MANDALA
Jurnal Hubungan Internasional

Vol.7 No.2
Juli-Desember
2024

Received: September 25, 2024
Accepted: October 25, 2024
Published: November 25, 2024

A BRIEF SKEPTICISM: THE DISCOURSE OF THE COPENHAGEN SCHOOL AND CYBER SECURITY IN INDONESIA

Muhammad Kamil Ghiffary Abdurrahman
FISIP UPN Veteran Jakarta
ghiffaryabdurrahman@upnvj.ac.id

Yosua Saut Marulitua Gultom
FISIP UPN Veteran Jakarta
Yosuagultom187@gmail.com

Abstract

The evidence shown from the last decade shows that Indonesia has been the constant target of cyber attacks, hence, the urgency to respond cyber threats with its according and appropriate response: a more securitized response. The existing literatures, however, have shown that the academic discourse national retaliation against the cyber threat is rarely guided by the Copenhagen School's Securitization Theory, which has established a massive gap on why the the discourse has not been the mainstream approach on tackling Indonesia's national threat on its cyber infrastructures. As a conclusion, the analytical lenses by the Barry Buzan and Ole Waever is strictly adopting concepts to define its own securitization process, but each concepts are still lacking of the depth required to wholefully understand how ideal securitization should and would work. Nonetheless, putting a state's political actor as the securitization actor deemed to be putting too much emphasize as the state as the main national stakeholders, putting the society in an absurd position within the process of securitization.

Keywords: Copenhagen School, Cyber securitization, Indonesia, Securitization.

Introduction

Cybersecurity issues in Indonesia seem like a knot that refuses to untangle. Cited from the Kaspersky report, a stakeholder of Indonesia's Communication and Informatics Ministry, Budi Arie, stated that Indonesia ranks 10th as a country that is most often targeted by cyberattacks (Abdurrahman, 2024). Some of the latest prominent examples of cyberattacks in Indonesia are the hacking of e-commerce platforms (Tokopedia, Bukalapak, and Bhinneka) and Data COVID-19 in 2020 (CNN Indonesia, 2020) to the more commonly known Bjorka case (CNN Indonesia, 2022) and the hacking of Indonesia's National Data Center (*Pusat Data Nasional Indonesia*) which caused multi-sectoral impacts on Indonesia's digital data, including the paralysis of several public services (Saptowalyono, 2024).

Many commentaries suggested that the looming problem of Indonesia's cyber concern is turning into a real, threatening national issues because of several apparent reasons, namely problematic approach on cybersecurity policymaking and overlapping jurisdictions from governmental institutions (Chen, 2022; Widianto et al., 2024; Priyandita, 2024, p. 4); the lost focus on addressing 'human error' by not establishing 'zero-trust architecture' on national cyber domain (Ikeda, 2024);the low-level of awareness from the level of national stakeholders (Priyandita, 2024, p. 3); and the reliance on regulations and legislations instead of overarching law of in cyberspace (2024, p. 4). These aforementioned explanations bring us to a further understanding that we can expect this cyberspace issue to emerge thus creating a nexus with the discourse of security studies, especially within the study of International Relations (IR).

As an academic discipline, IR is also generally concerned with security-themed issues. Rooted from the very first start, the contemporary discourse about security in IR was predominantly started after WW2 and during The Cold War, with an IR theory tagged as 'neorealism' as its mainstream theoretical framework of understanding.

The neorealist tries to move on from its previous foundation of thoughts of 'classical realism' that perceives states–that often semiotically represented by the use of the word 'men'–to have limitless desire for power without any overarching authority to govern over their 'egoistic behavior' (Walt, 2017: 3-4). Neorealists, such as Kenneth Waltz, does not necessarily reject the whole picture, but instead of putting the weight of morality towards men and their birth-by-right 'nature' of endless desire of power, he insisted that there is a better explanation

concerning security problems by exploring the structure of the international system: a view that's more rational and scientific than putting the spotlight exclusively to the egoistic, 'biological' power-thirsty behavior of men.

In short, Kenneth Waltz argues that international affairs concerning security is the natural consequences of anarchy as the ordering principle within an international structure: it shapes and shoves the states as the constituents of the structure to behave rationally so they can survive, or else (Waltz, 1979; Keohane, 1986: 343; and Buzan, 1983).

