Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 9 No. 3 (2023) pp.559-570
https://jurnal.idu.ac.id/index.php/DefenseJournal

Combating International Cyber Conflict: A Healthy Just War and International Law Analysis of NATO and Indonesian Policies

Rita Komalasari[1*], Cecep Mustafa[2]
[1]Yarsi University, Indonesia
[2]Ibnu Chaldun University, Indonesia

rita.komalasari161@gmail.com[1*], cecepmustafa97@gmail.com[2]
*Corresponding Author

Article Info

Article history:
Received: August 9, 2023
Revised: November 11, 2023
Accepted: December 28, 2023

Keywords:
Conflict Resolution,
Cyber Conflict,
Just War Theory,
International Law,
National Security,
NATO

DOI:
http://dx.doi.org/10.33172/jp.v9i3.16867

Abstract

This study explores the policies of the North Atlantic Treaty Organization (NATO) and Indonesia in the context of international cyber conflict, analyzing their alignment with just war theory principles and international legal norms. By applying just war theory principles and international law, this study aims to analyze the responsible conduct of states in the realm of cyber warfare, fostering a more secure and stable international environment. This study employs a qualitative analytical method, examining the policies of NATO and Indonesia through the ethical lens of just war theory and the legal perspective of international law. The principles of *jus ad bellum* (righteous reasons for conflict), *jus in bello* (ethical conduct during conflict), and international cooperation guide the analysis, providing a comprehensive framework for evaluating the policies of these entities. Adherence to righteous reasons for cyber response, ethical conduct during cyber conflict, and international legal norms are paramount in resolving conflicts arising from cyber threats. By incorporating just war theory principles into their policies, entities can demonstrate ethical responsibility, minimize unnecessary harm, and foster an environment conducive to conflict resolution. Through this approach, NATO and Indonesia, alongside the global community, can contribute to the development of a secure and stable digital landscape. This paper's novelty lies in its integrated analysis of NATO and Indonesia's policies, considering both ethical and legal dimensions through the lens of just war theory and international law.

INTRODUCTION

In today's interconnected world, where digital technologies permeate every aspect of society, international cyber conflicts have emerged as a pressing global concern (Solar, 2020). The urgency of this research lies in the critical need to understand and address the evolving landscape of cyber warfare. Unlike traditional warfare, cyber conflicts operate in a realm where boundaries are blurred, and attacks can be launched from anywhere, targeting critical infrastructures, political processes, and economies (Maschmeyer, 2023). The urgency stems from the potentially catastrophic consequences of unregulated cyber warfare, making it imperative for nations to develop robust ethical frameworks and legal policies to navigate this complex terrain effectively (Lu, 2022). Within the realm of cyber conflict, there exist notable research gaps that this study aims to address. First and foremost, the ethical implications of cyber warfare, especially when viewed through the lens of just war theory, remain a relatively unexplored area (Hjorthen & Pattison, 2023). Understanding the application of age-old ethical principles to digital battlegrounds constitutes a significant gap in the current literature (Barboza, 2020). Additionally, there is a paucity of research that comprehensively evaluates the policies of global entities, such as NATO, in alignment with the just war theory and international law (Tichenor, Merry, Grek, & Bandola-Gill, 2022). Bridging these gaps is vital for developing nuanced, context-specific ethical guidelines for cyber warfare strategies. What sets this research apart is its novel approach in combining just war theory, international law, and cyber conflict analysis. By synthesizing these diverse fields, this study offers a fresh perspective on evaluating the ethical and legal dimensions of international cyber conflicts. Furthermore, the incorporation of case studies and real-world incidents provides practical insights into the application of theoretical frameworks. This multidisciplinary approach not only addresses existing research gaps but also contributes to the emerging field of cyber ethics and policy formulation (Berglund, Dunlop, Koebele, & Weible 2022). In essence, this research is not merely a theoretical exploration; it represents a critical step toward establishing a comprehensive understanding of responsible state behavior in cyberspace, filling existing gaps in the literature, and offering practical guidelines for policymakers and scholars alike. The urgency to navigate the complexities of cyber warfare, coupled with the innovative methodology and interdisciplinary approach, underscores the significance and newness of this research endeavor.

