RUDN Journal of Studies in Literature and Journalism
Вестник РУДН. Серия: Литературоведение. Журналистика
ISSN 2312-9220 (Print); ISSN 2312-9247 (Online)
2025 Vol. 30 No. 1 186–198
http://journals.rudn.ru/literary-criticism

DOI: 10.22363/2312-9220-2025-30-1-186-198
EDN: URUQPH
UDC 004.738.5:070

Научная статья / Research article

Enduring Cybersecurity and Transitional Justice Aftermath of West Papua and Papua's Internet Shutdown in 2019

Adelisca Pramesti[1] ✉, Hikmat Z. Almubaroq[1], Aloysia V. Herawati[2], Bella A. Bulgarova[3,4]

[1] *The Republic of Indonesia Defense University, Jakarta, Indonesia*
[2] *University of Surabaya, Surabaya, Indonesia*
[3] *RUDN University, Moscow, Russian Federation*
[4] *Alnoor University, Mosul, Republic of Iraq*
✉ pramesti.adelisca@gmail.com

Abstract. The Internet shutdown in West Papua and Papua, in 2019 as an example of the Ministry of Communications and Informatics of the Republic of Indonesia failure to balance national security and digital freedoms. The Internet shutdown was suppress and control the flow of information has been criticized as an authoritarian strategy that undermines human rights and digital freedoms, further deepening mistrust between the state and citizens. The Ministry needs to refrain from abusing their powers and ensure that cybersecurity regulations do not violate civil liberties, as excessive restrictions weaken democratic values. Emphasized the Ministry's failure to comply with cybersecurity standards, which has led to human rights violations and manipulation of perceptions of national security, ultimately damaging Indonesia's reputation. Finally, the article highlights the value of long-term relationships in transitional justice, justifying the need for a human-centered approach to institutional transformation within the framework of national cybersecurity initiatives. This article highlights the importance of transparency, accountability, and the protection in preventing future abuses. This article calls for a reevaluation of cybersecurity practices for digital freedoms, emphasizing the necessity of transparent and inclusive policies that reflect democratic principles.

Keywords: media, human rights, digital freedom, Indonesia, communication, cybersecurity standards, mediasafety

Conflicts of interest. The authors declare that there is no conflict of interest.

Authors' contribution. Development of the research concept, data collection and analysis, manuscript writing – Adelisca Pramesti; development of the research concept, research data collection and analysis – Hikmat Z. Almubaroq; data collection and analysis, manuscript writing – Aloysia V. Herawati; data analysis, manuscript editing – Bella A. Bulgarova.

Article history: submitted August 31, 2024; revised October 19, 2024; accepted December 29, 2024.

For citation: Pramesti, A., Almubaroq, H.Z., Herawati, A.V., & Bulgarova, B.A. (2025). Enduring Cybersecurity and Transitional Justice: Aftermath of West Papua and Papua's Internet Shutdown in 2019. *RUDN Journal of Studies in Literature and Journalism*, *30*(1), 186–198. http://doi.org/ 10.22363/2312-9220-2025-30-1-186-198

Обеспечение кибербезопасности и правосудия переходного периода после отключения интернета в Западном Папуа – Новой Гвинее в 2019 году

А. Прамешти[1]✉, Х.З. Альмубарок[1], А.В. Херавати[2], Б.А. Булгарова[3,4]

[1] *Университет обороны, Джакарта, Индонезия*
[2] *Университет Сурабая, Сурабая, Индонезия*
[3] *Российский университет дружбы народов, Москва, Россия*
[4] *Университет Альнур, Мосул, Ирак*
✉ pramesti.adelisca@gmail.com