Still within the same discourse of security studies, neorealists argued that states are the only sovereign actors in the international system. It is logical to establish this argument since this view developed mainly in the middle of the 20th century, where world conflicts and security crises were predominantly initiated by state actors. Consequently, it is also logical *if* many neorealists are not on the same page towards the growing discourse of security that implies the concern of security is not limited by the domain of states and military, since the unit of analysis of neorealists are *almost exclusively on the power structure at the system and unit leve*l (Buzan et al., 1998, p. 11), therefore may not putting many security concerns on the other lower levels of analysis.

Most neorealists put the 'security' concern at the structure (*system level*) as the the source of the explanation, and its impact on the state actors (units level) with their '*self-help'* approach as the source of the outcome; but for a constructivist like Barry Buzan the view concerning 'security' is not limited only on those level of analysis but it continues towards a lower, more specific level: *subunits* (organized group of individuals) and *individuals* (the 'bottom line' of object analysis in social sciences) (p. 7).

To bring the issue of security more contextually approved in this modern day and ages, the debate of "Wide" versus "Narrow" concerning the Security Studies summarized by Buzan captured the perfect path on how the next discussion regarding this topic should continue: by moving on beyond traditionalist view of security complex theory.

> *Our solution comes down on the side of the wideners in terms of keeping the security agenda open to many different types of threats. We argue against the view that the core of security studies is war and force and that other issues are relevant only if they relate to war and force* (p.4)

The constructivist paradigm pulled into the table here then brings back the aspects of domestic politics to explain the actions of the state, as it was explained by Buzan et al, that security is '*something much more specific than just any threa*t' (p. 6). The conceptualization of securitization in this paradigm is crucial in understanding how states define and respond to threats.

Buzan therefore 'recapture' the term of securitization as the reconstruction of security threats, where it can exist within the domain of military or nonmilitary, strictly political, and staged as an 'existential threat' towards a referent object. Securitization theory argues that threats are not objective realities, but are socially constructed through discourse and political action, turning various issues into security concerns (Rosyidin, 2022).

Talking on a more specific issue of cybersecurity issues, one can argue that the discord of Indonesia's securitization towards cyber threats is still deep within the fog of arbitrary. Whereas there is a general understanding that cyberspace and other ICT domains can manifest into a threat vis-a-vis Indonesia's national interest and its societal order (Setiadi et al., 2012; Aulianisa S & Indirwan, 2020; Rizal & Yani, 2016), the general theme of research is standing on the same bridge that cybersecurity process in Indonesia, however, is thwarted because of many different vindications, namely: (1) unprepared socio-politics of Indonesia towards cyber threats (Pratiwi et al., 2023), (2) minimum technical and non-technical preparation (Febriawan & Marisa, 2024), and (3) the disunion of the state's executive, legislative, and judiciary branches (Martupa & Hartanto, 2023).

Nevertheless, few also note that there have been some efforts by Indonesia to tackle the crack in the foundation of its cyber safety: for starters, (1) by engaging all of its possible international branches of diplomacy and multilateral collaborations (Fransiska & Tobing, 2023; and Iswardhana, 2021), (2) by regulating the digital domain by adopting the Law on Electronic Transaction and Information (UU ITE) and The Law on The Security of Personal Data (UU PDP) (Saleh & Winata, 2023); and (3) by institutionalizing cyber regulator to National Cyber and Crypto Agency (BSSN) (Mulyadi & Rahayu, 2018).

This article, therefore, will try to emphasize on the puzzle pieces into the discourse of securitization of cyber in Indonesia by questioning why the theoretical discourse of securitization established and formulated by the Copenhagen School has not been the mainstream analytical lenses concerning

cyber security in Indonesia. By this question, we would like to descriptively review the modern understanding of Copenhagen School, specifically concerning the issue of cyber security.

The Debate Concerning Securitization

By not discrediting any findings from the previous studies revoking the knot in the head of cybersecurity, this article finds that the debate concerning Indonesia and its cybersecurity efforts has not put 'securitization theory' into the spotlight. While in contrast, securitization theory is important to help us identify the 'which is which' within the discord of cybersecurity in security studies.

As was once perfectly summarized by Cavelty and Egloff in their writing concerning the domain of security and ICT (2021), any analysis in security studies involving cybersecurity has to be generally rooted in the "Copenhagen School," which mainly implied that the one perception of security is not given by nature and by birth: it is about the construction and the formulation of political agendas and ideas that manifest into a security issue once a threat vis-a-vis national security and interest has been identified, presented, and established (Buzan et al., 1998), thus more importantly, done by the governing actors, political officials alike, a state actor, or non-state actors in the international system (Hansen, 2006).

