and 17 September 2019 the conversation turned out to be dominated by accounts agreeing to the revision of the KPK Law in the top picture, either in the form of a tweet or re-tweet, displaying various hashtags including: #KPK and Taliban, #KPKPATUHAturan, #KPKCengeng, #DukungRevisiUUKPK, #KPKLebihBaik, #RevisiUUKPKForNKRI, #TempoKacungKPK and #KPKKuatKorupsiTurun. Meanwhile, the accounts that rejected the revision appeared much less regularly.

Omnibus Law

The third illustration of a campaign concerns the passing of the Omnibus Law on October 5, 2020. The law generated much opposition, also online. This opposition gained momentum on October 3 when the Omnibus Law was first discussed in parliament. And while a range of civil society organisations rejected the Omnibus Law, the parliament actually accelerated the deliberations by cutting short the debate with three days and ratified the law on October 5.

This opposition to the Omnibus law was also very active on social media. From 1 to 16 October 2020, digital discussions related to the Omnibus Law and the Job Creation Law reached millions of interactions, dominated by social media with 2,689,034 digital interactions as in the image below:

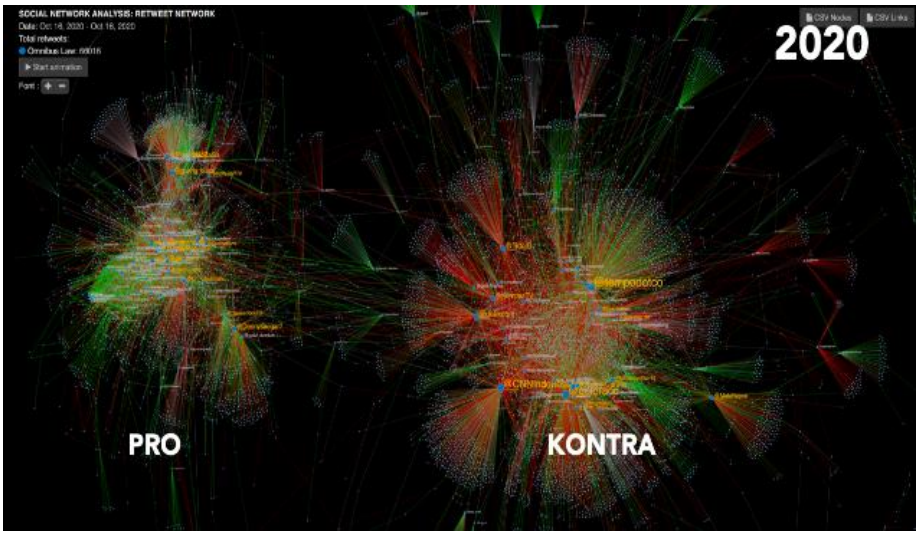
Figure 6. The volume of conversation on Omnibus Law



Source: Drone Emprit, 17 September 2019

Figure 6 above shows the interaction in digital media regarding Omnibus Law and Job Creation Law from 1 until 16 October 2020. There are more than 2,8 million conversations about Omnibus Law; more than 2,6 million out of that number occurred in social media. That condition means the volume of interaction is enormous. Those massive interactions consist of accounts that reject the Omnibus Law and also the supporter of that new regulation, as we can see on SNA below:

Figure 7. Social Network analysis on Omnibus Law



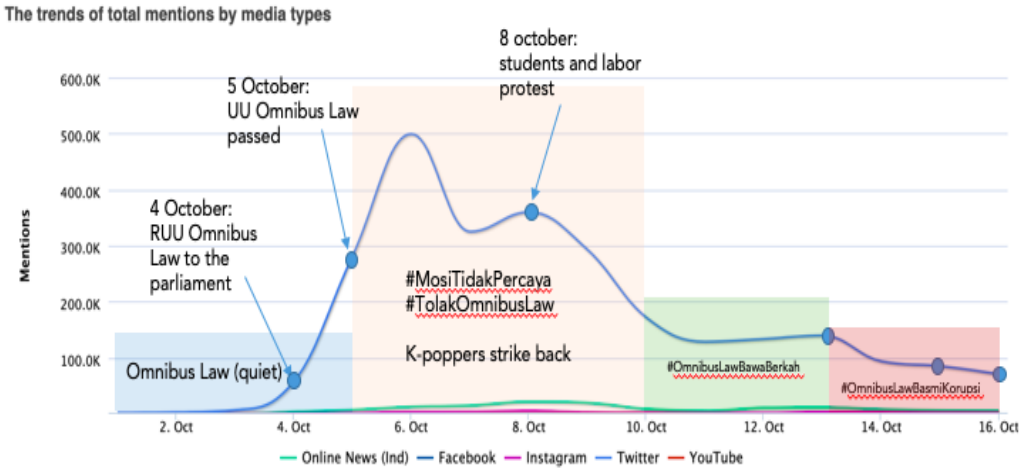
Source: Drone Emprit, 17 October 2019

Figure 7 is an SNA view of the tweet on October 16th. The data suggests that the actual volume of the critical tweets still outweighs the tweets supporting the law. We can also see from the SNA

