Social Media, Cyberhoaxes and National Security: Threats and Protection in Indonesian Cyberspace

Budi Gunawan and Barito Mulyo Ratmono
(Corresponding author: Budi Gunawan)

Higher School of State Intelligence
Sumur Batu, Babakan Madang, Bogor, West Java 16810, Indonesia
(Email: bgunawan9916@gmail.com)

(Received Mar. 3, 2018; Revised and Accepted Sept. 7, 2018; First Online July 11, 2019)

Abstract

This study examines the proliferation of hoaxes and hate speech through websites and social media in Indonesia. Such provocative content utilizes sectarian issues to attack its creators' political opponents. This study finds that hate has been politicized and hoaxes have been commodified, both for economic and political interests, in cyberspace. There has been a transformation from freedom of speech to freedom to hate, particularly on social networks. This proliferation of hoaxes, as a means of furthering specific political interests, may potentially threaten national security and stability. To overcome the threat posed by cyberhoaxes, the state, industry, and society must take an active role in protecting cyberspace.

Keywords: Cyberhoax; Cyber Security; Freedom to Hate; Politics of Threat

1 Introduction

Since mid-2015, hoaxes and fake news have become increasingly common in Indonesia, particularly on the internet and social media. This was not the first time that hoaxes spread in Indonesia. For example, during the 2014 presidential election the tabloid Obor Rakyat ('Torch of the People') deliberately disseminated provocative fake news and emphasized sectarian issues to attack political opponents. Similar cases have occurred in India, the United States, Germany, China, France, and Malaysia, where accurate news has been mixed with gossip and hate speech before being rapidly spread through social media.

The proliferation of hoaxes has been made possible through the widespread adoption of Facebook, Twitter, WhatsApp, Line, Google+, and other new media platforms, which have made the rapid dissemination of information possible through their high degrees of interactivity and interconnectivity. Hoaxes have spread uncontrolled through cyberspace, and some have had serious social implications. In response to hoaxes, people have been killed and national stability and security has been threatened. Most hoaxes have involved fake news about sensitive tribal, religious, and racial issues as well as hate speech directed towards those in power. The razing of Chinese temples in Tanjung Balai, North Sumatra, in July 2016, is just one example of social unrest and conflict caused by hoaxes disseminated through social media. Likewise, national security was threatened by hoaxes related to Chinese migrant labor that began to be spread in mid-2015.

The cyberhoax phenomenon has become crucial in an Indonesian context, and as such requires serious attention, particularly given that half of Indonesians are active internet users. According to a survey by the Association of Indonesian Internet Service Providers (Asosiasi Penyelenggara Jasa Internet Indonesia, APJII), in 2016 more than half of Indonesia's population enjoyed internet access. Of Indonesia's population of 256.2 million, 132.7 million actively use the internet. This represents a 51.8 percent increase from 2014. Similarly, a survey by the Singapore-based social marketing firm showed that internet penetration in Indonesia had reached 51 percent in January 2017.

The rapid increase in internet usage in Indonesia has been supported by new media technologies such as smartphones and tablets. According to the Directorate General of Public Communications and Information at the Ministry of Communications and Information, in 2013 some 240 million gadgets were in use in Indonesia (Kompas, 13/04/2015). Meanwhile, according to We are Social, as of January 2015 some 308.2 million cellular phones are used in Indonesia. A 2016 survey by APJII showed that most mobile gadgets in Indonesia (including smartphones and tablets) are used to access the internet, either to seek information or to participate actively in social networks. From this data, it is clear that half of Indonesia's population uses the internet and relies on new media technology in everyday personal and social activities. They are targeted by the cyberhoaxes and hate speech produced and circulated online.

This study will examine the cyberhoaxes in Indonesia and their implications for national security and stability. It focuses on the production and dissemination of hoaxes, particularly those that discredit the government, by five Indonesian websites—saracennews.com, postmetro.com, nusanews. com, portalpiyungan.co, and NBCIndonesia. com—between 2015 and 2017. This study is intended to examine the practice, identify actors involved, and the interests that inform their activities. Furthermore, this study will also examine the potential security threat posed by such hoaxes and the possibility of defending cyberspace as part of national security.

2 Cyberhoaxes and Politics of Threat

In everyday discourse, hoaxes are often understood as untrue or fake news. Boese, in his book The Museum of Hoaxes (2002), defines hoaxes as deception involving public response [15]. Boese writes that hoaxes are lies that successfully draw the attention and imagination of the public. In their study of the hoaxes perpetrated by Alex Sokal, Marie Sekor and Linda Walsh (2004) conclude that hoaxes are rhetoric devices used deliberately to attack those opposed to the hoaxer. In the case of Sokal, they identify two types of consumers/readers, i.e. those capable of quickly recognizing the intent of the hoaxer and become co-conspirators by rapidly and massively distributing and circulating the hoax, and those deceived by the hoax and ashamed of this fact.