Аннотация. Отключение интернета в Западном Папуа и Новой Гвинее рассматривается как пример неспособности министерства связи и информатизации Республики Индонезия сбалансировать национальную безопасность и цифровые свободы. Отключение интернета подверглось критике как авторитарная стратегия, которая подрывает права человека и цифровые свободы, создавая и углубляя недоверие между государством и гражданами. Государству (в данном случае министерству) необходимо воздержаться от злоупотребления своими полномочиями и гарантировать, что правила кибербезопасности не нарушат гражданские свободы, поскольку чрезмерные ограничения ослабляют демократические ценности. Показывается несоблюдение государством (министерством) стандартов кибербезопасности, что привело к нарушениям прав человека и манипулированию восприятием национальной безопасности, а в конечном итоге нанесло ущерб репутации Индонезии. Подчеркивается ценность долгосрочных отношений в переходном правосудии, обосновывается необходимость подхода, ориентированного на человека, институциональной трансформации в рамках национальных инициатив по кибербезопасности, важность прозрачности, подотчетности и защиты в предотвращении будущих злоупотреблений. Авторы призывают к переоценке практик кибербезопасности для цифровых свобод, указывая на необходимость прозрачной и инклюзивной политики, отражающей демократические принципы.

Ключевые слова: СМИ, права человека, цифровая свобода, Индонезия, коммуникация, стандарты кибербезопасности, медиабезопасность

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов. Разработка концепции исследования, сбор и анализ данных, написание рукописи – А. Прамешти; разработка концепции исследования, сбор и анализ материалов – Х.З. Альмубарок; сбор и анализ материала, написание рукописи – А.В. Херавати; анализ материала, редактирование рукописи – Б.А. Булгарова.

История статьи: поступила в редакцию 31 августа 2024 г.; отрецензирована 19 октября 2024 г.; принята к публикации 29 декабря 2024 г.

Для цитирования: *Pramesti A., Almubaroq H.Z., Herawati A.V., Bulgarova B.A.* Enduring cybersecurity and transitional justice: Aftermath of West Papua and Papua's Internet shutdown in 2019 // Вестник Российского университета дружбы народов. Серия: Литературоведение. Журналистика. 2025. Т. 30. № 1. С. 186–198. http://doi.org/10.22363/2312-9220-2025-30-1-186-198

Introduction

In the current situation, Indonesia still lacks knowledge about integrating closely between cybersecurity and transitional justice to eliminate conflict spreads. Thus, security system reform aims to change state institutions serve the public, and act with integrity. The importance of sustainable footpaths as stable turmoil reconciliation in society. Then proposition innovation is well prepared for the future. Cybersecurity should as a lesson for ensuring human rights protection. Security and defense affairs have been crucial national problems, and are part of the disturbance source of human rights welfare. These sectors impact national welfare, especially the national security and human security dimension.

First, the relationship with national security is serving as a service in government and people towards information-communication technology infrastructures (ICT) to be used or operationalized. Moreover, the existence of services would be in a policy and enactment as a law supremacy for handling digital public order. Second, the relationship with human security is usually connected with civil liberties needs, which means aiming to prevent and reduce digital harmfulness. In those approaches, cybersecurity could be a concern with micro prosperity, especially toward citizens having rights to embody access freedom, and empowerment from digital threats. Carries out from two dimensions, security and defense affairs are closely within the cybersecurity system. Those pivotal sectors impact the region and people's life sustainability development.

Cybersecurity would be a pivotal human-centric—and also prevent state-centric risk effects inside of overlapped policy and power used. According to the duo-edge sword preposition, brings dysfunctional problems to cybersecurity. In principally, the duo-edge sword preposition should be delicately integrated and consensus to other potential aspects, especially human-centric. As a democratic country, openness, fairness, and greater protection are benchmarks of a government system to achieve effective people's political will. The declaration of the United Nations Human Rights Council about cybersecurity in July 2012 committed to the availability of the same protection rights for people in offline and online environments (Liaropoulos, 2015, p. 19). Thus, cybersecurity is more drive broadly handled by private, national, or global domains in the ability to responsibly, integrity, and humanity on ICT's infrastructure prosperity.

