ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 165

2nd International Conference of Communication Science Research (ICCSR 2018)

Net-attack 2.0: Digital Post-Truth and its Regulatory Challenges in Indonesia

Vience Mutiara Rumata
Researcher
The Ministry of CIT
Indonesia
vien001@kominfo.go.id

Ashwin Sasongko Sastrosubroto
Senior Researcher
The Indonesian Institute of Sciences
Indonesia
ashw001@lipi.go.id

***Abstract*—Post Truth has been a global phenomenon. It emerged in the heightening political situation particularly during the 2016 US Presidential election and Brexit. It also echoed during the 2017 Jakarta Gubernatorial election where hoaxes, misleading information and hate speeches were massively produced and distributed within the social networks and created polarization between communities that might have led to a higher potential of horizontal conflicts. In this paper, we argue that misleading information is not solely in the form of hoaxes, but also valid news which is reframed in certain ways to paralyse people's ability to think critically and objectively. This is a new type of attack that we call "Net-attack 2.0". We set up a basic view of cyber-attack evolving stages based on its targets, which are: Cyberattack 1.0; Cyberattack 2.0; Netattack 1.0; and Netattack 2.0. The Net-attack 2.0 challenges the Indonesian internet regulatory systems. The existing Electronic and Information Transactions Act (the EIT Act) may be insufficient to address the issues. We present conclusions with several recommendations. First, the authority should take a legal review towards the EIT Act particularly article 28. Second, the authority may consider to treating user generated contents as a journalistic product and subject to Journalism Act and Code of Ethics. Lastly, the authority may treat the online attack as a physical space attack and subject to the Criminal Code. Even so, legal review should be taken on each article in the Criminal Code which is also referenced in the EIT Act.**

Keywords—net-attack; digital post-truth; electronic content; regulation; Indonesia

I. INTRODUCTION

Post truth is one of the most intensive topics of discussion nowadays. It might be triggered by the growing online misinformation which vigorously forms what people believe as the truth. "Post truth" is a global phenomenon. It was dubbed as an "international word of the year" by Oxford Dictionaries in 2016 [1]. Its popularity heightened during the election of Donald Trump as the 45th US President and Brexit in that year [2]. Long before that, the World Economic Forum (2013) listed "the rapid spread of misinformation online" as one of top 10 challenges in 2014 [3].

'Post truth' also echoed in Indonesia particularly during the Jakarta Gubernatorial election in 2017. The polarisation between pro Basuki Tjahaja Purnama a.k.a "Ahok" (represents the minority – Christian and Chinese) and pro Anies Baswedan (represents the majority – Moslem) is inevitable both offline and online. Several mass rallies, led by the Islam Defender Front, called for Ahok's detention after his Al Maidah 51 blasphemous controversy statement went viral on social media [4]. The Indonesian Institute of Sciences (LIPI) found that the identity (identitarian) politics mainly drove the polarisation during Jakarta gubernatorial election [5].

Social media play a significant role in escalating the polarized opinions mostly during the heightened political situation. Hoaxes, fake news, and hatred speeches towards both Anies and Ahok were relentlessly distributed online during the campaigns and voting. Agus Sudibyo, head of Antihoax Journalist Network, argued that 22 percent of political news distributed online was fake news during the Jakarta governor election [6]. The production and distribution of hoaxes or other misinformation forms online have given adverse impacts on the society. The Ministry of Communication and Information Technology (MCIT) monitors at least there are 800 thousand websites which allegedly distribute hoaxes and hate speeches contents online [7]. In addition, the Indonesian National Police detained Saracen online group (Saracen News Facebook, Saracen Cyber Team, Saracennews.com) which organized the distribution of provocative hate speeches and hoaxes online which has 800 thousands members on social media [8].

There is an emerging trend where misleading information is not solely present in the form of hoaxes but also in the form of valid information. The production of misleading information is not only aimed to deceive, but also to paralyse people's ability to think critically and objectively. Selective valid information is reproduced and reframed so that, therefore, considered as a new fact. This new fact is then redistributed within certain groups of networks on social media. This can be considered as a new form of digital post truth and may potentially create not only polarization, but also grass-root conflicts. We see digital post truth as a new form of cyber-attack, which we call 'Net-attack', mainly driven by reframed selected valid news distribution. While, the current content regulation, the Electronic Information and Transactions Act number 19/2016 (amendment of Electronic Information and Transactions Act number 11/2008), does not adequately address this issue.

