The objective of this research is to investigate the impact of the Indonesian citizen’s cyber culture on the Indonesian cyber security policy. It also identifies and potentially fills gaps in the Indonesian cyber security policy. In order to achieve this objective, the study commences with a comprehensive review of the research and relevant government documents. A number of in-depth interviews were conducted with seven sources representing a variety of cyber security stakeholders in Indonesia. Using content analysis and the application of Cyber Security Civic Discourse, Three Tenets of Cyber Security, and Copenhagen’s Securitization Theory, this research highlights two important points. Firstly, there are two ways the negative impacts of the Indonesian cyber security culture affect the Indonesian cyber security policy; firstly as the primary source of cyber threats and secondly as the most vulnerable part in the cyber security system. Secondly, all of interviewees believed that cyber culture is the most important element of cyber security policy, however this research finds it has not been addressed optimally within the policy. This study contributes to the existing body of knowledge in two major ways. Firstly, it broadens knowledge about cyber security culture to help address the lack of research on the cyber security issue in developing countries. Secondly, it strengthens the previous finding on the significance of cyber security culture as the main pillar of cyber security policy strategy. Finally, this study provides potential future related study needs.

**Keywords:** Cyber Culture, Cyber Security Policy, Cyber Security Culture, Cyber Security Civic Discourse, Cyber Security Tenets, and Copenhagen’s Securitization Theory
Hence, this research believed that it was essential to conduct research into the relationship between cyber culture and cyber security policy in Indonesia to show the gaps between the contemporary challenges and the policy of Indonesia, which will contribute to the discussion on the importance and significance of considering cyber culture in the process of decision-making of cyber security policy and strategy in general.

**Literature Review**

**Cyber Culture**

Cyber culture is the first concept that needs to be discussed. Since it cannot be separated from the Internet; hence, it is important to understand the nature of Internet. Coye and Ashwin (2012) define the Internet as a network of computer with a worldwide system that comprises of two kinds of networks; the technical network such as computer hardware, computer system, and communication mechanisms, and the social network that allows the user to share, store, and retrieve information. There are seven characteristics of the Internet (Delli-Carpini, 2000): (1) it enhances the speed of gathering and transmitting information, (2) it improves the volume of easy access to information, (3) it allows greater flexibility to access information, (4) it facilitates greater opportunity and blends of interaction, (5) it transforms the character of society from area to interest based, (6) it mixes variety types of media (audio, visual, and print), and (7) it challenges the conventional definitions of the producer and consumer of information.

From the theoretical perspective, Ardevol (2005) defines cyber culture as a concept that enables researchers to understand the Internet from the cultural oriented standpoint as well as to draw a subject of study for scholars from the variety of disciplines to collaboratively explore the social and cultural aspects of using the Internet. Furthermore, deriving from this cyber culture’s definition, Bell (2001) categorizes two types of cyber-subculture: (1) those that use cyberspace to advance their projects, in the same way as they might use other forms of communication, and (2) those that signal an expressive relationship to the technology through subcultural activities. The first type of cyber-subculture comprises two forms: *fan cultures* that formulated through a similar shared of interest (p. 167) and *conspiracy cultures* that develop from the “fringe beliefs” of the society (p. 170). There are four forms of the later type, which are the *MUDs* that stand for Multi-User Dungeons\(^1\), *Cyberpunks\(^2\)*, *Hackers\(^3\)*, and *Neo-Luddites\(^4\)*.

There are four approaches to understanding the cyber culture of community. Firstly, to approach cyber culture as a new model of culture (Levy, 1997; Escobar, 2000; Castells, 2002). The second approach is to investigate cyber culture as an emergent culture of the Internet (Porter, 1996; Reid, 1994). The third approaches cyber culture as the cultural product that develop on the Internet (Hall, 1997). Lastly, the fourth approaches cyber culture as a social practice within the Internet (Gauntlett, 2000). Adopted from Ardevol’s work on the anthropological perspectives of the Internet (2005), the diagram below shows the four approaches to understand the development of cyber culture in community (See Figure 1).