The process of 'identification and presentation' of the securitized issue can be done by using language as a performative act, highlighting the path on the map that 'speech of acts' is crucial during a securitization process. Inspired by the works of John L. Austin's (1962) and John Searle's (1969) regarding the Speech of Acts theory, Maciej Stępka (2022) then synthesizes that 'political statements,' regardless of whether they are right or wrong, will always contain a message that tries to initiate, institutionalize, or instigate 'new reality' into the society: to change a society's perception from a non-political issue–if possible–into a life-threatening one; hence the justification of its securitization efforts. In short, securitization is important to use to address the act of securitization of a state towards certain identified threats.

The gap of this article's research will therefore be summarized and explained in this passage. Based on the public observations and many cyber threat cases in 2024, experts and many commentators alike have agreed that Indonesia should seek better stones to break their deadlock of cybersecurity. The response and the policies are there; but both are deemed to be not enough. The empirical standpoint,

therefore, strongly suggests that Indonesia has serious problems to address the vulnerability of its cyber infrastructure.

Reflecting on the existing literature, the discourse of 'cyber security' is there, even with a general understanding that the problems of cyber incidents can snowball into national security concerns. There are many perspectives used to understand the reason for the national fragility in its cyber infrastructure, namely socio-politics, technical standpoints, and the thwarted bureaucracy.

This article also finds that much previous literature provides policy briefs regarding help Indonesia address this issue, by utilizing unique standpoints such as institutionalization of cyber threats, diplomacy, and multilateral collaborations, and by establishing overarching law over cyberspace in Indonesia. These collective agreements taken from the existing research and articles, however, does not necessarily utilize the Copenhagen's School approach of securitization as its lens of understanding.

Understanding that '*figure or speech*' is an important object of analysis in the study of securitization, this research uses qualitative-explanative methods, thus putting more emphasis on any form of verbal as the '*speech of act*' made by Indonesian's executive, important political figures, ministerial stakeholders, and other printed documents like its form. One can hypothesize that by manifesting securitization theory by Barry Buzan as the theoretical framework, the '*endless-wait*' of cyber-securitization in Indonesia is caused by the thwarted first process of securitization, proven by the unclear securitizing actors that initiates the call and movement of national cyber securitization. This early stage is particularly important for a securitization to occur since the identification of the threats and the referent objects that need to be protected will only be addressed by the securitizing actor.

The Gap Between

The principal objective of the studies done by the Copenhagen School and its development and critics so far are for nothing but to provide a clear guideline to study securitization. While generally it has been utilized as the mainstream framework of analysis in contemporary security studies, the Securitization Theory was deemed to be limited in its concepts, hence, the limitation to be utilized as the main 'real-world' security analysis framework (Stritzel, 2007), and is still very open to different interpretations, angles, and even critics (2014, p. 11-12).

Stritzel confronted the main issue by radically separating the work Securitization

into two separate thoughts of philosophical understanding: (1) a realist understanding towards the conceptualization of 'security', and (2) poststructuralist understanding that views speech to act as a security (p. 13). This view to address the definition towards 'what is security', is essentially about a 'negotiation' between the speaker and the audience, between a political actor and its society; a 'negotiation' so the people will adhere the efforts needed to do against the existential threat (Buzan et al., 1998).

Unsatisfied by this definition, Stritzler points out that this framework of thinking made by the Copenhagen School has reflected what the moderate realist like Arnold Wolfers had previously written in his book called *National Security as an Ambiguous Symbol* in 1952, where ultimately Wolfers believed about two things relevant to this issue: (1) Government as the decision makers are able to determine which value [referent object] which deserved to be securitized, including its level of emergency, the efforts, and the required resources (Wolfers, 1952, p. 502 in Stritzel, 2014, p. 13), and (2) the people [audience] followed by giving their approval for the political actor to use any means necessary since they have to experience the 'sheer discomfort' out of the securitization processes (Wolfers, 1952, p. 487-488 in Stritzel, 2014, p. 14).

Wolfer strongly disagrees, however, that the nation–or to what the Copenhagen School conceptualized it as the 'political actor'–is in the superior position in contrast to its people, a radical *regione di stato*: a position where nations 'completely subordinate' everything for the sake of what the political actor have perceived about their security.