Today, hoaxes generally operate using internet-based new media. User generated content platforms such as weblogs and social network accounts enable hoaxers to hide their authorship, and thus rapidly and anonymously disseminate their deceit—which Lovell defines as "content whose main purpose is to attract attention and encourage visitors to click on a link to a particular webpage" [11]—is also an important factor in the dissemination of deceptive content, as it enables people to spread hoaxes with a single click. Hoaxes are similar to chain letters in their distribution, as they are normally presented together with buttons intended to facilitated their reposting.

Referring to the findings of Sekor & Walsh [15] that hoaxes are devices used to attack one's opposition, power and control are concentrated on a single button used to attack others. This is congruent with the concept of dromology introduced by Virilio in Speed and Politics [16]. According to Virilio, war and conflict has been dematerialized, as people in conflict no longer require physical territory for conquest. The mobilization of soldiers and weapons is no longer necessary, as victory relies only on the vectors of virtual technology and speed with which a "virtual" button is pushed. Weapons no longer need to be borne by soldiers, as attacks can be made with the push of a button. Similarly, cyberhoaxes are a form of virtual warfare, with its attacks being rooted in visual imagery and clickbait. As such, it is not excessive to identify cyberhoaxes as part of the politics of threat practiced in cyberspace.

In Cyber Security and Threat Politics: US Efforts to Secure the Information Age, Myriam Dunn Cavelty [4] emphasizes the different threats that have emerged together with information and communication technologies [4]. More specifically, Cavelty positions cyberthreats as products of irresponsible use of global information infrastructures. According to Cavelty, threats in cyberspace must be understood as part of the political process, as their dynamics, characteristics, and transformations are framed and informed by political agendas. As an example, she identifies how cyberthreats have become important parts of national security agendas in the 21st century, both in the United States and in the United Kingdom. Where these countries' national security policies once focused solely on material threats that clearly and physically endangered people, the increased integration of information and communications technology in everyday life has transformed countries' framing of national threats and national security.

3 Cyberhoaxes in Indonesia

In Indonesia, the emergence of new media has invigorated civil society and empowerment movements, particularly following the fall of the New Order regime. Cyberspace has seemed to promise citizens the freedom of expression and active participation in political processes. At the same time, general elections, a common manifestation of the democratization process, have been faced with intense public distrust. Few citizens trust political parties or the commitment and performance of politicians. There has been considerable public disappointment in and resistance to political processes. In cyberspace, people have greater opportunity to voice criticism and resist those in power, something not possible under authoritarian regimes. However, resulting excesses have become the basis for fake news and hate speech in Indonesia.

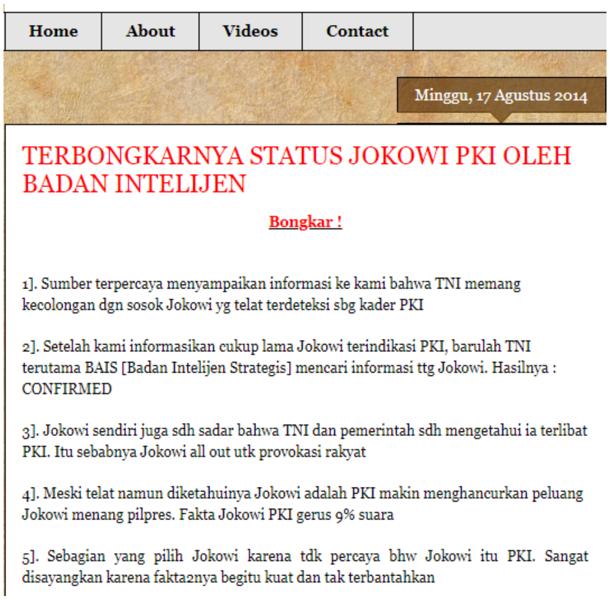
3.1 From "Freedom of Speech" to "Freedom to Hate"

According to previous research into cyberhoaxes, the websites in this researcher essentially follow the same template. These five websites position hoaxes within political contexts, particularly presidential and regional elections. In general, the creators of these hoaxes are considerably disappointed in election results, and they are dissatisfied with the performance of the political party and government in power. Initially, these hoaxers positioned themselves as critics of the government. They feel themselves to be 'victims' of government policies that they consider incapable of accommodating public interests. As citizens, they seek to represent people in similar positions.

Hoaxers' lack of trust in those in power is the basis for their criticism in cyberspace. They feel dissatisfied with the performance of the government and feel that their own interests are marginalized. This has, to some extent, become a positive influence on the democratization process. As mentioned by Dahlgren, voice is an important aspect of political participation [5]. Citing Couldry (2010), Dahlgren explains that having a voice is a fundamental part of being human, and as such silencing someone's voice is an affront to humanity. However, in the neoliberal structure some voices are unfortunately marginalized through particular economic and political designs. All peoples' voices should be accommodated within public space. The internet has been hoped to become such a new public space, in which once marginalized voices can be accommodated as a manifestation of active political participation.