above that the interactions between those who are contra are much more natural than those who are pro who seems to talk among themselves. The media kernels listening tool found several critical activists, such as Andreas Harsono, Laode M Syarif, Susi Pudji Astuti, Ridwan Kamil, Agus Yudhoyono, Rangga Widigda, PUKAT UGM, Said Didu, Hidayat Nur Wahid, Tifatul Sembiring and Green Peace. They interacted with each other and mingled dynamically with various mainstream media accounts: CNN Indonesia, Tempo.co, Tirto.id, detik.com, Matanajwa and KompasTV.

However, gradually the voices supporting the Omnibus law drowned out these critics. While the online debate was initially dominated by the critics, over time the accounts supporting the bill gained the upper hand, as shown in Figure 8.

Figure 8. The flow of narrative on omnibus bill



Source: Drone Emprit, 17 October 2019

As shown in the figure above, in the week after the ratification of the law on 5 October, the dominant narratives involved critical hashtags such as #MosiTidakPbelaya and #TolakOminbusLaw. At this time the accounts rejecting this omnibus law called themselves the K-poppers generation, and they named their movement 'K-poppers strike back'. At the same time, students and workers also held a movement against the omnibus law. As seen in the chart above, this online activity peaked on October 6, reaching a volume of up to half a million tweets. Yet after October 10, the narrative changed to #OmnibusLawBawaBerkah or 'omnibus law brings a blessing', involving between one hundred and hundred fifty thousand conversations in the week before October 14.

On October 16, within observed dataset collected from Twitter, our analysis of twitter posts show that the most trending hashtags are already supportive of the omnibus law, as shown in the figure below:

Figure 9. Popular hashtags on Omnibus Law bill

Source: Drone Emprit, 17 October 2019

From the figure above, we can see that the top 5 hashtags in the sequence include: #OmnibusLawBasmiKorupsi (Omnibus law eradicate corruption) with 8067 tweets, #KepalaDaerahSocialisasiUUCiptaker (regional head socialise the Ciptaker law -another acronym of Omnibus Law) with 3489 tweets, #UUCiptakerjauh people needs the Ciptaker law) with 3489 tweets, #OmnibusLawUntungBuruh (omnibus law favourable for workers) with 1512 tweets, #OmnibusLaw with 1448 tweets. Of the five hashtags, four of them support the omnibus law, and the other is neutral. There is not a single hashtag that rejects omnibus law in the top five. We only find it in seventh place with the hashtag #MosiTidakPercaya (do not trust-the government) with only 558 tweets.

These cases of cybertroops activity illustrate a number of important characteristics for online public opinion manipulation in Indonesia:

First, there is a tsunami of conversations on social media ahead of the ratification of a policy with an unusually large volume. Our research monitoring shows that ahead of the 2019 presidential election there were tens of thousands of conversations tagged #2019GantiPresiden against #2019TetapJokowi. During 2020 there were millions of conversations regarding the omnibus law. Next, between 10-17 September 2019 there were more than half a million conversations on various social media platforms, especially Twitter about the revision of the KPK Law. Half a million conversations on one topic in such a short amount of time is certainly not something commonplace. The tsunami of conversation was about one issue that was quite serious: the revision of the law. This is different, for example, from cases involving artists who are relatively followed by various layers of society.

Second, there is an intentional effort to create content on social media accompanied by massive dissemination so that it becomes a trending topic. As explained above, ahead of the 2019 election, two hashtags were trending: #2019GantiPresiden and #2019TetapJokowi. In the case of the revision of the KPK Law, efforts to make the hashtag viral were even carried out in other unreasonable ways, such as the "GiveAway" quiz where virtual citizens will get 50 thousand credits for 2 people who want to make any status but with the hashtag #KPKPATUHAruran. This is intended to put pressure on the KPK whose commissioners rejected the revisions to comply with the existing revisions. In this case the quiz proved to be successful because the hashtag #KPKPATUHOrgan was tweeted 18,043 times.