---

\(^1\) MUDs are “interesting and particular online social systems, where issues of community, identity, and sociality coalesce and are contested” (Bell, 2001: 174)

\(^2\) Cyberpunks refers to “a new hybrid of subcultures that is produced by a *bricolage* of technofuturism and recycled pasts” (p. 176)

\(^3\) Hackers is someone or group of people, who “accesses other people’s computers and data” (p. 180)

\(^4\) Neo-Luddites is “anti-technological fringe beliefs, which rails against the negative impacts of advanced technologies and industrial society” (p. 182)
Cyber Security

This research attempts to find the gap between the development of cyber culture of Indonesian citizen and the contemporary cyber security policy of Indonesia. Thus, it is necessary to comprehend the concept of cyber security. Cyber security has been a daily issue that can be found anywhere, from the news that reports spam, scams, frauds, and identity theft, to academic articles that discuss cyber warfare, cyber espionage, and cyber defense (Dunn-Cavelty, 2010). However, it remains a complicated task to approach cyber security as merely a simple issue of network security or individual security as it connects to a larger issue of the state, society, the nation, and the economy (Hansen & Niessenbaum, 2010).

Furthermore, there are three main pillars of cyber security issue, which are confidentiality, integrity and availability, and known as the CIA triad. According to Agarwal et. al (2011), confidentiality is the effort to prevent the unauthorized revelation of others’ personal information (p. 257) in order to ensure the information is not made available or disclosed to unauthorized individuals, entities or processes. While integrity is the guarantee that assures the accuracy and completeness of the information (p. 258), availability is the guarantee that pledges the accessibility and usability of information, upon demand, by the authorized user in a timely and unremitting manner (Stapleton, 2014, p. 5). The primary objective of any cyber security policy is to ensure the operation of these three pillars by diminishing any potential threats (Dunn-Cavelty, 2010).

Also, there are three primary elements of cyber security, which are people, process, and technology. Andress (2003) argues that security is the result of interaction between these three elements. He further insists that people are not only the most important element, but also the “weakest link in the security eco-system” (p. 5). Nonetheless, Andress (2003) points out that, within these three elements, technology is the least important component in the system, because it relies on the other two elements. Moreover, according to Janes (2012), the element that links people and technology is process, which comprises policy and procedures. The vulnerability of any of these three elements will significantly threaten the system as a whole; hence, Andress (2003) emphasizes the importance of integrating these three elements in the policy in order to preserve security.

Figure 1. Four Approaches to understanding Cyber Culture

<table>
<thead>
<tr>
<th>The new model of Culture</th>
<th>The Internet Culture</th>
<th>The cultural product develop on the Internet</th>
<th>The social practice within the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Internet as a technology</td>
<td>• Virtual space as a new social context</td>
<td>• Internet as an instrument</td>
<td>• Internet as medium of communication</td>
</tr>
<tr>
<td>• Formulation of a new society</td>
<td>• Formulation of a new cultural form</td>
<td>• Digital culture</td>
<td>• Consumption behaviors</td>
</tr>
<tr>
<td>• Social and cultural transformation</td>
<td>• Virtual communities, virtual societies</td>
<td>• Culture as a symbolic production</td>
<td>• Culture as a social practice</td>
</tr>
</tbody>
</table>
Our interpretation of cyber security will not be only informed by what we perceive to be the most significant to our daily lives, but also by the view of the government and other prominent actors. The interplay of political expression to the variety of cyber threat is one of the reasons why it is difficult to understand cyber security issue (Dunn-Cavelty, 2013).

Dunn-Cavelty (2010) defines cyber security, as pertaining both to the insecure conditions existing in cyberspace and the technical and non-technical efforts to make it more secure from any potential threats (p. 363). This definition attempts to suggest that cyber security is not merely a technical matter, which always associated with computer science, cryptography or information technology, as many cyber security related researchers that have been discussed in recent years (e.g. Vacca 2013, McLean 2013). In reality, cyber security entails larger study areas and complex matters. To further explain it, Dunn-Cavelty (2010) categorizes three interlocking cyber-security discourses. First is technical discourse that involves the matters of ‘viruses, worms, and other bugs’ (p. 364). Second is the discourse of crime and espionage that entails of ‘cyber-crooks and digital spies’ (p. 347). The last is military and civil defense discourse that encompasses the subject of ‘cyber(ed) conflicts and vital system security’ (p. 349).