This initial logic lies behind the rise of websites with provocative content. The administrators of these websites felt disappointed because they perceived that their own interests were being marginalized. They felt that those in power, whom they hoped would defend their interests, were not performing as they hoped. They also felt that those in mainstream media were unable and unwilling to promote the interests of the common people, with corporate-owned media being not neutral in their coverage because their owners are political elites affiliated with the government. Consequently, they held that mainstream media served only to support those in power. Observers and informants in the media likewise, they argued, supported the status quo.

The administrators of hoax websites thus used cyberspace as an alternative space for resisting and criticizing those in power, hoping to transform the dynamics and policies of the government. This is important given that freedom of speech and public participation have frequently been promoted during the democratization process. Citizens, it is argued, should have the agency to voice their opinions and inform governance. However, their criticism and resistance has been transformed into anarchy, hatred, and agitation, while their disapproval has transformed into provocation and incitement. They have positioned the government and those affiliated with it as common enemies to be conquered. The freedom of expression facilitated by cyberspace has been transformed into the freedom to hate. In elections, where different political parties compete for volunteers and buzzers to promote their candidates and challenge their opponents. As noted by Lim [10], in the 2017 Jakarta election volunteers and buzzers generally defend their activities as part of freedom of speech even as they were silencing their opponents. They demanded freedom of speech for their own interests, but silenced those whose interests were opposed to their group. As a result of such practices, constructive criticism was reduced to deception and hate speech with a minimal basis in objective fact as shown in Figure 1.



Minggu, 17 Agustus 2014

TERBONGKARNYA STATUS JOKOWI PKI OLEH BADAN INTELIJEN

Bongkar !

1]. Sumber terpercaya menyampaikan informasi ke kami bahwa TNI memang kecolongan dgn sosok Jokowi yg telat terdeteksi sbg kader PKI

2]. Setelah kami informasikan cukup lama Jokowi terindikasi PKI, barulah TNI terutama BAIS [Badan Intelijen Strategis] mencari informasi ttg Jokowi. Hasilnya : CONFIRMED

3]. Jokowi sendiri juga sdh sadar bahwa TNI dan pemerintah sdh mengetahui ia terlibat PKI. Itu sebabnya Jokowi all out utk provokasi rakyat

4]. Meski telat namun diketahuinya Jokowi adalah PKI makin menghancurkan peluang Jokowi menang pilpres. Fakta Jokowi PKI gerus 9% suara

5]. Sebagian yang pilih Jokowi karena tdk percaya bhw Jokowi itu PKI. Sangat disayangkan karena fakta2nya begitu kuat dan tak terbantahkan

Figure 1: Opinions about the president is a communist

3.2 The Production and Dissemination of Hoaxes

Interestingly, the cyberhoaxes perpetrated by the five websites investigated in this researcher utilize a similar modus operandi. Desiring to criticize the government in power, the website administrators use cyberspace to voice their aspirations, holding that social media and microblogs do not offer them sufficient space to promote their interests. Visibility is a central aspect of public participation [5], as people seek to gain the attention and recognition of others for their interests. This, according to Dahlgren, creates a "regime of democratic visibility".

The desire for visibility and attention, not only from those being criticized but also from others, underlay administrators' decision to create websites where they began producing hoaxes. These websites lack clear information on their founders, and their "About Us" pages appear perfunctory or even deceptive. Information on these websites' organizational structures and addresses are often not included.

At their core, these hoax websites rely on the journalistic products of the mainstream media. In selecting specific issues, they observe mainstream media coverage. Issues with the potential for controversy and support the administrators' own interests (or can be used to attack their opponents) are identified and selected. The issues they select are modified by administrators using one or more of the techniques discussed below. First, facts may be exaggerated with fiction, particularly that which can be mobilized to promote tribal, religious, and racial tensions and hatred. Second, the substance of the story may remain unchanged, but be given a provocative and bombastic headline. Third, the main points of the coverage may be maintained, but presented in clear, direct, and provocative language. Fourth, the titles of photographs or illustrations may be changed to make them more provocative. Fifth, photographs or illustrations of incidents unrelated to that being covered may be used to suggest a connection and thereby provoke readers.