Third, cyber troops appeal to social identities to spread their messages. The 2014 election saw sharp political polarization in Indonesia. On social media, polarization led a dehumanization of people holding opposing views, as they were referred to as *cebong*, *kampret* and *kadrun*.

In the case of the revision of the KPK Law, identity politics was also used. One of the posts that went viral at the time was still fresh in our minds, was a picture of the organizational structure which explained how some investigators and commissioners of the Corruption Eradication Commission were related to the Taliban organization. Such sophisticated images certainly require experts to produce them. On those days, Twitter was also filled with hashtags saying #KPK and the Taliban. Our research monitoring shows that there are 16,521 tweets using that hashtag. The goal is clear to sway public opinion as if the KPK were a nest of radical Islamic groups which has never been proven to this day.

From the various patterns above, it seems that the use of identity issues is a powerful tool to influencing public opinion. Ong and Cabanes (2020) note that social media propaganda will be able to influence public opinion when it resonates with social issues and aspirations of the community, especially those that are not sufficiently acknowledged and mentioned by the mainstream media. The descriptions of these two scholars are relevant to the Indonesian situation where political elites have used sentiments based on religious identity in three elections: the 2014 election, the 2017 DKI governor election and the 2019 election which have successfully spawned political polarization. For at least the last five years, various political scientists have given warnings about the threat of this political polarization. Identity-based political polarization can have a number of negative effects on democratic governance, including the erosion of democratic institutions and norms, as well as deepening social divisions.

As can be seen in the explanation above, in Indonesia this identity-based political polarization has also spawned divisions on social media in pejorative terms: *Cebong* and *Kampret,* and later also *Kadrun*. If *cebong* refers to groups that support the government, then *kampret* or *kadrun* refer to hard-line Islamic groups who are always suspicious of anything the government does. In a situation of affective political polarization, politics is no longer just a struggle for power but also emotions and desires to fulfill the ego and even survival. The pejorative labeling using animal names that takes place in Indonesia shows the truth of this theory. Here, the division between us (us) and them (them) reaches a very extreme point. In these circumstances, the judgment of right or wrong is no longer about facts or evidence but more about whether it is postulated by our group or theirs.

This helps to understand why the propaganda for the existence of the Taliban or hard-line Islamic groups within the KPK was successful. It seems that the KPK and Taliban hashtags succeeded because the mainstream media started to report on the online posts in more than 250 articles, which greatly amplified the reach of the influence campaign. Moreover, there are indications that the campaign succeeded in influencing public sentiment in general. A survey published in the Kompas daily on September 16 2019 found that the majority of the public (44.9%) supported the revision of the KPK Law, while 39,9% opposed the law.[13] - while in earlier years trust in the KPK was very high[14]. In these earlier years, any attempt to weaken the KPK was met with public opposition[15]. In short, this public opinion survey suggests that, indeed, cyber troops activity contributed to changing public opinion on the KPK.

IV. Organisation and Coordination of Cybertroops

Having discussed these three examples of cyber troops campaigns, how do cyber troops actually execute such campaigns? Our conversations with individuals involved in cybertroop campaigns suggest that these online groups possess great adaptability. Typically, people collaborate on a project basis for specific campaigns, often in a freelance capacity. Despite this limited formal structure, these networks demonstrate extensive collaboration and a division of responsibilities. Our findings reveal that these influence endeavours are not only executed by individuals known as "buzzers", but also involve others who fulfil different roles, with coordinators, content creators, and influencers being the most significant ones. We will now delve into the various roles played by these participants within cyber groups.

The lowest and most numerous layer within of cyber troops consists of anonymous account handlers, to whom we refer to as buzzers. Their primary responsibility, involving numerous social media accounts, is to widely circulate content and viewpoints. This entails sharing specific content received from their coordinators. However, buzzers also enjoy substantial autonomy to retweet and comment on others' posts. Some buzzers even participate in attacking or 'trolling' individuals, aiming to stifle contrary viewpoints or inundate them.