The abovementioned discourse categorization of Dunn-Cavelty is based on the interplay between the threat sources and threatened objects. To understand this relationship, the work of Hansen and Niessanbaum (2010), using Copenhagen’s securitization theory, will be helpful. By using the theory of securitization, they theorize cyber security is a divergent division with a precise collection of threats and referent objects (p. 1155). The major point to understanding the cyber threat potential magnitude is the natural character of the computer system linked as “a network controlling physical objects, such as chemical vats, electrical conductors, pipeline pumps, radars, and trains” (p. 1161). To explain it in more detail, they use three grammars of cyber securitization. First is hyper-securitization (p. 1163). This hyper-securitization grammar is used to explain the development of securitization that goes beyond a normal level of threats and dangers by defining the tendency to amplify threats in order to enable the implementation and deployment of the extreme countermeasures.

Second is everyday security practice. The actor of securitization, that includes not only government but also business and private organizations, uses this grammar to describe their experiences of insecurity, and to mobilize larger groups in two ways: “to secure the individual’s partnership and compliance in protecting network security, and to make hyper-securitization scenarios more plausible by linking elements of the disaster scenario to familiar experiences from everyday life” (p. 1165).

The third is technification. This grammar is used to explain the important role of technical experts, such as the securitizing actor in “legitimizing cyber security, on their own, as well as in supporting hyper-securitizations and in speaking with authority to the public about the significance of its everyday practices” (p. 1169).

In addition to the significance of the interaction between collective threats and threatened objects, the three grammars of cyber securitization demonstrate the important role of securitization actors in cyber security, in which according to Dunn-Cavelty in another article (2013) called “heterogeneous political manifestation that linked to different threat representations” (p. 105). Dunn-Cavelty conveys that the actors of securitization in cyber security are not only government as visible elite actors, but also non-government as less visible actors (p. 118). Furthermore, she argues that these actors shape “a reservoir of acceptable threat representations” that affects the cyber security practice (p. 115). Moreover, she explains that the three-cyber threats representations, which are biologizing technology, socio-politico clusters, and interdependent human-machine vulnerabilities, are solidified by the attribution problem of cyber nature that refers to the difficulty to identify “the sources of a cyber-attack and their motivations” (p. 113). Unless the attackers declare they are responsible for the attack, like Al Qaida in 9/11 tragedy, they will remain unknown, as in “the case of Estonia” (Hansen & Niessanbaum, 2010, p. 1170).

**Cyber Security Culture**

One of the main outcomes of this research is the investigation of the development of cyber security culture of Indonesian citizen. Therefore, the discussion of cyber security culture concept is important. People are one of the primary elements in cyber security (Andress, 2003). Furthermore, Schulz (2005) contends that cyber security is not only about a technical issue, more than that it is about people that
need to be carefully considered. As Huang et al. (2007, 2009) argue that the role of humans in handling information is constantly considered as the weakest link in information security. Hence, this shows the significance of the study of cyber security culture to the development of cyber security.

Moreover, the research of Sabillon et al. (2016) on the strategy of cyber security of ten advanced countries, five intergovernmental organizations, and eleven cyber security frameworks, found that cyber security culture is placed as the primary pillar of cyber security strategy and policy by these all countries, organizations and frameworks. Nonetheless, the research of Karlsson et al. (2014) that investigated the state-of-the-art of cyber security culture literature published between 2000 and 2013 found that the concept of cyber security culture has not been vigorously researched.

Cyber security culture is about “how citizens and society apply the use of cyber security measures” (Sabillon et al., 2016, p. 79). Lacohee et al. (2006) in his research on the significance of people in cyberspace, notes that people often have the problem of awareness and understanding of what is the actual meaning of being secured. Furthermore, the study of Rotvold (2008) on creating security culture in organization notes that to make users aware and understand of security, they need to be informed of their exact roles and responsibilities in securing the information and be trained to take appropriate measures when facing any potential security threats. The Cyber Security Strategy that proposed by Nugraha et al. (2016) to the government of Indonesia also addresses the importance of cyber security mindset and awareness. Also, one of the recommendations emphasizes the need of promoting “cyber security training and education programs” to society that starts from government employees to small-medium enterprises (p. 98).

The research of Shaaban and Conrad (2012) on democracy, culture and information security in Zanzíbar found four important factors in the relationship between democracy and information security culture, which are power distance, uncertainty avoidance, in-group collectivism, and future orientation. Besides, the study on Cybersecurity decision-making in Australia by Parsons et al. (2015) suggests that improving the security culture of an organization is the best way to embed cyber security culture to the employee.