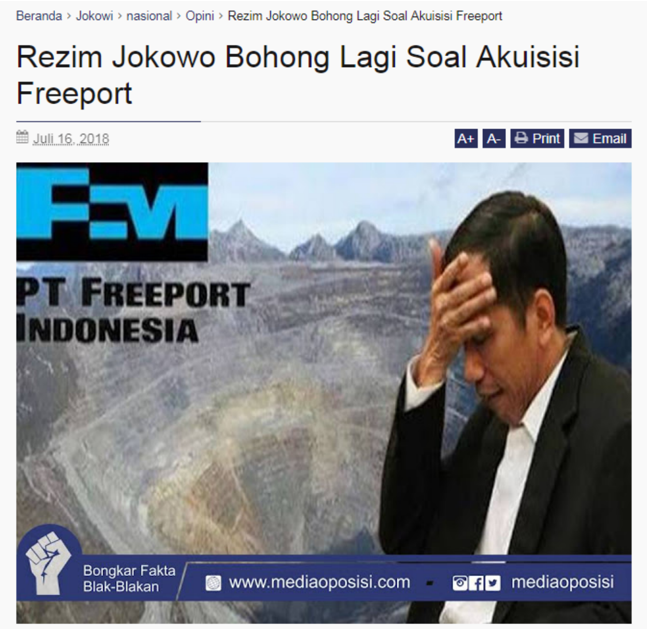
Aside from modifying coverage from the mainstream media, the administrators of these websites may also cover statements and opinions from politicians and commentators who share their vision. To do so, the administrators cultivate relations and friendships with such politicians and commentators, who are frequently opposed to existing government policy. Furthermore, these politicians and commentators are used as references or given space to voice their (anti-government) opinions on the websites.

The fake news and hate speech produced by these websites are not journalistic products that follow the accuracy and accountability standards of the profession. However, the website administrators do not care that their content violates journalistic principles. The owner and operator of postmetro.co, for example, holds that many in the mainstream media are dishonest and deliberately violate journalistic ethics. He views his website as only reproducing practices that are common, even in reputable mainstream media. They also do not fear their websites being blocked by the government, as their medium allows them to create new websites readily. For example, postmetro.com has changed domains several times after being blocked; it was first posmetro.info, before becoming postmetro.com and finally postmetro.co. They do not fear losing readers, because they believe that their readers are loyal consumers that will actively seek out their new domains. Their relations with their audiences are more emotional than rational; if these relations were rational, readers would reconsider trusting such sources or seeking content updates from websites with little accountability.

Once fake news items are produced, it is most crucial to distribute them. The most rapid means of distributing such fake news is making it go viral. To reach as many internet users as possible, the stories must become as virulent as possible. These websites' visibility and ability to draw readers' interest is key to their popularity. Website administrators are perfectly aware that, to become popular, the stories on their websites must become viral, and for this they rely on social media. As noted by Allcott & Gentzkow [1] in their study of fake news in the United States, "...social media are well-suited for fake news dissemination, and social media use has risen sharply." In an Indonesian context, Lim [10] in her investigation of the 2017 Jakarta gubernatorial election, also identified the role of social media in disseminating fake news, sectarian provocations, and racist content. The selection of social media for the virulation of hoaxes in Indonesia is not without grounds. According to data from We are Social, as of January 2017, 92 million Indonesians use social media on their mobile devices. Facebook, one of the most popular social media platforms, records 106 million Indonesian users. Based on this data, it can be said that social media networks have become an integral part of Indonesians' mobility. Regarding this, Lim (2017) writes:

> "Across the world, and most certainly in Indonesia, the expansion of social media usage has sparked new hopes of and hype about political participation and civic engagement."

Based on this statement, it is apparent that social media—particularly in Indonesia—has been seen as offering the potential to empower people and increase civil participation in political processes. These new media platforms are also thought to ease residents' shaping and sharing of their political opinions and aspirations. Nonetheless, Lim also identifies pessimism for the negative aspects of social media, such as loss of privacy, decreased quality of information, proliferation of lies, and emergence of online radical groups. This last tendency has become problematic in Indonesia, particularly given the widespread dissemination of hoaxes in social media. The popularity of social media in Indonesia has eased hoaxers in rapidly spreading provocative content (Figure 2).



Beranda › Jokowi › nasional › Opini › Rezim Jokowo Bohong Lagi Soal Akuisisi Freeport

Rezim Jokowo Bohong Lagi Soal Akuisisi Freeport

Juli 16, 2018

Figure 2: Another lie about Freeport

3.3 The Commodification of Hoaxes and Politicization of Hate

Why have fake news and hate speech become widespread on the internet, particularly on social networks? Allcott & Gentzkow [1] write that, in the United States, the main reason for spreading hoaxes are financial. The virulation of fake news through social media promises them tempting financial incentives. Every news story that goes viral will bring significant financial income for the website that originated it. Clickbait logic does not only promote the virulation of hoaxes, but also directs traffic towards the websites that originate hoaxes, bringing significant funding for their administrators. A similar phenomenon is apparent in Indonesia.

Although the administrators of websites that spread hoaxes and hate speech originally intended to promote active participation in political processes and their ideals, the financial income they have received has transformed their orientation. Their political participation was thus easily diverted towards the seeking of profit, a transformation made possible by the media industry that has used cyberspace for its political activism. Media platforms such as Facebook and Google AdSense have had an important role in promoting the commodification of hoaxes and hate speech. The advertising revenue that they receive for every click offers website administrators an extraordinary financial incentive. The higher the traffic (i.e. readers) on websites that originate hoaxes and hate speech, the higher the revenue received from advertisements.