To execute these tasks, a typical buzzer generally employs anywhere from 10 to 300 accounts, according to the buzzers we interviewed. The cultivation of these accounts constitutes a significant dimension in the buzzers' 'career progression'. Acquiring these accounts necessitates a phone number, which clarifies why buzzers not only manage multiple phones but also require a substantial quantity of SIM cards. The process of gradually amassing followers is crucial: buzzers

[13] Kompas, 16 September 2019
[14] Based on the survey by Indikator Politik, for instance, it was found that in 2018 84.8% public trusted KPK.
[15] It can be found, for instance, in the study of Merlyna Lim, "Many Clicks but Little Sticks: Social Media Activism in Indonesia", *Journal of Contemporary Asia 43*, no. 4 (2013): 636–657; Fiona Suwana, "What Motivates Digital Activism? The Case of the Save KPK Movement In Indonesia", *Information, Communication & Society 23*, no. 9 (2019): 1295–1310; Ahmad Khoirul Umam, Gillian Whitehouse, Brian Head, and Mohammed Adil Khan, "Addressing Corruption in Post-Soeharto Indonesia: The Role of the Corruption Eradication Commission", *Journal of Contemporary Asia 50*, no. 1 (2020): 125–143.

must cultivate numerous accounts that have a considerable following to attract potential clients seeking their services. A buzzer with an array of accounts boasting a substantial number of followers can usually command higher compensation for their services. This pattern of initially nurturing accounts and subsequently employing them for influence campaigns is occasionally evident on Twitter: certain accounts may share celebrity news for months, then abruptly transition to posting regularly about political subjects.

Buzzers tend to link their diverse accounts in a partially automated fashion. Our sources mentioned the presence of a 'leading account' (referred to as the "akun general") alongside 'troop accounts' (known as the "akun prajurit"). The leading account is utilized to publish specific content, which is subsequently retweeted by the troop accounts, often using software like Tweetdeck. The intention behind these tactics is to produce a substantial volume of posts centered around a particular hashtag or topic. This approach aims to amplify further dissemination by causing the hashtag or topic to trend on Twitter. One of our sources described (and took pride in) this approach in the following manner: "[you need] speed in posting. (...) In the end, even if the volume [of tweets] is small, but the speed is good, it can go straight to the top [of trending topics [?) (...)And that matters, right? If a hashtag is trending in the world, it is read by the world. If it is trending in Indonesia, all Indonesians will read it, right? Because that is how Twitter works" (interview with buzzer, 25 Maret 2021)

Buzzers generally obtain the content for these posts from individuals that we call "content creators". These content creators are tasked with crafting specific memes, hashtags, images, and textual content that convey the message(s) of the influence campaign. They undertake this role based on guidelines from coordinators, yet they also appear to possess a certain degree of autonomy in generating content that is engaging and visually captivating. Their substantial ability to generate such captivating content offers a distinct way of recognizing the endeavours of cyber troops on Twitter: whereas regular users often express their viewpoints without images or with hastily edited visuals, the posts propagated by buzzers can feature highly appealing visuals. In some of our interviews content creators appeared to think very strategically about how to craft formulating effective posts and hashtags. One content creator, for example, said that "[It is important to] [speaking softly] feel and understand the emotions of people. (...) I make up these hashtags on my own [according to] my principle. The hashtag must have a philosophical value [pauses] [and depending on] what is the target, what [message] has to be accepted by society. If the hashtag does not match [with society] I will not use it. But if the hashtag is appropriate, I will make it big" (interview with a content creator with a large amount of followers, 21 February 2021).

The efforts of both buzzers and content creators are overseen by a third category of participants within cyber troops, the "coordinators". These individuals, often experienced buzzers, undertake the task of planning and guiding influence campaigns. They make decisions regarding the content of the influence campaign, the content of posts, the selection of hashtags, and they manage the coordination of buzzer activities. A coordinator distributes the memes or texts produced by content creators to the buzzers, while also synchronizing the timing of posts. In certain cases, coordinators strive to ensure that all buzzers post around the same time using a designated hashtag, thereby aiming to optimize the potential for generating a trending topic. One coordinator we interviewed described this potential as follows: "It is very important that this posting is done

collectively (*bersamaan*). It should not happen that someone starts early or too late, because that could endanger their capacity to raise this hashtag to become trending topic (Interview with a coordinator, 18 June 2021).

The coordinator also serves as the point of contact with the client. Although our interview data is limited in this area, it appears that cybertroops campaigns are typically established after clients approach these coordinators with assignments and provide the necessary funding for executing the campaign. Throughout the campaign, the coordinator and the client may maintain regular communication to address strategic aspects, such as the selection of narratives promoted by the cyber troops.

A fourth category of participants engaged in cybertrooper campaigns concerns influencers. Unlike buzzers, these individuals operate on social media using their real identities. They often enjoy recognition as celebrities, prominent figures in society, or simply as well-known online personalities, thus having a relatively extensive follower base. Our conversations with buzzers suggest that due to their substantial social media following, coordinators of cyber troops frequently seek to engage influencers in their campaigns. For instance, they might offer influencers compensation in exchange for posting viewpoints that align with the promoted narrative. Subsequently, as buzzers intensify their efforts to disseminate such posts, collaboration with an influencer can prove to be highly impactful. In interviews, buzzers indicated that they are asked to retweet or quote posts from specific influencers and, as one of them said during an interview, “we do not interact directly with the influencers behind the scenes [but] we are told that they are our influencers” (Interview, 24 April 2021).