METHOD

A research method is important because it provides an outline to achieve the established objective of the research. As Cavana, Delahaye and Sekaran (2001) points out that research method not only helps the researcher to answer the research questions but also to effectively control the logic by linking to methods to be employed in answering the questions of research. Moreover, this research method with reference to the study, the setting, the extent of researcher interference, the time scope and the analysis units, includes a series of rational decisions (Cavana et al., 2001). This research uses qualitative methodology to collect and analyze the information needed to answer the research question and to achieve the objective of the research.

Before collecting the information, this research conducts reviewed the literature related to the concepts of cyber culture and cyber security, and the discourse of democracy and reformation in Indonesia to continue the earlier investigation on the appropriate methodology. On this further literature review, the research sought to gain better and deeper understandings of the core concepts, theory, characteristics, and all substances related to the discourse of cyber culture and cyber security as well as democracy and Indonesian reformation. In addition to an effort to connect this study to the previous findings (Hall, 2008), reviewing pieces of literature enable this research to provide a theoretical or conceptual framework as a solid basis for the further empirical findings. Following this literature review, the next step of the research design is the information collection.

In collecting the information, this researcher opted to use two methods: document analysis and in-depth interviews. The document analysis was used to obtain information that has been proven devoid of researcher involvement, while the in-depth interview will help the researcher to collect empirical information from the direct sources to confirm and support the written pieces of evidence from the documents. This research uses most of the criteria of the cyber security stakeholders based on the Cyber Security Strategy Guide that released by the International Telecommunication Union (ITU)
(Wamala, 2011). Furthermore, in analyzing this collected information, this research employs content analysis in order to help in examining the validity and reliability of the information before it is processed by the main analysis part of this research.

Findings and Discussion

This research found that there are two ways the negative impacts of the Indonesian cyber culture affect the Indonesian cyber security policy. Firstly, all of the interviewees argue that cyber culture of the Indonesian citizen is the main source of threat to the contemporary national civic discourse of Indonesian cyber security. Secondly, most of the respondents believe that the people element, the citizen is the most vulnerable part of the cyber system. Although, all of the interviewees believed that cyber culture is the most important element of cyber security policy, this research found it has not been addressed optimally within the contemporary policy.

Additionally, from the review of documents related to the impact of Indonesian citizen cyber culture, the International Intellectual Property Alliance reports that the cyber crime related to property rights increase yearly. As can be seen from the Figures 4 and 5, the estimated loss due to copyright violation increased from 197.5 million in 2003 to 255.2 million 2007.

![Figure 2. Estimated Trade Losses in Indonesia due to Internet Piracy (IIPA, 2008, p. 207)](image)

![Figure 3. Criminal Copyright Enforcement in Indonesia (IIPA, 2008, pp. 210-211)](image)

**ENFORCEMENT UPDATES FOR INDONESIA**

<table>
<thead>
<tr>
<th>INDONESIA: CRIMINAL COPYRIGHT ENFORCEMENT STATISTICS 2007</th>
<th>SOUND RECORDINGS²</th>
<th>MOTION PICTURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMBER OF RAIDS CONDUCTED</td>
<td>10 (73)</td>
<td>110</td>
</tr>
<tr>
<td>NUMBER OF VCD'S SEIZED</td>
<td>153,205</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF DVD'S SEIZED</td>
<td>334,076</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF CD-Rs/DVD-Rs SEIZED</td>
<td>257,096</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF INVESTIGATIONS</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF VCD LAB/FACTORY RAIDS</td>
<td>3 (30)</td>
<td>NA</td>
</tr>
<tr>
<td>NUMBER OF CASES COMMENCED</td>
<td>3</td>
<td>109</td>
</tr>
<tr>
<td>NUMBER OF ARRESTS</td>
<td>21 (230)</td>
<td>NA</td>
</tr>
<tr>
<td>NUMBER OF DEFENDANTS CONVICTED (INCLUDING GUILTY PLEAS)</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>ACQUITTALS AND DISMISSEALS</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>NUMBER OF CASES PENDING</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
Furthermore, as reported by the Akamai International, Indonesia, with its 1.3 percent share of world Internet users in 2013, has the highest rate of cyber traffic attack in the world, which contributes 38 percent to the total cyber attack in the world (see Figure 6).