According to the administrators of hoax websites, they can earn an annual income of 600 to 700 million rupiah from advertisements. For example, by producing some eighty fake news stories per annum, the administrator of postmetro.com can earn some 25 to 30 million per month. Owing to the highly profitable nature of deceit and agitation, postmetro.com recruited several personnel to manage the website. A new administrative structure was established, with staff working specifically on seeking out stories from the mainstream media and rewriting them with their own titles and styles. Others, meanwhile, focus specifically on the virulation of their agitation and deceit.

Similar practices are used by nusanews.com and NBCIndonesia.com. Meanwhile, nusanews.com and postmetro.co spent some time as partners. The success of these websites' advertisements can be measured through websites such as Site Worth Traffic. A single hoax story that is seen 1,000 times will earn US $1 for the hoaxer; clicks on advertisements earn them US $0.04 each. As such, the amount of money earned by websites can be measured by the number of visitors. Using Site Worth Traffic, it can be seen that NBCIndonesia.com—before being blocked by the government—received an average of 481 visits/day, 83.73% of which came from Facebook. As such, the website operator could earn US $194 per day or US $69,840 (approximately 1 billion rupiah) per annum, a fantastic amount. To maximize its income from advertisements, another hoax website, portalpiyungan.co, hired an advertising consultant to ease its dissemination of fake news. The results were impressive. Advertising income from portalpiyungan.com increased from 1.5 million per month to 150 million per month [12].

Of the five hoax providers discussed here, only Saracen was organized and had massive operations. Police investigations into the Saracen syndicate found that 33 people were involved, divided into two groups. The first group, the core team, consisted of 22 people. This team was responsible for the production of hoaxes, including fake news, hate speech, and provocative memes. The second team, which consisted of 11 people, worked to disseminate these hoaxes by making them go viral on social media. This indicates that, within this group at least, hoaxes were viewed as a business needing a professional and structured system. According to reports, the Saracen syndicate offered hoax production and dissemination services, charging between 75 and 100 million rupiah. Following the laws of supply and demand, such hoaxing practices have emerged not only because of the availability of advertising platforms such as Google AdSense, but also because of demand from specific sectors. Hoaxers have people—most of whom remain invisible—who pay for their services and their website management.

In Economies of Signs and Spaces, Lash & Urry [8] writes that, in the 21st century, the capitalist economy is no longer motored by tangible goods, but rather by indeterminate symbols that are borderless and fluid. According to Lash & Urry, the production of symbols has proliferated cognitive symbols (such as information and digital codes), abstract symbols, as well as aesthetic and expressive symbols that are used in representation (i.e. branding and image-building). The production of hoaxes is one such example. As businesses, cyberhoax websites produce intangible products, specifically cognitive symbols of hate and incitement presented as inaccurate information and hate speech. Fake news is made more "pretty" and interesting by packaging real news stories as provocative stories, with misleading titles and fiction replacing fact. To draw attention, they mobilize sensitive issues to draw readers' anger and hatred. Tribal, religious, and racial tensions are exploited to draw public attention. Symbolic and sectarian language (such as kafir "unbeliever", cina "Chinese", penista agama "blasphemer", and komunis "communist') is used to exploit primordial tensions. This language is circulated in the unlimited space known as cyberspace for mass consumption. These hoaxes are disseminated among the masses and bring with them significant profits.

The proliferation of hoaxes and hate speech in cyberspace also has ideological reasons, as it is intended to exert power and to counter that exerted by those in power. As such, these actors seemingly attempt to utilize the optimistic views of politics and civil participation. Owing to their disappointment in various government policies, which they consider to marginalize them or not represent their interests, these actors have used social media as an alternative space for voicing their views and searching for information.

The sharing and reposting of provocative news, filled with hate and incitement, can be understood as a means of gaining others' attention and recognition, part of the desire for social visibility [5]. In the context of political participation, as supported by new media platforms, the accumulation of knowledge also offers users' power. The sharing, reposting, and retweeting of news on social media indicates that this practice is perpetrated by those already drawn-in by the stories. They are people with knowledge of these stories and the issues they contain. The sharing of news stories on social media is intended to show their friends that they are knowledgeable. In other words, the people who regularly share posts on social media are those with the desire for power, as they seek to control and shape their friends' knowledge. People such as these frequently become opinion leaders among their friends. By sharing news stories, they feel in power, as they accumulate knowledge and gain greater visibility in social media. This feeling of being in power brings them pleasure. Such actors work on their own, becoming effective means of disseminating the hoaxes and provocations produced by hoaxers. Actors involved in cyberhoax practices and their underlying interests can be seen in Table 1.