What our interview material shows, in other words, is that these social media campaigns involve considerable collaboration and coordination between various individuals, involving different roles and tasks.

V. Funding of Cybertroops

The manipulation of public opinion appears to be evolving into a substantial industry that provides a source of livelihood for a significant number of people. Some informants estimated that Jakarta alone housing 'thousands' of people engaged in this work. While some buzzers acknowledged being driven by political preferences, particularly support for specific candidates, the majority of those we interviewed were transparent about their primary motivation being the income generated. This emerging industry seems to offer relatively attractive remuneration, which varies considerably based on the aforementioned roles within cyber troops.

For most buzzers, compensation is tied to the number of accounts they utilize for a given campaign. As an exception, one buzzer mentioned earning 250 thousand rupiah per account. However, since they operated only ten accounts, they earned 2.5 million rupiah per month (approximately 160 dollars). Another informant revealed receiving between 50 and 100 thousand rupiah per account, resulting in around 3 million per month from managing 35 accounts.

Other members of cyber troops receive payment per campaign rather than per account. A content creator we interviewed mentioned earning four million rupiah per month. Coordinators seem to earn more. One coordinator stated that they were paid based on the accounts they could recruit for the campaign, including those managed by the buzzers under them. Another coordinator mentioned receiving a total of 190 million rupiah (about 12,500 dollars) for supporting a politician during a four-month election project. This coordinator hired six people with this money.

However, the most significant earnings are garnered by influencers who agree to endorse a policy or politician through a few social media posts. While influencers usually keep these arrangements confidential, including the financial aspects, we did manage to interview a journalist influencer who supported a presidential candidate in exchange for 20 million rupiah (around 1300 dollars). As such endorsements demand minimal effort and influencers can endorse multiple campaigns, it follows that certain influencers are amassing considerable income from their involvement in cybertroops activities. Interestingly, influencers appear to yield benefits beyond financial gains. We encountered two influencers, Gesiz Chalifah and Hasreza, who were reportedly appointed as commissioners at state enterprises by Governor Anies Baswedan after apparently supporting his election campaign. While the monthly earnings of buzzers may appear relatively modest, these individual sums do add up to considerable expenses. So who provides the financial support for these cybertroops campaigns? Most of our interviewees lacked precise knowledge in this regard, often relying on hearsay from others. Some coordinators we interviewed, who were in direct contact with clients, were hesitant to reveal the identities of those who hired them. Given these limitations, the insights we glean from our interviews remain somewhat speculative.

With this disclaimer in mind, these comments from interviewed buzzers and coordinators suggests that the clients of cyber troops are quite diverse. Through conversations with buzzers and coordinators, we identified four distinct categories of clients. Firstly, it does appear that certain cybertroops activities are sometimes financed by the Indonesian government or individuals closely affiliated with government ministers. An informant engaged in a campaign promoting the aforementioned omnibus law revealed being compensated by someone linked to Airlangga Hartarto, the coordinating minister of economic affairs during Joko Widodo's second term, and Chief of the Golkar Party. Similarly, another informant involved in a campaign to endorse Indonesia's COVID-19 policies indicated receiving support from individuals associated with Erick Thohir, the minister of state-owned enterprises and the figure overseeing the government's response to the pandemic, and one of Indonesia's wealthiest businessmen.

The second category of cybertroops clients comprises individual politicians. Indonesia's candidate-centred electoral system necessitates politicians to diligently manage their public image. Cyber troops offer valuable means to achieve this. Multiple informants shared instances of being hired by politicians to enhance their online presence and propagate positive messages about them. For instance, we interviewed a buzzer engaged in a project aimed at elevating the online visibility of a politician who was being considered for a cabinet position. This politician believed that an active Twitter account with a substantial follower count would be advantageous. The interviewed buzzer was paid three million rupiah per month to engage with and retweet posts from this politician's Twitter account. Political parties also appear to engage cyber troops for their campaigns. For

instance, during the 2019 election, our research found that both camps of running candidates were supported by cyber troopers whose fundings came from, among others: the political parties.