This paper explores the technology aided deceiving practice and in what way this may challenge the Indonesian regulators. The discussion is divided into two main discussions: the digital

post-truth both in conceptual and practical matters, and the challenges that the Indonesian regulators may face in the near future.

This article presents a literature study followed by the development of a basic way of thinking that aims to obtain a better understanding of the current Net-attack, which we argue, is different from the traditional cyberattack. A traditional literature study relies on personal efficacy to select certain literatures which significantly contribute to the current knowledge [10]. Based on this, we distinguish Cyber-attack and Net attack. Following our previous study, this study starts with conceptual reviews on scientific articles which discuss Cyber-attack and Net-attack. The scientific articles are mainly obtained from EBSCO host database, Semantic Scholar, and Google Scholar search engine. Then, the study reviews on Indonesian existing cyber policies and regulations. We recommend some possible regulatory actions that can be carried out to address the Net-attack, including necessary further studies in the future.

II. Conceptual Framework

A. Cyberwar and Netwar

Most of the literatures use the term "cyber war" to describe a purposive attack by sending a virus or any malicious software to others (software or hardware) through networks. It is not surprising since related incidents may involve destructing weapons (known as malware, Botnets, or DDoS and many others) which then paralyze computer-dependent systems. The discovery of Conficker in 2008 or a cyber-super weapon Stuxnet in 2010, for instance, might alert world leaders to increase their security system to protect their critical infrastructures [11].

Furthermore, these physically damaging purposive attacks may involve inter-government (military) actions. According to Hughes and Colarik's (2017) discourse analysis on cyber war and cyber warfare, the most cited cyber war definition is "conducting, and preparing to conduct, military operations according to information-related principles" [12]. Some terminologies may appear to describe the type of cyber war, such as: cyber-terrorism (conducted by terrorist); cyber-crime (online 'daily basis crime' e.g. online banking fraud); and cyber-espionage [13]. The last one could be also considered as cyberwar if it leads to large-scale and significant computers and networks, such as Computer Network Exploitation and Computer Network Attack [14].

The increasing information and communication technology (ICT) technology usage and development may shift the emerging cyber-attack forms and purposes, and hence the terminology of classic 'cyberwarfare' may be irrelevant to describe the current situation. Valuch and his colleagues (2017) distinguish between cyberwarfare and information warfare which later on they perceive it as postmodern warfare [15]. The later one becomes our main concern in this paper. Some literatures may refer this information related attack in this super connected cyber world as 'cyber-attack' instead of 'cyberwar' or 'cyberwarfare' [15], [16]. The Cyber-attack is considered as "the new front of 4th generation warfare" (1948 until the 9/11 incident) in which the idea of "warfare" is no longer perceived as a state affair, but open for non-state actors including individuals, or extremist groups [17]. In addition, the future cyber-attack, particularly in the fourth industrial revolution, aims to create social, political, and psychological disturbance by using social networking sites [16].

Nevertheless, we argue that the notion of cyberwar goes beyond computer system based attacks. We may believe that today and in the coming years, cyberwar will be no longer paralyzing hardware devices or data merely, but will target people's way of thinking. Arquilla and Ronfeldt's notion of "Netwar" needs to be revisited to support our argument. Netwar, according to them, is co-exists and terminologically distinct with the notion of 'Cyberwar. It refers as "information-related conflict" that may harm society's perception towards themselves and the world. It also has two sides of nature in which extremist driven conflict on one side and civil society activist driven on the other side [18].

B. Post-Truth Practices

'Post truth' is not a harbinger of a new era. In fact, Keyes (2004) states that we are living in the 'Post Truth' era, an era when lies are no longer perceived as "antithesis of truth" but rationally "tampering with truth" [19]. Lewandowsky and colleagues (2017) propose that post truth claims do not seek alternative reality; instead, they eradicate trust in facts and reality so that the facts become meaningless [20]. This means people stop believing in facts. The root of post-truth relates to the practice of lying. Lying or being dishonest is a human common daily practice whether with or without intention or reason. We may tell lie or being lied with several casual lies or fibs every day. The more we get used to lie or be lied, the more we accept that "lies can be told with impunity" [19].