3.4 Production of Uncertainty: Political Symbolism and Misinformation

As economic and political commodities, hoaxes represent an exchange of deceptive and inflammatory symbols. According to Edelman [6], the use of such symbols in a political context is an element of political symbolism [7]. The proliferation of symbols, including their use and misuse, is intended to manipulate political discourse and public opinion, According to Edelman, symbols have taken an increasingly important role in politics. Political influence and power is no longer based on material and objective facts, but the mobilization of symbols. For example, political symbolism is rampant in political campaigns. Eriksson & Giacomello [7] argue that political practices in the digital media ecosystem emphasize the exploiting of various symbols for mass mobilization and manipulation.

In the practice of hoaxing, linguistic symbols (both verbal and visual) are used to construct certain views of the issues discussed. Edelman [6] identifies two different types of symbols used in political practice symbolism: referential symbols and condensation symbols [2]. Referential systems are those related to objective elements of certain situations and objects. These symbols are frequently used to legitimize specific political views and guide the masses towards a specific and shared understanding of a situation or object, such as statistics or budgets. Meanwhile, condensational symbols are those that create certain emotions and subjective reactions to a situation or object. Such symbols are capable of shaping people's imagination of a desired world, one quite different from the real world. It is such condensational symbols that are mobilized by cyberhoaxes in Indonesia. Nonetheless, according to Edelman, both types of symbols can be used to manipulate public discourse and public opinion about certain issues. This is one-sided, intended to justify specific ideas and logics.

In cyberspace, political symbolism promotes specific simplified narratives and framings of certain situations and objects. The new media, which enables the consumption of information (and distraction), contributes importantly to this symbolization process. This can be seen, for example, in the use of clickbait, in which symbols (images) in cyberspace serve are provided as "keys" to exploring issues and problems. Through clickbait, overly simplified logics are brought into the digital ecosystem. Lim [9] writes that it is no surprise that "trailer vision" dominates social media, with "light packages" or simplified narratives presented to whet audiences "headline appetite". The (over) simplification of narratives is common in new media, and consequently very few media users seek detailed information or seriously investigate the events and processes reported. Spaces for discussion and reflection disappear as access is accelerated. Events and processes are framed as nothing but headlines, visual images that draw the eye, and short commentary. All of this is oriented towards rapid consumption, and as a result various problems are reduced and simplified through one-sided and stereotypical coverage.

Political symbolism and simplification of issues are national threats that must be minded, as they are deceptive and present nothing but misinformation mistaken beliefs [6], which can promote improper activities and result in physical conflict. The politics of threat use political symbols to produce uncertainty within society, particularly in the tense periods in the lead-up to elections. In such times of uncertainty, chaos is very possible, as people lack clear and objective information.

3.5 Tribal Nationalism based on Political Identity

When undergoing activities on social media, users frequently ignore platforms' ability to filter and sort users' digital activities. Social media platforms such as Facebook, for example, use specific mechanisms to identify users' interests and content, and presenting content to users with specific interests. These algorithms construct what is known as a bubble, in which people are isolated from different people and their diverse opinions and views [10]. As a result, social media users are only exposed to content that reaffirms their own political views and people that share said views. Differences of opinion, as well as argument, are seemingly eliminated by the "bubble" created. Because people's political preferences differ, these filters and algorithms produce bubbles of shared political views that can be termed algorithmic enclaves [10]. Lim defines these algorithmic enclaves as groups "that are formed whenever a group of individuals, facilitated by their constant interactions with algorithms, attempt to create a (perceived) shared identity online for defending their beliefs and protecting their resources from both real and perceived threats".

Algorithmic enclaves are dynamic imagined communities, membership in which may change over time. Their algorithms focus on sorting, classifying, and creating a hierarchy of political preferences, information, and people.

Borrowing Lim's concept of algorithmic enclaves, hoax consumers establish their own enclaves. Such enclaves are formed as part of an identity formation process, in which they use their resources to defend their beliefs and

Table 1: Actors, roles, and interests in cyberhoaxes

Actor	Role	Interest
Hoaxers	Commodification of Hoaxes: - Producing and disseminating hate and incitement - Seeking clients for their services	Economic: Profiting from advertisements (up to 600 million–700 million per year).
Clients	- Pay for production and virulation of hoaxes - Conspirators in hoaxing	Political: - Spread hate and incitement against their opponents
Observers/ Politicians	Politicization of Hate: - Use hoaxes as political commodities - Co-conspirators in hoaxing - Make hoaxes go viral	Political: - Spread hate and incitement against their opponents - Political personal branding - Become visible and gain political influence
Consumers/	- Consume hoaxes - Make hoaxes go viral - Co-conspirators in hoaxing	Political: - Spread hate and incitement against their opponents
	- Consume hoaxes - Make hoaxes go viral	Pleasure: Become visible and gain public attention - Feel in power