A third group of financial backers consists of economic elites. In Indonesia, economic and political elites maintain close ties, with wealthy entrepreneurs either entering politics or financially supporting political endeavors to gain favor with ruling elites. Within this context, some buzzers said that business figures also offered to pay for the online activities of politicians. For instance, we interviewed a coordinator of a social media team for the 2019 presidential election who stated that various entrepreneurs offered to cover his expenses.

Yet the commonality of these funders mentioned by our informants, is that they all belong to Indonesia's powerful elite. It seems that the political and economic elites have embraced cyber troops as a new instrument to defend their interests.

VI. Cybertroops as Threat to Democracy

In an era where the virtual realm intertwines seamlessly with the physical world, the rise of cyber troops has emerged as a threat to the very foundations of democracy. These digital mercenary armies manipulate information, sow discord, and subvert public discourse with unprecedented precision. In doing so, they undermine the principles of transparency, truth, and fair representation that underpin democratic societies. The convergence of technology and propaganda caste shadows over the democratic ideals many hold dear.

In this regard, we argue that there are at least six damaging impact of cyber troops and its social media propaganda on the quality and strength of democracy in Indonesia. Firstly, cybertroops activities undermine electoral integrity. In democracy, sovereignty is in the hands of the citizens. During election, it was the voice of citizens which will determine who will run as the next president and vice president as well as parliamentary members. This voice manifests in their votes during election. Indeed, democracy assumed that citizens as individual can rationally take decision for their own selves. In this regards, citizens vote for the candidates based on the information they obtained in the public sphere. In the digital era like today, the social media as digital public sphere has been one of the source to gain information about the candidates. Based on the survey conducted by CSIS conducted between 8-13August 2022, for instance, found that more than half of the Indonesian young voters (59%) aged between 17-39 years relied on internet as the main source of political information. The question then is: what happens if the information they end up believing about the candidates were actually full of hoaxes and hate speech produced by the cyber troopers? Surely, it leads to a wrong vote in the election day.

Second, cyber troops help to create political polarization. While the polarization that occurred during the 2019 elections had various causes (see Mietzner, 2020), as discussed earlier, social media propaganda fostered political polarization during the presidential elections of 2019. The hostile rivalries between the buzzers of both candidates have exploited sentiment and created

resentments between their followers to an extend that it even creates verbal dehumanization as in the label as *cebong* (tadpoles), *kampret* (bat), and *kadrun* (desert lizard). We clearly see that this hostile polarization during the 2019 election has not been settled when the election was over and even after Prabowo was then appointed as Jokowi's minister which reflects the reconciliation between the two figures.

In one hand, this polarization can then lead to a breakdown of trust between different political groups and institutions. When people view those with differing political views as not just opponents but as enemies, it becomes harder to trust the intentions and actions of the opposing side. This erosion of trust can undermine the legitimacy of democratic processes and institutions. In another hand, the polarization can also undermine social cohesion. When political polarization reaches extreme levels, it can contribute to social divisions and animosity between different groups in society. This can lead to social unrest, protests, and even violence, as people become increasingly polarized and view those on the other side of the political spectrum as threats. We have not seen this physical damage in Indonesia, however there is no guarantee that it will never happen in the future if we don't seriously overcome this polarization.

Third, public opinion manipulation through social media can endanger quality debates extremely important for a good public policy. In a democratic politics, public sphere is also a place for exchanges of ideas on how to best solve collective actions problems. We can discuss how to best overcome problems such as: air pollution, traffic jam, extreme poverty, unemployment, climate change, economic inequality, and healthcare reform. Citizens can involve in the debates and share their ideas. Politicians can use the internet to learn and understand not only on what problems perceived to be important for the public but also their thoughts on how to best solve them. However, when the digital public sphere was flooded with the voice of the paid buzzers we can not expect this quality debates.

Fourth, it can seriously erode public trust in government policy and government institution and in the end in democracy itself. This research clearly found that cyber troops have successfully manufactured citizen's consent to public policy in the internet in the case of bills on the revision of the KPK Law, new normal, and omnibus law. Millions of tweets have been produced by cyber troops to flood the digital public sphere with fake supports to those policies. In a short term, it might be effective to create fake legitimacy. However, in the long term the citizens will finally realize that their opinions were being manipulated and, when that happened, this can undermine trust in political leaders.