The post truth practice excessively occurs in contemporary political event [21]. In 2016 US Presidential election for example, the elected President Donald Trump was dubbed as first post truth President in the US presidential election history [22]. During his presidential campaign, Mr. Trump deliberately launched several aggressive, vicious, and lacks of evidences claims. A US based fact-checking website PolitiFact awarded Mr. Trump "lie of the Year" in 2015 and his statement scorecard mainly is False (32%) and Mostly False (22%) [23]. The Trump favourable voters chose to believe their own reality based on prejudice that may be formed by exaggerated and misleading claims. Trump's supporters, particularly, were unable to separate truth from fiction [24]. Human brain helps human to justify a fact or claim. The problem is when the brain justifies emotional based mechanism in which humans tend to be "cheery-picking", gathering information that supports what they want to believe and ignoring the available contradictory evidence [25].

III. Discussion

In this paper, we set up a basic view of cyber-attack evolving stages based on the nature of the targets, which are: Cyberattack 1.0; Cyberattack 2.0; Netattack 1.0; and Netattack 2.0 (Table 1.). In the cyber-attack 1.0, the target is to impair computer dependent system, but not necessarily the data. The

Cyber-attack 2.0 envisages the data manipulation although the computer system may run properly. Both Cyber-attacks allow the adversaries to target and to destruct the critical infrastructure, the operation system as well as its critical data or information. Wilson (2008) reports that these two types are basic methods of cyber-attack [26]. It needs to be acknowledged that the use of electromagnetic bomb that may destroy electronic components and computer system is similar to the use of conventional bomb, so that cannot be considered as cyber-attack.

As the use of social networking sites increases, the type of Cyber-attack has evolved into Net-attack which targets to manipulate users, not the computer system and not the data as well. It may involve non-governmental actors and may need global social networking platforms. The Net-attack 1.0 features the distribution of false information (e.g. fake news and hoaxes). The goal is to destabilize not only commercial interest but also societal and political systems. Facebook and Google allegedly sold thousands of US dollars of ads and accounts to Russian-based companies and government during the 2016 US Presidential campaign. The aim was to spread misinformation and ruin the election [27].

TABLE I. CYBER-ATTACK INVOLVING STAGES

	Actors		**Targets of Attacks**	
	Attackers	**Terminology**	**1.0**	**2.0**
Cyber Attack	Government (military)	*Cyber war*	Hardware & Software (malwares, botnets, viruses)	Data (phishing, data manipulation)
	Terrorist	*Cyber Terrorism*		
	Criminals	*Cyber Crime*		
Net Attack (*Digital Post Truth*)	Government (military)	*Netwar*	Perception (hoaxes, pornography, defamation, gambling, threats)	Perception (reframed selective valid news)
	Terrorist	*Net Terrorist*		
	Criminals	*Net Crime*		

The underlying approach to understand digital post truth practice is framing. Framing, in classical media study, refers to the way media select, portray, and promote a particular aspect of an issue or an event [28]. Within the digital study, particularly in social construction of technology (SCOT) field, Bijker proposes a notion of 'technological frame' which refers to a shared meaning or interpretation within a relevant social group related to certain technological artefacts [29]. By presenting the understanding of framing from two fields, we may conclude that framing is used to create image, meaning, and portrait of reality. In the media sociology literature, media have a significant role in shape a social reality in the society. Mass media were once a dominant tool to access social reality. Baudrillard proposes the idea of 'the power of simulacra'. It refers to the image represented by media which has four phases: 1) reflecting the basic reality; 2) twisting the reality; 3) covering that there is no truth; and 4) having no relation with reality [30].

Digital post truth is produced from any valid news that is framed in certain ways to create as if it were new information (Fig. 1). In practice, the content creator selects some pieces of valid news from different sources, frames it with a new title that may contain some provoking sentences. He or she may also provide or not provide links to the original sources. The issue emerges when the readers fail to do cross check in other credible sources, or fail to read the link that was provided earlier by the content creator. The form of post truth digital content may continue to evolve in the future.

Fig 1. Selected Valid News Framing Process

Fig 2. A Meme during flood in Jakarta

Figure 2 shows a meme which went viral during flood in Jakarta after the election of Anies Baswedan as governor last year [31]. The picture is a real photo, while the text is the interpretation of Mr. Baswedan's statement during the first gubernatorial debate which refers to jobs opportunity topic [32]. The intriguing part of this meme is the linkage between the real photo and the text. The word "kolam" (pool or pond in English) could be interpreted as flood. This meme could lead people to believe that Mr. Baswedan keeps his campaign promise to turn Jakarta into a pond of flood, instead of a pond of jobs opportunities.