On the other hand, cybersecurity is used as an allegation of human rights abuses within malpractice. Internet shutdowns are a tool for generating an information void that authoritarian regimes can take advantage of by aggressively terminating (Thumfart, 2024, p. 3). The aftermath in West Papua and Papua in 2019 was evidence of the government's failure in cybersecurity operations. The government's disease today is a lack of awareness of to rebuilding of cybersecurity aspects. The source of conflict was misperception about disrespect and complicated because of persecution, terror, and discrimination against Papua students. Afterward, the escalating information about the incident was tightened. In response to the information tension, the Ministry of Communications and Informatics of the Republic of Indonesia terminated the Internet to prevent the spread of misinformation. The Ministry of Communications and Informatics of the Republic of Indonesia did not briefly present cybersecurity and transitional justice as national security strategies as a non-military aspect. This article proposes prominent principles and approaches in formulating structures managing to force modernization of national security in systemic policies prosperity.

Analysis Framework

The types of constitute analysis in this article are provided to describe the reflective malpractice in cybersecurity force in West Papua and Papua toward other countries. It also describes the gridlock of power abuse and surveillance, and it details overlapping institutional authority and accountability interests. In results and discussion, the section examines the enduring transnational justice connectivity post-conflict within institutional reform figures. In conclusion, this article has the recommendation to examine chapter highlights and persuasive scholars that could drive more cybersecurity as digital products should support and adhere engagement to national humanity's welfare development.

This article's aim has resulted in securitization incompetent framework for terminating the imperishable conflict. If this incompetent matter is never solved with swift steps, both civilian and military troops will always be victims targeted by government ego and ambition. The proliferation and termination of the counterinsurgency through an autonomous enactment only temporarily solved the problems. It is because of the aim of terminating only to cease spreading the escalating of the separatism movement. Those autonomous enactments could be giving frustrated separatism is broadly sporadic. This national security catastrophe should concern the securitization process as defense forces are competent, mostly reducing lingering weaponized tension and rapidly violence-abuses victims.

Materials and Methods

This article is based on research that uses a Systematic Literature Review (SLR) methodology, which is to discover empirical findings of pre-specified inclusion criteria and future studies to answer particular research questions (Snyder, 2019, p. 334–335). It aims to assemble, compare, and examine the documents and scientific articles. Those two steps belong to the empirical findings to be found and accordingly in The security sector, and Institutional and democracy. Accordingly, this article's methodology aims findings renewable empirical research (table) highlights an inventory in conducting, and mainly provides four systematic literature reviews.

Table

Inventory of systematic literature review approach by author (2024)

Divisions	Authors	Discipline	Type of Literature Review	Key Contribution
Legal Studies	Putusan PTUN JAKARTA Nomor 230/G/TF/2019/ PTUN.JKT	Beschikking (Written Determination)	Review papers and systematic review	1. Defines a lawsuit. 2. Provides guidelines for law review
Cybersecurity and Defense	Ryng et al. (2023)	National and international defense	Systematic review	1. Provides an overview of cybersecurity studies with cross-country comparisons. 2. Discusses common cybersecurity risk problems
Interdisciplinary Social Studies	Antony Lee (2020)	Social sciences and humanities	Systematic review and meta-analysis	1. Provides numerical evidence of problem research. 2. Examines challenges associated with the triumvirate research approach
Transitional Justice and Policy	Aulund, & Levorsen (2012)	Social sciences and humanities	Systematic review	1. Defines transitional justice. 2. Offers recommendations within MoU agreements and the TRC approach

Illustrated and developed by the researcher (2024)

This article uses a systemic literature review as the primary method. Gathering secondary data from government publications, such as legal-formal sources, policy papers, and official statements. Moreover, within gathering the data addendum, this article contributes to mitigating of malpractice of cybersecurity and could give a policy ambiguity towards human rights sovereignty. It could be emphasized to resolve counterinsurgency proliferation in the Papua conflict. Admittedly, security fundamentals must be representative of human-centric. This article proposes to save the integrity of cybersecurity by protecting national security. With a greater focus on merits analysis on legitimacy freedom and eliminating abusive power.