Finally, cyber troops hamper the freedom of expression. When individuals fear online harassment, smear campaigns, or personal attacks for voicing their opinions, they are more likely to self-censor, abstaining from participating in public discourse altogether. This erosion of free speech is antithetical to democratic principles, as it stifles the open exchange of ideas that is necessary for a vibrant and thriving society. However, this study found that cyber troops have been tasked with launching digital attacks and cyber bullying to critical accounts towards government's policies. This can discourage citizens to express their opinion in the internet. In fact, survey conducted by

LP3ES[16] and Indikator Politik[17] show that more than half or our citizens are scared to express their opinion in the internet. In both cases of the weakening of political opposition as well as cyber bullying to critical citizens we can see how cyber troops can create chilling effect to democracy.

Underlying the existence of cyber troops was the oligarchic elites in Indonesia whose economic power has manipulated public opinion, dominated the discourse and even co-opted the Indonesian social media. Thus, the phenomena of cyber troops reinforces the theory on the existence of oligarchic power in Indonesian politics (Winters, 2011). This also reflected the inability of the civil society in general to counter the public opinion manipulation. Despites its attempts to counter the discourse through launching social media post carrying opposite narrative, the number of their post were outnumbered and they only had a short endurance.

VII. Preserving Democracy in the Digital Age

To counter the threat posed by cyber troops, a multi-pronged approach is imperative. No one solution will be a panacea to the problems encroaching our digital public sphere, but if we aim to tackle the problem from a number of directions, a healthier online media environment can be achieved. Digital platforms must enhance their efforts to detect and dismantle fake accounts and networks that are used to amplify disinformation. Algorithmic transparency and responsible content curation can help prevent the viral spread of misleading narratives. Governments should strengthen regulations that promote online transparency and hold platforms accountable for their role in enabling the spread of misinformation.

Politicians should be aware the extreme danger of the use of cyber troops to democracy for both ethical and pragmatic reason. Ethically, they should refrain from engaging in "black campaigning" which is based on hoaxes, hate speech and identity politics. Pragmatically, they should be aware that in a longterm employing cyber troops will be harmful, as citizens will realize that they were being manipulated and engage less with political sphere, distrusting elites and ultimately voting them out of power. Approaching election, party politics and politicians should sit together to sign declaration promising to never use cyber troops and social media propaganda to win public votes and to attack political opponents.

Media literacy education should become an integral part of curriculum at schools, with the aim of empowering citizens to critically evaluate information sources and discern fact from fiction. Fact-checking organizations and independent journalism play a pivotal role in debunking false narratives and providing accurate information to the public. Indeed, civil society needs to take more role in the moderation of digital public sphere in Indonesia.

In conclusion, the rise of cyber troops poses a serious threat to democracy by exploiting the vulnerabilities of the digital age. These organized groups manipulate information, sow division,

[16] https://nasional.tempo.co/read/1459846/survei-lp3es-publik-semakin-takut-menyatakan-pendapat

[17] https://nasional.tempo.co/read/1580168/survei-indikator-politik-indonesia-629-persen-rakyat-semakin-takut-berpendapat

and erode trust in institutions, undermining the very essence of democratic ideals. To safeguard the integrity of democratic systems, collective efforts among relevant stakeholders such as among others: civil society organizations, academics, journalists, government, as well as digital platforms are needed to counter the spread of disinformation, enhance digital literacy, and foster a digital environment that encourages open discourse and truth. Failure to address this threat could lead to a future where the virtual realm is dominated by falsehoods, and where democracy is compromised.

References

Bradshaw, Samantha, & Howard, Philip N., (2017). "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation." In Computational Propaganda Research Project (pp. 1–37). Oxford Internet Institute.

Bradshaw, Samantha and Howard, Philip N., (2019). "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation" Copyright, Fair Use, Scholarly Communication, etc.. 207. https://digitalcommons.unl.edu/scholcom/207

Bradshaw, Samantha, Hannah Bailey & Philip N. Howard. (2021). "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation." Oxford, UK: Programme on Democracy & Technology. demtech.oii.ox.ac.uk. 26 pp.

Hopkins, Julian. (2014). Cybertroopers and tea parties: government use of the Internet in Malaysia, Asian Journal of Communication, 24:1, 5-24, DOI: 10.1080/01292986.2013.851721

Levitsky, Steven, and Daniel Ziblatt. (2019.) *How Democracies Die*. Harlow, England: Penguin Books.

Masduki (2022) Cyber-troops, digital attacks, and media freedom in Indonesia, Asian Journal of Communication, 218-233**,** DOI: 10.1080/01292986.2022.2062609

Marcus Mietzner, "Populist Anti-Scientism, Religious Polarisation and Institutionalised Corruption: How Indonesia's Democratic Decline Shaped its COVID-19 Response", *Journal of Current Southeast Asian Affairs* 39, no. 2 (2020): 227–249.