to protect themselves from threats. Such groups establish their own "tribes", which live in and influence cyberspace. Borrowing a concept first formulated by the German political scientist Hannah Arendt, Lim [10] argues that such algorithmic enclaves promote the development of tribal nationalism. In her book, the Origins of Totalitarianism, Arendt (1973) identifies tribal nationalism as one that differs from mainstream models. Where the mainstream model of nationalism is constructed on actual political experiences, tribal nationalism is based on a sense of feeling and inner soul [3]. In other words, within tribal nationalism there exists a disconnect with real-world political processes. This sense of nationalism is primarily based on a sense of fate shared among a "tribe" (group). The spreading of hoaxes on Indonesian social media also has the potential to create tribal nationalism through which political identities are mobilized. This can be seen in the religious sentiments that underlie many of the hoaxes shared on the five websites examined here, as well as the stories shared on social media. Although it is true that religious sentiments are not the only ones exploited to provoke readers—questions of ethnicity and liberalism are also used by these websites—these non-religious issues are ultimately subordinated to religions ones.

The administrators of hoax websites position Islam as a "victim", despite the religion being the most commonly practiced in Indonesia. As mentioned by Arendt, those who create a sense of tribal nationalism tend to feel threatened by "outsiders". They feel surrounded by a "world of enemies", and thus seek to create a shared sense of solidarity and struggle [3]. They may quickly form mobs and create social fragmentation. For example, the 212 Demonstrations mobilized religious issues to attack incumbent governor Basuki Tjahaya Purnama during the 2017 Jakarta gubernatorial election. In particular, the administrator of postmetro.co expressed satisfaction with the fake news he created and its ability to unite Muslims against the governor. Members of such groups tend to legitimize the exclusion of persons outside their group. For example, again using the 2017 Jakarta gubernatorial elections, a number of imams and mosque administrators refused to pray for deceased community members with different political beliefs (i.e. who supported Basuki Tjahaya Purnama). In cyber hoaxes, tribes are created through online enclaves that are formed through the production and dissemination of hoax. The emergence of political tribes poses a serious threat to national unity and stability.

4 Cybersecurity: Combatting and Preventing Hoaxes

The production and dissemination of cyberhoaxes and hate speech are part of the politics of threat and designed by certain actors to promote certain interests. Hoaxes, as with cyber threats in general, are not material, nor do they cause direct physical harm to humans. Nonetheless, they have serious social effects. In other words, the cyberhoaxes that have become increasingly widespread in Indonesia have the potential to threaten national stability. Pursuant to Law No. 17 of 2011 on State Intelligence, intelligence is an important means of maintaining national security, and the Indonesian State Intelligence Agency is tasked with the coordination of the national intelligence system. In combating the hoaxes that have become rampant in Indonesia, the Indonesian State Intelligence Agency is also tasked and authorized to conduct studies regarding various threats and the potential dangers they pose. Once these threats and their potential dangers have been identified, the Indonesian State Intelligence Agency has the duty and authority to combat them and anticipate the emergence of further threats—i.e. the future spread of hoaxes. The role and contribution of the Indonesian State Intelligence Agency is central, recognizing that several social conflicts have become physical because of the proliferation of hoaxes.

To combat cyberhoaxes, three different parties must work together: the state, market, and civil society. They must collaborate to address various strategic issues that threaten cybersecurity (in particular), as well as national security and stability in general. In the context of national authority, specific legal products must be prepared to provide stricter judicative sanctions. Referring to the concept of reflexive politics presented by Beck in his book Risk Society (1992), in risk management the government does not need rule-directed politics (i.e. politics based on existing regulations). Because risks are always transforming, society requires what is known as rule-altering politics [14]. To provide cybersecurity in Indonesia, particularly against cyberhoaxes, it is possible to apply this latter concept, for example by regulating domain ownership and setting fines for platform providers. Furthermore, it is important to increase the capacity of the State's cyber troops. The main actors behind cyberhoaxes have shown considerable reflectivity in examining Law No. 19 of 2016 about Electronic Information and Transactions, as by doing so they have been able to avoid legal snares. They do not simply accept their websites' blocking by the government, even though they only need to move to another domain. They have studied the blocking mechanisms to best avoid them. As such, the government must act to change those regulations it has enacted. The Indonesian government must transform the regulations applicable to the media platforms used to make hoaxes go viral. Thus far, Indonesia has not provided for any fines for them, relying solely on blocking mechanisms—even though forcing platforms such as Facebook and Google to pay large fines if they fail to remove fake news, hate speech, and hoaxes may serve to limit their spread on social media.

Media industries, meanwhile, must work together with corporations and media platforms. Aside from urging advertising services such as Google Ad Senseto stop providing incentives to domains that contain and propagate hoaxes, they can also urge that the code necessary to detect hoaxes and other deceptive content be enacted. The government can also prepare an agreement regarding the algorithms used to prevent the rise of online enclaves and thus the spread of a tribal nationalism based on political identity.