Results and Discussion

Identification of Reflective Malpractice in Cybersecurity

The concept of cybersecurity needs to be specifically centered on non-military dimensions. This article approaches cybersecurity through a historical lens, examining its definitions within the framework of national security. It positions cybersecurity as a component of sovereign and defense protection. It is argued that the definition of cybersecurity should be prioritized as a national security defense.

Cybersecurity is more complicated with differences in legal, facets, and legislative analyses. Complications are more ruined by only focusing on defining and solving cybersecurity issues within cyber threat actors, such as terrorists, criminals, hackers, and nation-states. It should reflect different varieties of cyber threats, such as critical infrastructure that could lead to life, economic damage, and intellectual property, which could as a nation's long-term competitiveness (Lowrie, 2015, p. 203–204).

Some significant research findings are that Indonesia used Law Number 11 of 2008 on Electronic Information and Transactions on the Internet Shutdown through The Ministry of Communication and Informatics and Presidential Office Staff. The government claimed that demonstrations and riot waves made emergency varieties of misinformation news spread, national security instability, and economic backlash in many districts and cities of West Papua and Papua (Hadi et al., 2021). The effects of that strategy will trigger explosive riots political mobilization, and economic disturbance. As a result, the Internet on ICT infrastructures could spread frustrated the disrupted society that had potentially built duo-edge swords within government over power control justified as an autonomous weapon, which is under-addressed in handling national security problems.

Identification of the Gridlock Between Abuse of Power and Surveillance

The Internet shutdown did not do democracy enforcement, including disadvantage protection in technological communication and significant growth. It is an especially filter-bubble narrative inside digital censorship laws toward filtering fake information to the next level but found in physical apparatus – abuse of power – violations in blackouts infrastructure (De Gregorio, & Stremlau, 2020; Shah, 2021). Many perceptions are still overwhelmed by an exponential scale of fake information distributions, "shared by uncritical publics" (Ireton, & Posetti, 2018, p. 15). The West Papua and Papua Internet Shutdown in 2019 has already started immobilizing national insecurity with cybersecurity malpractice, which terminated ICT infrastructure. On the other hand, the Internet shutdown precisely escalated people's overwhelming feelings of anger and distrust toward the government. Ministry of Communications and Informatics of the Republic of Indonesia, as a government representative responsible for terminating the ICT infrastructure, was fatally handling policy and service. Tragically in this problem, malpractice was more complicated in the cybersecurity aspect too, in favor of recovery and growth of peacekeeping operations and also potential continuing national security and human security destruction.

First, the Ministry of Communications and Informatics of the Republic of Indonesia used cybersecurity as an autonomous weapon in chaotic situations during the Internet shutdown. Cybersecurity has been sabotaged and manipulated to cover political chaos and immobilization under national security matters. The government system through the Ministry of Communications and Informatics of the Republic of Indonesia wanted to prevent and mobilize disturbances instantly coming after the effects of civilians protesting waves. It could essentially lose accountability through sabotage and manipulated methods. Those methods can repress digital community and communicative interactions – ICT infrastructure, also it has illiberal interferences to covered protection under autonomous weapons to slash freedom of expression and privacy on the technologies side (Glasius, & Michaelsen, 2018; Wagner, 2018). These kinds of sabotage and manipulated effects not only spread chaos and mobilization of those disturbance national security matters by the Ministry of Communications and Informatics of the Republic of Indonesia but also limited the development of democracy access and processes as usual in authoritarian regimes.