Morgan, Susan. (2018). Fake news, disinformation, manipulation and online tactics to undermine democracy, Journal of Cyber Policy, 3:1, 39-43, DOI: 10.1080/23738871.2018.1462395

Ong, Jonathan Corpus and Cabañes, Jason Vincent A., "Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines" (2018). Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines. 74. https://doi.org/10.7275/2cq4-5396

Ong, Jonathan Corpus and Cabañes, Jason Vincent, "When Disinformation Studies Meets Production Studies: Social Identities and Moral Justifications in the Political Trolling Industry" (2019). International Journal of Communication. 110.

Ong, Jonathan Corpus & Ross Tapsell. (2022). Demystifying disinformation shadow economies: fake news work models in Indonesia and the Philippines, Asian Journal of Communication, 32:3, 251-267, DOI: 10.1080/01292986.2021.1971270

R. Keller, Tobias & Ulrike Klinger (2019) Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications, Political Communication, 36:1, 171-189, DOI: 10.1080/10584609.2018.1526238

Rakhmani, Inaya and Muninggar Sri Saraswati (2021) Authoritarian Populism in Indonesia: The Role of the Political Campaign Industry in Engineering Consent and Coercion. Journal of Current Southeast Asian Affairs 2021 40:3, 436-460. https://doi.org/10.1177/18681034211027885

Sastramidjaja, Yatun, Ward Berenschot, Wijayanto, and Ismail Fahmi. 2021. The threat of cyber troop in Indonesia. *Inside Indonesia* 146 (Oct–Dec). Url link: https://www.insideindonesia.org/the-threat-of-cyber-troops

Sastramidjaja, Yatun and Wijayanto. (2022). *Cyber Troops, Online Manipulation of Public Opinion and Co-optation of Indonesia's Cybersphere*, Singapore: ISEAS Publishing, 2022, pp. VII-VIII. https://doi.org/10.1355/9789815011500-002

Sri Saraswati, Muninggar. "3. The Political Campaign Industry and the Rise of Disinformation in Indonesia". *From Grassroots Activism to Disinformation: Social Media in Southeast Asia*, edited by Aim Sinpeng and Ross Tapsell, Singapore: ISEAS Publishing, 2020, pp. 43-62. https://doi.org/10.1355/9789814951036-004

Tapsell, Ross (2021) Social Media and Elections in Southeast Asia: The Emergence of Subversive, Underground Campaigning, Asian Studies Review, 45:1, 117-134, DOI: 10.1080/10357823.2020.1841093

Thomas P. Power, "Jokowi's Authoritarian Turn and Indonesia's Democratic Decline", *Bulletin of Indonesian Economic Studies* 54, no. 3 (2018): 307–338.

Thomas Power and Eve Warburton, *Democracy in Indonesia: From Stagnation to Regression?* (Singapore: ISEAS – Yusof Ishak Institute, 2020).

Vedi R. Hadiz, "Indonesia's Year of Democratic Setbacks: Towards a New Phase of Deepening Illiberalism?", *Bulletin of Indonesian Economic Studies* 53, no. 3 (2017): 261–278.

Wijayanto, Didik J. Rachbini, Malik Ruslan & Fachru Nofrian Bakarudin. 2019. *Menyelamatkan Demokrasi* (Outlook Demokrasi LP3ES). Jakarta: LP3ES.

Wijayanto, Fiona Suwana, and Nur Hidayat Sardini. 2022. Cyber Terror, the Academic Anti-corruption Movement and Indonesian Democratic Regression. *Contemporary Southeast Asia*, *44*(1), 31–55. https://www.jstor.org/stable/27130807

Wijayanto, Malik Ruslan, Fachru Nofrian Bakarudin, Herlambang P. Wiratraman, Fajar Nursahid, Aisah Putri Budiatri & Ismail Fahmi. 2021. *Nestapa Demokrasi di Masa Pandemi: Refleksi 2020, Outlook 2021.* Depok: Pustaka LP3ES.

Wijayanto, Ward Berenschot, Yatun Sastramidjaja, and Kris Ruijgrok. The Infrastructure of Social Media Influence Operations: Cyber Troops and Public Opinion Manipulation in Indonesia (forthcoming, 2024)

Winters, J. (2011). *Oligarchy*. Cambridge: Cambridge University Press.

csis.or.id
csis@csis.or.id
@csisindonesia
CSIS Indonesia

Centre for Strategic and International Studies (CSIS Indonesia)
Jl Tanah Abang III No 23-27
Gambir, Jakarta Pusat 10160
Indonesia