A. Regulatory challenges and recommendations

The emerging digital post truth brings challenges for the Indonesian government in dealing online content. The Electronic Information and Transaction (EIT) Act number 19

year 2016 (amendment of the 2008 EIT Act) is the primary electronic content regulation in Indonesia [9]. There are several policies and regulations that have been carried out in accordance to the Act including the MCIT's online content crawling machine "Cyber Drone 9" [33]; The Indonesian police formed taskforce Satuan Tugas Nusantara [34] and A Cyber and National Encryption Agency (BSSN) which based on the Presidential Decree number 53 Year 2017 [35]. BSSN is authorized to commissioning, implementing, monitoring and evaluating technical cyber policy but not to authorize to censor or block any illegal content [36].

Nevertheless, the EIT Act may not be able to regulate the net-attack 2.0. The main argument is that some Articles in the Act are multi interpreted rules and need to be clarified by the authority. For instance, the Article 28 (1) and (2) prohibits individual to distribute fake and misleading news as well as any information that may lead hate and hostile attitudes towards particular race, religion or group. It remains unclear whether reframed valid news (digital post truth) is considered as 'misleading information'. Also, in what way and to what extent that this reframed valid news indicates hatred speeches. In this case, the Supreme Council should review this Article in order to clarify the definition and/or the boundary.

Beside EIT Act, another content regulation is the Press Act number 40 year 1999 [37]. This Act stipulates the formation of Press Council (Article 15). This council issued Journalistic Code of Ethic which prohibits journalists to deliver fake news [38]. In the beginning of 2017, the council started to verify the existing press companies in Indonesia both mainstream and online media. There are at least 43,400 online media in Indonesia whereby only 234 media that have been registered, but not yet verified [39]. The Press Act and the Press Council verification, nonetheless, may be insufficient to address net-attack 2.0 which the contents are mostly produced by non-journalists and social media users. Therefore, a legal revision should be conducted in order to accommodate user generated online contents on social networks under the Press Council's supervision. To do this, the revision should get strong support from the MCIT and BSSN.

The revision of both the EIT and Press Act may take time. The feasible way may be treating the online attacks as crimes in physical space and subject to the Criminal Code (Kitab Undang-Undang Hukum Pidana/ KUHP). It has to be noted that the Criminal code is Dutch-colonial law product and also under international spotlight over human rights abuse allegation [40]. To address this, we call legal reviews on each article in the Criminal Code that also regulated in the EIT Act. This legal reviews aim to make clear definitions and reduce any potential multi interpretations so that the law enforcers may be able to charge persons who disseminate digital post truth contents

IV. Conclusion

In this paper, we argue that cyberattack has evolved into net-attack in recent post truth era. We propose a basic view of cyber-attack development framework based on its targets, which are: Cyberattack 1.0; Cyberattack 2.0; Netattack 1.0; and Netattack 2.0. It determines the shifting process of the nature of the attack from computer and data to the users (perception). We distinguish net-attack 1.0 is envisaged by fake news or hoaxes, and net-attack 2.0 is characterized by reframed valid information.

The net-attack 2.0 opens a new challenge for the Indonesian regulators. The EIT and Press Act may be hardly to regulate the net-attack 2.0 issue. We propose three recommendations. First, the authority should take a legal review towards misinterpretation articles in the EIT Act. Second, the authority may consider treating user generated contents as journalistic products subject to Journalism Code of Ethics. Lastly, the authority may treat the online attack as physical space attacks subject to the Criminal Code. Even so, a legal review should be conducted to the Criminal Code in order to accommodate net-attack 2.0 practice.

Acknowledgement

We would like to thank the Centre of Informatics Application and Public Information and Communication, the Research and Development Agency of the Ministry of Communication and Information Technology of the Republic of Indonesia.

Biography

Vience Mutiara Rumata is a researcher at the Ministry of Communication and Information Technology. Her research interests include internet governance, media and communication fields.

Ashwin S. Sastrosubroto is a researcher at the Indonesian Institute of Sciences. His research interest is mainly internet governance. He is also a member of the Indonesian National ICT Council.

References

[1] Alison Flood, "'Post Truth' named word of the year by Oxford Dictionaries," Nov. 15, 2016. [Online]. Available: https://www.theguardian.com/books/2016/nov/15/post-truth-named-word-of-the-year-by-oxford-dictionaries. [Accessed: Dec. 20,2017].