Second, the government through the Ministry of Communications and Informatics of the Republic of Indonesia – or other ministries – was only focused, ambitious, and concerned without acknowledging diagnosis and solving within brilliant national security policy toward the counterinsurgency's reconciliation as transformational handled roots affairs. Conversely, the Ministry of Communications and Informatics of the Republic of Indonesia chose another option, the Internet shutdown, which brought a setback in government institutions to reduce democracy enforcement through restrained accessing Internet connectivity under authoritative and authorized peacekeeping ICT infrastructure distribution development.

Ministry of Communications and Informatics of the Republic of Indonesia did Internet shutdowns won't stop the flow of misinformation news or block resources, but only delay the control of information traffic based on deliberate government instructions. Eventually, it will widespread destruction to other national security sectors, and threats to intellectual property, which could affect our nation's long-term competitiveness. However, the malpractice of Internet shutdown as a new weapon model is creating digital mass killings within terminated ICT infrastructure under singular control. The Internet shutdown is usually adopted in authoritarian regimes to control and limit civilian security using ICT infrastructure – as a digital freedom – to demands of government cooptation which causes national human insecurity. Especially in this problem, the Ministry of Communications and Informatics of the Republic of Indonesia responsibility used a very uncommon standard – Internet shutdown – in the democratic government system, but this happened as a common to repulse misinformation news.

Identification of Enduring Connectivity in Transitional Justice

Internet Shutdown affairs as a sense of cybersecurity emergency issues could be a weapon regime to curb a threat, meanwhile protecting cover contrary debate and democracy procedures (Ryng et al., 2022). The dual-use dilemma, cybersecurity as a weapon provides effectors to components – ICTs and society – for doing the killing, destruction, the delivery vehicles – drone warfare – the launcher to the destination or into range (Riebe, & Reuter, 2019). This overlapping nagging felt confusing in describing the purposes of impact, advantages, and hidden harm in a wide range. It means the items, knowledge, and technology have various beneficial, also harmful applications (Riebe, & Reuter, 2019). Regarding those cybersecurity ambiguity problems is a dual-use dilemma within the Internet Shutdowns affair as an autonomous weapon in West Papua and Papua.

The court's decision, documented in the *Decision of Administrative Court Jakarta* Number 230/G/TF/2019/PTUN.JKT that the access was cut off in 4 cities/regencies in Papua province (Jayapura City, Jayapura District, Mimika District, and Jayawijaya District) and 2 cities/regencies in West Papua province (Manokwari City and Sorong City), and as well, the access was cut on September 4, 2019, at 23.00 WIT until September 9, 2019, at 18.00/20.00 WIT. Instead, the government ended up as suspected of violating the 1959 State Emergency Law in The Jakarta Administrative Courts. That response to the national instability, which used Internet Shutdowns is an autonomous weapon to push back a misinformation news spread. It recalls many provoked debates in West Papua and Papua. It still curbs many questions, using a national cybersecurity infrastructure to solve counterinsurgency in West Papua and Papua to over misinformation news tension.

The aim of our government use a cybersecurity strategy to solve those problems, used Internet Shutdown within terminated ICT infrastructure was an instant core to not direct physical attack and damage towards West Papua and Papua. If those dual-use dilemmas in cybersecurity never get attention, it will continue to fear more decreased democracy – liberty and security – regimes. The transitional Justice pattern refers to how reforming, building, and developing efficiency and fairness in public institutions into institutional reform in post-conflict and transitional government to prevent future human rights violations and abuses (Aulund, 2012, p. 25–26). As it is very name suggests, the Transitional Justice pattern could solve the aftermath Internet Shutdown in West and Papua, and provide future national cybersecurity as national security prosperity.

The availability of strengthening the relationship between institutional and infrastructure to tighten up responsible research and innovation as national security anatomy development, especially cybersecurity aim. Cybersecurity and the Ministry of Communications and Informatics of the Republic of Indonesia as other national cyber institutions can be reformed to define cybersecurity functions to prevent overlapping awareness. In essence to reckon post-conflict, restore justice, and reconciliation to stable national security in the future. Especially transitional justice existence now and future should be balanced between political and technical structures for finding and evaluating each other in the truth-seeking process. It should be a focus and help to mobilize public deliberation in the governance system to fulfill the needs and capacity building to endure cybersecurity to respect human rights policy esteem.