**Figure 4. Attack traffic in 2013 (Akamai International, 2013, p. 4)**

From the aforementioned findings review, it can be seen that there are three different responses on the significance of cyber culture in the making of the national cyber security policy by the government of Indonesia. Most respondents believed the government, in determining the cyber security policy, has considered the cyber culture of the Indonesian citizen. It can be seen from the dynamic of the development of government regulations related cyber security. Nevertheless, another response views the dynamic of this regulation development was sub-optimal as compared to the development of the cyber culture of the Indonesian citizen. Furthermore, other respondents believed that cyber culture had not been considered significantly, and one of their primary evidence was that there is no specific policy based on an assessment of Indonesian citizen cyber culture.

To understand the argument of most of the respondents on how cyber culture of Indonesian citizen becomes a consideration in the policy making of cyber security in Indonesia, it is useful to apply the civic discourse of the three-interlocking cyber security categorization by Dunn-Cavelty (2013) and the three tenets of cyber security. From Dunn-Cavelty’s definition of cyber security (See Chapter 2), it can be seen that the primary goal of any cyber security policy is to make the cyberspace secure from any potential threat. Also, the three tenets (See Chapter 2) that bolster cyber security are confidentiality, integrity and availability. Thus, identifying and addressing any potential attack from these three threats is the core of cyber security policy.

Moreover, all of the respondents argue that the cyber culture of the Indonesian citizen is the main source of threat to the contemporary national civic discourse of Indonesian cyber security. There are two justification points of this argument.
First, the excessive freedom that embeds in the cyber culture of Indonesian citizen to some extent allows the high availability of information. However, on the other hand, it does not guarantee the accuracy and trustworthiness of such information, which in cyber security tenets is considered an integrity issue (Agarwal, 2011). Interviewee 1 contends that, after the reformation, there have been many hoaxes and fake news flooding the Internet, which stem from unreliable information and sources. Besides, Interviewee 2 points out the poor awareness and understanding of the citizens related to this integrity issue which allows the rapid spread of hoaxes and fake news, because citizens easily share information. The National Press Council insists that the hoaxes and fake news in Indonesia have been at a very critical level (Hukum Online, 2017). Furthermore, Interviewee 3 argues that most of these hoaxes and fake news items are related to ethnic and religious issues, which in Indonesia, is very sensitive and might threaten the national security of Indonesia.

Second, the confidentiality issue of information that prevents unauthorized access (Agarwal, 2011) also becomes a concern due to the cyber culture of the Indonesian citizen. Interviewee 6 argues that most of Indonesian citizens easily share their personal data, which actually should remain confidential on the Internet, especially on social media, that anyone can access. Besides, Interviewee 7 insists that the low level of knowledge and understanding in terms of how to limit access to shared information intensifies the insecurity of personal data. As a consequence, there has been an increasing number of cyber crimes attacking the principles of confidentiality and integrity that have been reported to the Indonesian police. According to the Indonesian National Police, 1,207 of 1,627 reported criminal cases is related to cyber crime, dominated by hoaxes, fake news, and hate speech (Ratnasari, 2016).

The other factor that makes the cyber culture of the citizen relevant to policymaking is the vulnerability of the citizen. As discussed in Chapter 2, there are three main elements of cyber security: people, technology and process (Andress, 2003). In the case of Indonesia, as argued by most of the respondents, the people element is the most critical. Only a small number of people in Indonesia have knowledge of cyber security. As Interviewee 7 contends, most of the Indonesian citizens have limited knowledge in terms of how to technically protect their personal data on the Internet; they are thus vulnerable to attack.

From the prior discussion, it can be concluded that the main source of threat on the civil discourse of cyber security in Indonesia is the citizen; the people element. Also, the most vulnerable part of the system is the people. These justifications demonstrate the significance and importance of the government policy makers considering cyber security culture of the Indonesian citizens. However, the contemporary policy has not optimally addressed these problems. The policy provides general legal measures to respond any related criminal actions; nonetheless, it has not comprehensively addressed the source of the insecurities. As a result the government tends to take a shortcut policy such as blocking any website or platform, like what happened with Telegram (Beo Da Costa, 2017) and a block ultimatum to Facebook and YouTube (Antara, 2017). This brings into question the adequacy of the current policy development approach.

Furthermore, the theory of Copenhagen’s securitization (See Chapter 2) is helpful to explain the justifications proffered by the rest of respondents on why cyber culture has not been considered optimally in the development of the Indonesian cyber security policy. There are two essential elements of the concept that explain the contemporary circumstance of the cyber security policy of Indonesia, which are the three grammars of cyber securitization and the securitization actor.