[2] C. Gaffey, "Donald Trump and Brexit Make 'Post-Truth' the Word of the Year," Nov. 16, 2016. [Online]. Available: http://www.newsweek.com/donald-trump-and-brexit-make-post-truth-word-year-521731. [Accessed: Jan. 22, 2018].

[3] W. L. Howell, M. N. Gmür, P. Bisanz, and Et_al., "Outlook on the Global Agenda 2014," World Econ. Forum, 2013.

[4] C. A. Wijaya, "Religious expert says Ahok's remarks blasphemous," Jakarta Post, 2017. [Online]. Available: http://www.thejakartapost.com/news/2017/02/21/religious-expert-says-ahoks-remarks-blasphemous.html. [Accessed: Jun. 12, 2018].

[5] LIPI, "LIPI Paparkan Hasil Riset dan Analisis Pilkada Jakarta 2017 [LIPI Explains Research and Analisis Results of Jakarta Gubernatorial Election 2017]," May 3, 2017. [Online]. Available: http://lipi.go.id/siaranpress/lipi-paparkan-hasil-riset-dan-analisis-pilkada-jakarta-2017-/18099. [Accessed: Jan. 22, 2018].

[6] S. Dharma, "Selama Pilgub DKI Jakarta, Berita Hoax Terbesar Kedua [Along the Jakarta Gubernatorial Election, Hoax News Appearance is the Second Largest]," May 2, 2017. [Online]. Available: https://news.okezone.com/read/2017/05/02/338/1680791/selama-pilgub-dki-jakarta-berita-hoax-terbesar-kedua. [Accessed: Jan. 22, 2018].

[7] A. B. Pratama, "Ada 800 Ribu Situs Penyebar Hoax di Indonesia [There are 800.000 Hoax-spreader Sites in Indonesia]," Dec. 29, 2016. [Online]. Available: https://www.cnnindonesia.com/teknologi/20161229170130-

185-182956/ada-800-ribu-situs-penyebar-hoax-di-indonesia. [Accessed: Jan. 22, 2018].

[8] BBC Indonesia, "Kasus Saracen: Pesan kebencian dan hoax di media sosial 'memang terorganisir' [The Saracen Case: Hate and Hoax Messages in Social Media are 'certainly organised']," Aug. 24, 2017. [Online]. Available: http://www.bbc.com/indonesia/trensosial-41022914. [Accessed: Jan. 22, 2018].

[9] Republic of Indonesia, The Act number 19 year 2016 on Electronic and Information Transactions (amandment). Indonesia, 2016.

[10] J. Jesson, L. Matheson, and F. M. Lacey, Doing Your Literature Review: Traditional and Sistematic Techniques. Sage Publication Ltd., 2011, pp. 1–193.

[11] P. J. Parks, Cyberwarfare. San Diego: Reference Point Press, Inc., 2013.

[12] D. Hughes and A. Colarik, "Intelligence and Security Informatics," vol. 5376, pp. 15–33, 2008.

[13] K. Saalbach, Cyber war Methods and Practice, p. 114, 2016.

[14] B. Schneier, "Computer Network Exploitation vs. Computer Network Attack," Mar. 10, 2014. [Online]. Available: https://www.schneier.com/blog/archives/2014/03/computer_networ.html. [Accessed: Feb. 6, 2018].

[15] J. Valuch, T. Gábriš, and O. Hamul'ák, "Cyber Attacks, Information Attacks, and Postmodern Warfare," Balt. J. Law Polit., vol. 10, no. 1, pp. 63–89, 2017.

[16] C.-H. Hur, S.-P. Kim, Y.-S. Kim, and J.-H. Eom, "Changes of Cyber-Attacks Techniques and Patterns after the Fourth Industrial Revolution," 2017 5th Int. Conf. Futur. Internet Things Cloud Work., pp. 69–74, 2017.

[17] H. Kuru, "Evolution of War and Cyber-attacks in the Concept of Conventional Warfare," J. Learn. Teach. Digit. Age, vol. 3, no. 1, 2018.

[18] J. Arquilla and D. Ronfeldt, "Cyberwar is coming!," Comp. Strateg., vol. 12, no. 2, pp. 141–165, 1993.

[19] R. Keyes, The Post-Truth Era: Dishonesty and Deception in Contemporary Life. St. Martin's Press, 2004.

[20] S. Lewandowsky, U. K. H. Ecker, and J. Cook, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," J. Appl. Res. Mem. Cogn., vol. 6, no. 4, pp. 353–369, 2017.