Institutional reform must be an agenda of attention after West Papua and Papua in 2019. It namely part of the institutional reform of institutions that have so far committed abuse to transform towards integrity, accountability, and trust towards full rights to give birth to and empower a sovereign society security (Davis, 2012). Therefore, the government system must be learned from West Papua and Papua as counterinsurgency regions. It means doing a bearing within promotes the empowerment of a human-centric approach, an essential commitment to preventing more people or states as a victim or perpetrators from mislead of overlapping interests.

Cybersecurity and human security occupies center priority rights, which means civilians must protected in trust and security during accessing devices and networks towards less differentiation of national security and security of the global Internet[1] (Pavlova, 2020). The importance of an integral component to implement it, must both government and regional partners – the private sector – must have adequate involvement in the mission in the long-term strategies, including a rapid response, so as not to fall too deep into malpractice and national security dysfunction. For instance, needs to urge specific narratives within the formation of a special internal team under the special supervision of the ombudsman, the National Human Rights Commission, and the private cybersecurity-telecommunication companies sector.

So, the overlapping caused by government power control and centralized Internet structure never happened again. Governments and associated institutions may successfully prevent overlapping protection and control power in institutions. Furthermore, could be properly used cybersecurity by following ethical and human rights guidelines to combat misinformation without an Internet Shutdown. Lastly, infringing on people's digital rights by adopting a more inclusive institutional approach grounded on humanity.

Therefore, the transitional justice process through institutional reform requires an effective conflict communication process in negotiations to run optimally. This is done using both parties to the conflict agreeing to carry out a peaceful resolution of the dispute. Determining that holding open negotiations between representatives that take place behind closed doors is more optimal than open negotiations that

[1] Association for Progressive Communications (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity

involve intervention from external parties outside the country and other pressure groups. Although conflict communication is a mechanism that can lead to successful conflict resolution between parties in conflict.

For this reason, it must be responded to positively because it is part of what is capable of initiating future-oriented movements to guide other parties towards the desired targets (Zartman, 2008), one of which is increasing trust in government again. However, for audiences to accept their narratives, the actors must hold authority or be seen as trustworthy to implement securitization involving both government officials and civil society actor's power engagement (Lee, 2020). So, parties in conflict must also play a responsive, responsible, and practical role so that the resolution in managing conflict communication management strategies can analyze the resolution process well in achieving the desired results and mutually agreed decisions. Remember, in a democratic society, anyone can act as a securitizing agent.

The implementation of the Internet shutdown in West Papua and Papua regions is a failure manifestation by the government after facing duo-edge swords between to protect from information news streams and order demonstrations waves. Even though, duo-edge swords as a dilemma turmoil, the Internet shutdown into an autonomous weapon to reduce and prevent more new demonstration waves. Meanwhile, it also seems to intentionally attack ICT infrastructure, likely through digital violations in the destruction of ICT infrastructure within the limit accessing the Internet, slowing down the signal of Internet distributions, and using Indonesia Law Number 11 of 2008 on Electronic Information and Transactions as abusive power occasion. In this article, the author examines three chapters to encourage readers to explore and emphasize West Papua and Papua in 2019 as crucial affairs to restore advancing human rights and digital freedom comprehension to protect national security.

First, the malpractice of cybersecurity in Papua Internet shutdown must be the last overlapping on governance policy decision-making to handling local affairs. Ministry of Communications and Informatics of the Republic of Indonesia as a representative of the government or another government institution must not allow an authoritarian regime to control, abuse, repress, and institutional centralize on Internet flow. Second, the gridlock between power abuse and surveillance explains that the Ministry of Communications and Informatics of the Republic of Indonesia failed to acknowledge the meaning of cybersecurity principles. It showed that the Ministry of Communications and Informatics of the Republic of Indonesia did not undertake accountability and blunders, also spreading catastrophe by attacking people's rights before and after the Internet shutdown. It means had considered as sabotage and manipulation figures to national cybersecurity. Last but not least, enduring connectivity in transitional justice. In this chapter, the author carries out transitional justice on institutional reform to take seriously rebuilding human-centric and government-regional partner approach to the national cybersecurity mission as protect and respect freedom from digital violations, and vice-versa.