Moreover, Stritzel also highlighted that the attempts made by the Copenhagen School to define securitization as the creation of '*intersubjective understanding made by political community to justify its exceptional security measures*' (2007, p. 358) was too focusing on the *'single security articulation at a particular point in time*' (p. 377), hence, causing contradiction against its own '*triology'* of concepts between speech of act, securitizing actor, and the audience in the theory of securitization.

By still adhering to the principle of the theory, Stritzel asked for a more systematic and clearer emphasis of concepts embedded within Securitization Theory by adding more comprehensive and detailed definition towards its layer of concepts: (1) *the performative force of an articulated text, (2) its embeddedness in existing discourses, and (3) the positional power of securitizing actors.*

Conclusion

This brief article is trying to descriptively showcase why the discourse cyber securitization in Indonesia has not been the mainstream theme throughout the field of security studies. By utilizing Strizel views as an alternative to observe how securitization theory works, the analytical lenses introduced by Barry Buzan and Ole Waever is deemed to be too simplifying the underlying concepts underneath the securitization theory itself. In short, the theory needs a lot of criticism to help it rebuilds and remanifests its relevancy with the growing and developing global political affairs.

Generally, the effort done by the Copenhagen School on understanding how securitization works are distributed into three different 'basic' concepts of (1) securitizing actor; (2) a speech of act; and (3) an audience. Within these three seems to be like simple concepts, with the true intentions were which to help us identify a process of securitization, were deemed to simplistic to its meaning.

The first concept of 'speech of act' for starter, requires further questioning whether the 'performative act' must be centered around the leading, nation-wide political figure or the other way around. Barry and Buzan seems to be putting the focus and the weight down to a singular political figure, which in Indonesia, a stakeholder in the cyber security is not single-handedly managed and overseered.

This writing also wants to mention that the approach of how Copenhagen School is trying to emphasize more on the subjective interpretation of a state on understanding threat—which can also be interpretated by a few figures of people as a state stakeholder—is establishing a huge question whether the view of the people should be as important as the perception of the state's securitizing actors.

This interpretation that solely relies on how the state perceives the threat has created a great distance with its society, therefore creating more question with its theoretical relevancy to a society that adopts liberal democracy; where the system works from the people, for the people, and by the people. This criticism falls into my conclusion why securitization theory has been a less mainstream framework to use in Indonesia's cyber security: it put less attention to its people, yet put heavy expectations to the political actors.

References

Aulianisa Sarah, & Indirwan. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in

Indonesia. *lex Scientia Law Review*, *Vol 4*(No 1), 31-45. https://doi.org/10.15294/lesrev.v4i1.38197

Austin, J. K. (1962). *How To Do Things With Words*. Oxford University Press. https://pure.mpg.de/rest/items/item_2271128_3/component/file_2271430/content

Buzan, B. (1983). *People, States, and Fear: The National Security Problem in International Relations*. University of North Carolina Press.

Buzan, B., Wæver, O., & Wilde, J. d. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Pub.

Cavelty, M. D. (2022). Cybersecurity between hypersecuritization and technological routine. In E. Tikk (Ed.), *Routledge Handbook of International Cybersecurity* (pp. 11-21). Routledge, Chapman & Hall, Incorporated. https://www.routledge.com/Routledge-Handbook-of-International-Cybersecurity/Tikk-Kerttunen/p/book/9781032400709?srsltid=AfmBOormdQkgudQBxBaYya2S_bEK6izULfm7Oshxw81li8KIbsBUZp4f

Cavelty, M. D., & Egloff, F. J. (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. *Swiss Political Science Review*, *Vol. 27*(No. 1), 139-149. https://onlinelibrary.wiley.com/doi/pdf/10.1111/spsr.12433

Chen, E. (2022, June 30). *As Cyber Threats Grow, Indonesia's Data Protection Efforts Are Falling Short*. The Diplomat. Retrieved October 17, 2024, from https://thediplomat.com/2022/06/as-cyber-threats-grow-indonesias-data-protection-efforts-are-falling-short/

Febriawan, D., & Marisa, H. (2024). Understanding Indonesia's Cyber Security Policies: Opportunities and Challenges In The Digitalization Transformation Era. *Journal of Election and Leadership*, *Vol. 5*(No. 1), 13-21. https://doi.org/10.31849/joels.v5i1.15908