First, the three grammars of securitization, which are the hypersecuritization, everyday security practice and technification, have not been used during the process of Indonesia cyber security policy making. Hansen and Niessanbaum argue (2010) that the use of three grammars of securitization is critical because it allows the decision-makers to link the cyber problems that exist in virtual life to real life in an attempt to reflect the urgency of the issue. Moreover, they contend that the hypersecuritization grammar is used by securitization actors to explain the threats and dangerous circumstances, that go beyond the level of normal, to allow the access and use of the ultimate countermeasure. Besides, the use of everyday security practice grammar will link the elements of insecurity scenario to the everyday life of larger people to make hypersecuritization scenarios more
credible. Also, the technification grammar by the cyber technical expert is essential to legitimize the countermeasures taken on the hypersecuritization scenario and in communicating about the significance of its everyday practices with authority to the public. Nonetheless, in contemporary Indonesian cyber security, the absence of cyber culture assessment by experts, as argued by Interviewee 1, the suboptimal role of non government institutions to highlight everyday cyber insecurity life as confirmed by most of the Interviewees, and the non-existence of cyber security concerns in the priority program of the Coordinating Minister for Political, Legal, and Security Affairs (Polkam, 2017), demonstrate the absence of these three securitization grammars.

Second, the cyber securitization actor that is supposed to highlight the impact of cyber security threats to threatened objects is also absent. Dunn-Cavelty (2013) contends that the securitization actor is crucial in bringing about a ‘heterogeneous political manifestation that linked to different threat representations’ that influences the cyber security policy’ (p. 118). In Indonesia, there has not been any cyber securitization actor who could nationally augment the issue of cyber security, especially the cyber culture factor. However, recently the President of Indonesia established the new cyber security organization, the NCCA, which has the authority to coordinate and organize all related cyber security issues and agencies in Indonesia (Ayuwuragil, 2017). Most of the Interviewees put their hopes and beliefs in this new agency to be the future cyber securitization actor. The absence of these two important elements of Copenhagen’s securitization theory shows why the cyber culture of Indonesian citizens has not been optimally considered in the current cyber security policy making. Furthermore, all of the respondents view cyber security culture as the most important factor in cyber security policy. Yet it has not been addressed optimally and therefore, this leads to the conclusion that dealing with the cyber security culture of the Indonesian citizen is urgent.

CONCLUSION

This research was conducted in response to the need for more empirical investigations that focus on examining the gap between the contemporary challenges of the development of the cyber culture of Indonesian citizen and the cyber security policy of Indonesia. To achieve the objective of this research, using Dunn-Cavelty’s civic discourse and three tenets of cyber security this research found the negative impacts of this cyber culture of Indonesian citizen affect the cyber security policy of Indonesia in two ways; (1) it becomes the main source of threat to the contemporary national civic discourse of Indonesian cyber security on the issue of integrity and confidentiality of information, and (2) the Indonesian citizen becomes the most vulnerable element. However, the development of cyber security culture of Indonesian citizen has not been the priority of the government, and by employing the Copenhagen’s Securitization Theory, this research discovered two important elements that explain the contemporary circumstance of the cyber security policy of Indonesia. First, the three grammars of securitization, which are the hypersecuritization, everyday security practice and technification, have not been used in the process of cyber security policy making. Second, there has been no cyber securitization actor, who could amplify the urgency of cyber security in Indonesia. These findings contribute to existing knowledge by providing an initial understanding of the relationship between democracy and cyber culture of Indonesian citizen in addition to providing an empirical analysis of the impact of cyber culture of Indonesian citizen to the cyber security policy of Indonesia. Besides, the current study provides practical implications for the government and non-government stakeholders about the gap between the contemporary challenges of the development of cyber culture of Indonesian citizen and cyber security policy of Indonesia by offering academic analysis on the development of cyber security circumstance in Indonesia and general assessment of the contemporary cyber security policy of Indonesia.
REFERENCES

*International Journal of Computer Applications in Engineering Sciences* Vol. 1 Special Issue on CNS


Interviewee 1. Personal Interview. 12 June 2017
Interviewee 2. Personal Interview. 13 June 2017
Interviewee 3. Personal Interview. 17 June 2017
Interviewee 4. Personal Interview. 15 June 2017
Interviewee 5. Personal Interview. 19 June 2017
Interviewee 6. Personal Interview. 14 June 2017
Interviewee 7. Personal Interview. 7 July 2017


Vacca, JR. (2013). Cyber Security and IT Infrastructure Protection. Waltham: Steven Elliot