Conclusion

The purpose of the national government within security-cyber defense ministries and the private sector could be focused on cooperation engagement to rebuild again aftermath of West Papua and Papua catastrophe on connectivity in transitional justice within a human centric approach. Take example, it will be in enacting legislation, developing risk assessments and policies, imposing regulations and standards, establishing an industrial security operations center, improving critical system resilience, and responding effectively to cyberattacks and incidents. Eventually, people's needs within cybersecurity should be respected and reduce vulnerability to human-centric dimensions, such as freedom from torture, repression, and deprivation.

However, it should also be remembered that the consequences of the Internet shutdown in West Papua and Papua in 2019 did not provide a solution to the human insecurity conflict. In addition, the Ministry of Communication and Information must also carry out cybersecurity accountability as it should and must instill respect and obey human rights. Therefore, academics must explore contemporary conflict studies more curiously, especially cybersecurity, which is an inseparable component of technology in human rights affairs. Now, academics must specifically consider the paradox between the stability of security that is applied and the meaning of security that is seized. Most cybersecurity interventions have the potential to cause repressive conflicts, such as the deadlock between abuse of power and surveillance. This marks a multifaceted paradox in an unhealthy cybersecurity sector and raises the possibility uncontrolled surveillance by the government system that births an authoritarian regime will emerge.

References

Aulund, M.L. (2012). *Transitional justice for Papua: Lessons to be learned from Indonesian experiences?* [Master's thesis in the Theory and Practice of Human Rights]. University of Oslo. https://www.duo.uio.no/handle/10852/34051

Davis, L. (2009). *Transitional justice and security system reform*. Initiative for Peacebuilding Paper. International Centre for Transitional Justice. https://www.peacewomen.org/assets/file/Resources/NGO/recon_transjusticessr_ictj_2009.pdf

De Gregorio, G., & Stremlau, N. (2020). Internet shutdowns and the limits of law. *International Journal of Communication, 14*, 4224–4243. https://ssrn.com/abstract=3622928

Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere: Prologue. *International Journal of Communication, 12*, 3795–3813. https://ijoc.org/index.php/ijoc/article/view/8899/2459

Hadi, I.S., Arfani, R.N., & Ikhwan, H. (2022). Dynamics of People, State, and Cyber Power in the Internet Shutdown Policy at Papua and West Papua in 2019. In *3rd International Media Conference 2021* (pp. 234–248). Atlantis Press. https://doi.org/10.2991/assehr.k.220705.025

Ireton, C., & Posetti, J. (Eds.). (2018). *Journalism, fake news & disinformation: Handbook for journalism education and training*. United Nations Educational, Scientific and Cultural Organization.

Lee, A. (2020). Online hoaxes, existential threat, and Internet shutdown: A case study of securitization dynamics in Indonesia. *Journal of Indonesian Social Sciences and Humanities*, *10*(1), 17–34. https://ejournal.brin.go.id/jissh/article/view/8650/6664

Liaropoulos, A. (2015). A human-centric approach to cybersecurity: Securing the human in the era of cyberphobia. *Journal of Information Warfare, 14*(4), 15–24.

Lowrie, J. (2015). Cybersecurity: A primer of U.S. and international legal aspects. In T.A. Johnson (Ed.), *Cybersecurity: Protecting critical infrastructures from Cyber attack and cyber warfare* (pp. 199–251). CRC Press.