Fransiska, F. B., & Tobing, F. B. (2023, June). Securing Indonesia Cyber Space: Strategies for Cyber Security in the Digital Era. *Jurnal Studi Sosial dan Politik (JSSP)*, *Vol. 7*(No. 1), 50-62. https://openrecruitment.radenfatah.ac.id/index.php/jssp/article/view/15925/5958

Hansen, L. (2006). *Security as Practice: Discourse Analysis and the Bosnian War*. Routledge. https://www.routledge.com/Security-as-Practice-Discourse-Analysis-and-the-Bosnian-War/Hansen/p/book/9780415335751?srsltid=AfmBOoqwRF9D4htuA6K1ROtE8wa0IQr7wvZPZVy23lCUU0THDZ8vX0YW

Ikeda, S. (2024, June 27). *Indonesian National Data Center Hit by Cyber Attack, Disrupting Government Services*. CPO Magazine. Retrieved October 17, 2024, from https://www.cpomagazine.com/cyber-security/indonesian-national-data-center-hit-by-cyber-attack-disrupting-government-services/

Iswardhana, M. R. (2021, December). Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia. *Journal of Islamic World and Politics, Vol. 5*(No. 2). https://journal.umy.ac.id/index.php/jiwp/article/view/12242

Keohane, R. O. (1986). *Neorealism and Its Critics* (R. O. Keohane, Ed.). Columbia University Press.

Martupa, A. E., & Hartanto, B. (2023). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development, Vol. 2*(No. 4), 143-152. https://doi.org/10.46336/ijbesd.v2i4.170

Mulyadi, & Rahayu, D. (2018). Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN). *2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia*, 1-6. 10.1109/CITSM.2018.8674265.

Pratiwi, F. I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D. Y., Dewi, C. S., & Intan, A. A. (2023). Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. *Perspectives on Global Development and Technology, Vol. 22*(No. 3-4), 239-264. https://scholar.unair.ac.id/en/publications/cybersecurity-challenges-in-indonesia-threat-and-responses-analys

Priyandita, G. (2024, February 12). *Indonesia's Cybersecurity Woes: Reflections for the Next Goverment*. CSIS Commentaries. https://s3-csis-

web.s3.ap-southeast-1.amazonaws.com/doc/CSIS_Commentaries_CSISCOM00624.pdf?download=1

Rizal, M., & Yani, Y. M. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies, Vol. 4*(No. 1), 61-78. https://d1wqtxts1xzle7.cloudfront.net/68544704/ssoar-jas-2016-1-rizal_et_al-Cybersecurity_policy_and_its_implementation-libre.pdf?1628019560=&response-content-disposition=inline%3B+filename%3DCybersecurity_Policy_and_Its_Implementat.pdf&Expires=1728549517&

Saleh, A. I., & Winata, M. D. (2023). Indonesia's Cyber Security Strategy: Problems and Challenges. *Proceedings of the International Joint Conference on Arts and Humanities 2023 (IJCAH 2023)*, 1675-1693. 10.2991/978-2-38476-152-4_169

Searle, J. R. (1969). *Speech Acts: An Essay in the Philosophy of Language*. Cambridge University Press. https://www.cambridge.org/core/books/speech-acts/D2D7B03E472C8A390ED60B86E08640E7

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). An Overview of the Development Indonesia National Cyber Security. *International Journal of Information Technology & Computer Science, Volume 6*(Issue on November / December , 2012), 106-114. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=225621ba915d4d5b95acf33ef2655f6aace9d669

Stępka, M. (2022). *Identifying Security Logics in the EU Policy Discourse: The "Migration Crisis" and the EU*. Springer International Publishing. https://doi.org/10.1007/978-3-030-93035-6_2

Stritzel, H. (2007). Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relation, Volume 13*(Issue 3), 357-383. https://doi.org/10.1177/1354066107080128

Stritzel, H. (2014). *Securitization Theory and the Localization of Threat* (1st ed.). Palgrave Macmillan London. https://doi.org/10.1057/9781137307576

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill. https://books.google.co.id/books/about/Theory_of_International_Politics.html?id=j6qOAAAAMAAJ&redir_esc=y

Widianto, S., Teresia, A., Mair, J., & Russell, R. (2024, June 24). *Cyber attack compromised Indonesia data centre, ransom sought*. Reuters. Retrieved October 17, 2024, from https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/

Wolfers, A. (1952). National Security as an Ambiguous Symbol. *Political Science Quarterly*, *Volume 67*(Number 4), 481-502. https://doi.org/10.2307/2145138