[21] J. Rose, "Brexit, Trump, and Post-Truth Politics," Public Integr., vol. 19, no. 6, pp. 555–558, 2017.

[22] G. Tsipursky, "Towards a Post-Lies Future: Fighting 'Alternative Facts' and 'Post Truth' Politics," the Humanist, 2017.

[23] PolitiFact, "Donald Trump's File." [Online]. Available: http://www.politifact.com/personalities/donald-trump/. [Accessed: Jun. 12, 2018].

[24] J. Ball, Post-Truth: How Bullshits Conquered the World. Biteback Publishing, 2017.

[25] D. J. Levitin, A Field Guide to Lies: A Critical Thinking in the Information Age. New York: DUTTON, 2016.

[26] C. Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 2008.

[27] B. Carey, "How Fiction Becomes Fact on Social Media." [Online]. Available: https://www.nytimes.com/2017/10/20/health/social-media-fake-news.html. [Accessed: Feb. 07, 2018].

[28] A. Holton, N. Lee, and R. Coleman, "Commenting on health: A framing analysis of user comments in response to health articles online," J. Health Commun., vol. 19, no. 7, pp. 825–837, 2014.

[29] H. K. Klein and D. L. Kleinman, "The Social Construction of Technology : Structural Considerations," vol. 27, no. 1, pp. 28–52, 2014.

[30] D. Holmes, Communication Theory: Media, Technology and Society. London: SAGE Publications, 2005.

[31] I. Saqila, "Anies Sasaran Bully, Benarkah Ahokers Belum Move On [Anies Becomes Bullying Target, Does Ahokers Have Not Moved On]," [Online]. Available: http://merdekanews.co/read/649/Anies-Sasaran-Bully-Benarkah-Ahokers-Belum-Move-On. [Accessed: May 26, 2018].

[32] T. Yulianti, "Transkrip Debat Perdana Pilgub DKI Jakarta Segmen Dua [Transcript of the First Debate of Jakarta Gubernatorial Election, Second Segment]," 2017. [Online]. Available: https://tirto.id/transkrip-debat-perdana-pilgub-dki-jakarta-segmen-dua-cgXp. [Accessed: May 26, 2018].

[33] Kominfo, "Mesin Pengais Konten Negatif di Kementerian Kominfo Telah Berfungsi [Negative Content Scavanger Machine at the Ministry of Communication and Information Technology has Activated]." [Online]. Available: https://kominfo.go.id/content/detail/12240/siaran-pers-no-263hmkominfo122017-tentang-mesin-pengais-konten-negatif-di-kementerian-kominfo-telah-berfungsi/0/siaran_pers. [Accessed: Mar. 6, 2018].

[34] A. Santoso, "Setara Institute: MCA Beda dengan Saracen, Lebih Merusak [Setara Institute: MCA different with Saracen, it is More Destructive]," Mar. 5, 2018. [Online]. Available: https://news.detik.com/berita/3899240/setara-institute-mca-beda-dengan-saracen-lebih-merusak. [Accessed: Mar. 6, 2018].

[35] President of the Republic of Indonesia, Presidential Decree number 23 year 2017 on A Cyber and National Encryption Agency. Indonesia.

[36] Cyber and National Encryption Agency, The Regulation of Cyber and National Encryption Agency number 2 year 2018 on Cyber and National Encryption Agency Organization and Procedures. Indonesia.

[37] Republic of Indonesia, The Act number 40 year 1999 on Press. Indonesia.

[38] Indonesian Press Council, The Press Council Regulation number 6 year 2008 on the legalisation of Press Council decree number 3 year 2006 on Journalistic Code of Ethic as Press Council Regulation. Indonesia.

[39] F. J. Kuwado, "Dari 43.000 Media 'Online', Hanya 234 yang Sesuai Syarat UU Pers [Of 43.000 Online Media, Only 234 that Qualifies Press Law Requirements]," 21 december 2016. [Online]. Available: https://nasional.kompas.com/read/2016/12/21/19022441/dari.43.000.media.online.hanya.234.yang.sesuai.syarat.uu.pers. [Accessed: Mar. 8, 2018].

[40] Sheany, "Criminal Code Draft Revision 'Inherently Discriminatory': UN Human Rights Chief," 2018. [Online]. Available: http://jakartaglobe.id/news/criminal-code-draft-revision-inherently-discriminatory-un-human-rights-chief/. [Accessed: Jun. 12, 2018].