Pavlova, P. (2020). Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance, 4*(3), 391–418. https://doi.org/10.14658/PUPJ-PHRG-2020-3-4

Riebe, T., & Reuter, C. (2019). Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 165–183). Wiesbaden: Springer Vieweg. https://doi.org/10.1007/978-3-658-25652-4_8

Ryng, J., Guicherd, G., Saman, J.A., Choudhury, P., & Kellett, A. (2022). Internet Shutdowns: A Human Rights Issue. *The RUSI Journal*, *167*(4/5), 50–63. https://doi.org/10.1080/03071847.2022.2156234

Shah, N. (2021). (Dis)information Blackouts: Politics and Practices of Internet Shutdowns. *International Journal of Communication*, *15*, 2693–2709. https://ijoc.org/index.php/ijoc/article/view/13977/3466

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Thumfart, J. (2024). Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of Global Security Studies*, *9*(1). https://doi.org/10.1093/jogss/ogad024

Wagner, B. (2018). Understanding Internet Shutdowns: A Case Study from Pakistan. *International Journal of Communication, 12*(1), 22. https://ijoc.org/index.php/ijoc/article/view/8545

Zartman, I.W. (2008). *Negotiation and conflict: Essays on theory and practice*. Routledge.

Bio notes:

Adelisca Pramesti, Master's Student in the Defense Management Program, Department of Defense Management, The Republic of Indonesia Defense University, 3 Salemba Raya, Central Jakarta, 10440, Indonesia. ORCID: 0009-0001-1588-8052. E-mail: pramesti.adelisca@gmail.com

Hikmat Zakky Almubaroq, Head of the Master's Program in Defense Management, Department of Defense Management, The Republic of Indonesia Defense University, 3 Salemba Raya, Central Jakarta, 10440, Indonesia. ORCID: 0000-0002-9644-9245. Email: zakkyauri94@gmail.com

Aloysia Vira Herawati, Researcher, Teacher Researcher in Pedagogy, Lecturer, Faculty of Law, University of Surabaya, Raya Kalirungkut Tenggilis, Surabaya, 60293, Indonesia. ORCID: 0000-0003-4375-5246. E-mail: vira@staff.ubaya.ac.id

Bella A. Bulgarova, PhD in Philology, Associate Professor, Department of Mass Communication, RUDN University, 6 Miklukho-Maklaya St, Moscow, 117198, Russian Federation; Professor, Department of Digital Media, College of Arts, Alnoor University, Mosul, 41012, Republic of Iraq. ORCID: 0000-0001-6005-2505; SPINE-code: 8571-8231. E-mail: bulgarova-ba@rudn.ru

Сведения об авторах:

Прамешти Аделиска, магистр программы «Управление обороной», департамент управления обороной, Университет обороны Республики Индонезия, Индонезия, 104403, Центральная Джакарта, ул. Салемба Рая. ORCID: 0009-0001-1588-8052. E-mail: pramesti.adelisca@gmail.com

Альмубарок Хикмат Закки, руководитель магистерской программы по управлению обороной, департамент управления обороной, Университет обороны Республики Индонезия, Индонезия, 104403, Центральная Джакарта, ул. Салемба Рая. ORCID: 0000-0002-9644-9245. E-mail: zakkyauri94@gmail.com

Херавати Алоизия Вира, научный сотрудник, преподаватель-исследователь в области педагогики, юридический факультет, Университет Сурабая, Индонезия, 60293, Сурабая, Рая Калирунгкут Тенгилис. ORCID: 0000-0003-4375-5246. E-mail: vira@staff.ubaya.ac.id

Булгарова Белла Ахмедовна, кандидат филологических наук, доцент кафедры массовых коммуникаций, Российский университет дружбы народов, Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, д. 6; профессор кафедры цифровых медиа, Колледж гуманитарных наук, Университет Альнур, Республика Ирак, 41012, Мосул. ORCID: 0000-0001-6005-2505; SPINE-код: 8571-8231. E-mail: bulgarova-ba@rudn.ru