To face and abate the threat of hoaxes, it is insufficient for the state to collaborate solely with the media industry. Civil society itself, which is targeted by hoaxers, must be involved. The involvement of various communities in combating hoaxes is paramount. This may be done, for example, by promoting digital literacy, so that members of society act can more intelligently and critically in cyberspace.

The government must also work with and accommodate civil troops in its combating hoaxes. Groups such as the Anti-Defamation League of Indonesia (Mafindo), which was established in 2012, are actively working to combat hoaxes and promote the honest dissemination of knowledge throughout Indonesia, both online and offline. Mafindo recognizes that the scale of its activities pales in comparison to that of hoax propagation and proliferation [13], and as such it is urgent to create synergy between state-operated cyber troops and civil troops. As hoaxes become increasingly common online, attempts to counter them must also be intensified. As such, collaboration between the above three elements—the state, industry, and civil society—is paramount.

5 Conclusion

The creation and dissemination of cyberhoaxes in Indonesia is a deliberate practice intended to promote certain motives and interests. It is perpetrated by actors who seek to spread deceit and hate in the digital ecosystem. The proliferation of hoaxes in cyberspace indicates a shift from freedom of speech (facilitated by new media platforms) into freedom to hate, which is used to attack those opposed to them. The websites in this study use similar production patterns. To draw public attention, they mobilize rumors and tribal, religious, and racial sentiments. To popularize their websites, hoaxers use social media and networks to spread fake news and hate speech. The proliferation of hoaxes and hate speech in cyberspace threaten national security and stability. The State, and specifically the Indonesian State Intelligence Agency, should pay serious attention to the risks posed by such cyberhoaxes. Efforts to secure cyberspace require the active participation of not only the state, but also industry and civil society.

Acknowledgments

This study was supported by the Higher School of State Intelligence through Research Initiative Program. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author (s) and do not necessarily reflect the views of the Higher School of State Intelligence.

References

[1] H. Allcott, M. Gentzkow, "Social media and fake news in the 2016 election," *Journal of Economic Perspectives*, vol. 31, no. 2, pp. 211–236, 2017.

[2] L. Arnhart, "Murray edelman, political symbolism, and the incoherence of political science," *Political Science Reviewer*, vol. 15, no. 1, pp. 185–213, 1985.

[3] R. J. Bernstein, *Hannah Arendt and the Jewish Question*, Cambridge: Polity Pres, 1996.

[4] M. D. Cavelty, *Cyber Security and Threat Politics: US Efforts to Secure the Information Age*. London, New York: Routledge, 2008.

[5] P. Dahlgren, *The Political Web: Media, Participation and Alternative Democracy*, New York: Palgrave Macmillan, 2013.

[6] M. Edelman, *The Politics of Misinformation*, Cambridge: Cambridge University Press, 2013.

[7] J. Eriksson, G. Giacomello, *International Relations and Security in the Digital Age*, London, New York: Routledge, 2007.

[8] S. Lash, J. Urry, *Economies of Signs and Spaces*, London, Thousand Oaks, New York: Sage, 1993.

[9] M. Lim, "Many clicks but little sticks: Social media activism in Indonesia," *Journal of Contemporary Asia*, vol. 43, no. 4, pp. 636–657, 2013.

[10] M. Lim, "Freedom to hate: Social media, algorithmic enclaves, and the rise of tribal nationalism in Indonesia," *Critical Asian Studies*, vol. 49, no. 3, pp. 411–427, 2017.

[11] D. Lovell, *Native Advertising: The Essential Guide*, London, New York, New Delhi: Kogan Page, 2017.

[12] T. Majalah, *Wabah Hoax*, 8 January 2017.

[13] S. E. Nugroho, "Upaya masyarakat anti-fitnah Indonesia mengembalikan jatidiri bangsa dengan gerakan anti hoax," in *Proceedings of the National Conference of Young Indonesian Psychology Researchers*, vol. 2, no. 1, pp. 1–4, 2017.

[14] M. V. Rasmussen, "Reflexive security: NATO and international risk society," *Millennium: Journal of International Studies*, vol. 30, no. 2, pp. 285–309, 2001.

[15] M. Sekor, L. Walsh, "A rhetorical perspective on the Sokal hoax: Genre, style, and context," *Written Communication*, vol. 21, no. 1, pp. 69–91, 2004.

[16] P. Virilio, *Speed and Politics*, Los Angeles: Semiotext(e), 2007.

Biography

Budi Gunawan, Ph.D. and Senior Lecturer at the Higher School of State Intelligence, Indonesia. Currently he is the Director of National Intelligence Board of the Republic of Indonesia. His main research interests include Computer Law and Information Security Management.

Barito Mulyo Ratmono, Ph.D. and Associate Director at the Higher School of State Intelligence, Indonesia. His main research interests include Information Security System and Digital Right Management.