In the contemporary era, as the digital landscape becomes increasingly interconnected, the realm of conflict has expanded to encompass not only physical battlegrounds but also virtual domains (Valentini, Lorusso, & Stephan, 2020). International cyber conflicts have emerged as a potent challenge, transcending borders and posing significant threats to nations' security, stability, and economic well-being. Addressing this new frontier of warfare requires the careful consideration of both policy approaches and ethical frameworks. This essay delves into the strategies employed by two entities, the North Atlantic Treaty Organization (NATO) and the Republic of Indonesia, in combating international cyber conflicts. The evaluation is conducted within the ethical context of just war theory, a centuries-old framework that seeks to determine the morality and legality of armed conflict (Barboza, 2020). The central argument of this essay is that in the face of international cyber conflict, both NATO and Indonesia have adopted policies that demand evaluation within the framework of just war theory and international law. By examining their approaches through these ethical and legal lenses, the reader can gain insights into the extent to which their actions are justified, proportionate, and aligned with the established norms of the global community. As the

digital landscape continues to evolve and cyber conflicts become more prevalent, understanding the ethical and legal dimensions of policy decisions is paramount (Yousefi, 2022). By engaging in this analysis, this study seeks not only to evaluate the policies of specific entities but also to contribute to a broader discourse on the responsible conduct of states in the realm of cyber warfare, fostering a more secure and stable international environment. A tool to analyze is just war theory. This study aims to analyses the responsible conduct of states in the realm of cyber warfare, fostering a more secure and stable international environment.

METHODS

Conducting literature research involves a systematic process, from identifying the research question to analyzing the gathered information. Here is a detailed explanation of each stage, encompassing data collection and processing in the context of literature research: choose Google Scholar repositories relevant to international cyber conflicts. The primary data sources are academic databases. This study develops a set of keywords and phrases related to the research question to use during searches (i.e., cyber conflict, just war theory, international law, national security, conflict resolution). The 'samples' in this context refer to the diverse range of academic articles related to NATO and Indonesia's cyber policies, for example, the cyber security strategy and action plan. This document prioritizes defending critical infrastructure, responding to cyber threats, and international cooperation (Yanti, Aviolita, & Marsetio, 2020). While not directly addressing *jus ad bellum*, it fosters responsible cyber defense, potentially minimizing escalation and unnecessary harm. The inclusion criteria were relevant to cyber conflict, and just war theory. Google Scholar was chosen for its comprehensiveness in aggregating scholarly articles, conference papers, and academic publications. Its broad scope allowed for a comprehensive examination of existing literature related to cyber conflict, just war theory, and international law.

Systematically search for scholarly articles, books, reports, and other academic materials using the identified keywords. Define criteria for including or excluding sources based on relevance and publication date (from 2018 or newer). The abstracts of the identified literature were read by this study to assess their relevance to the research question. Access and review the full text of selected articles and books to extract relevant information. Extract key data, including theories, methodologies, findings, and conclusions, from the selected literature. This study organizes the collected literature into categories based on themes, methodologies, or other relevant criteria. This study takes detailed notes on each source, summarising key points and ideas. Develop a conceptual framework or model based on the synthesized information, illustrating the relationships between different concepts and theories (Suryadi & Komalasari, 2020). This study employs a descriptive qualitative methodology. News sources, journals, publications, reports, and official statements are used to collect data. By classifying the data and assigning codes depending on a study topic, the data is qualitatively analyzed. The study's results are then incorporated into the publication. The primary objective was to evaluate NATO and Indonesia's cyber policies through the ethical lens of just war theory.

RESULT AND DISCUSSION

In addressing the research question: Is just war theory still valid in addressing international cyber conflict? This section presents the results and discusses the

applicability and validity of the just war theory in the context of international cyber conflict (Hjorthen & Pattison, 2023).

The Applicability and Validity of the Just War Theory in the Context of International Cyber Conflict

The principles of just war theory, rooted in centuries of ethical reflection on armed conflict, provide a framework for evaluating the morality and legality of engaging in war (Evans, 2005). In the contemporary context of international cyber conflict, these principles offer a valuable perspective on the responsible use of cyber capabilities by states. This section will delve into the key principles of *jus ad bellum* (righteous reasons for conflict), *jus in bello* (ethical conduct during conflict), and elucidate their adaptation to the unique challenges posed by cyber warfare. This groundwork will establish the foundation for analyzing and evaluating the policies of NATO and Indonesia in addressing international cyber conflicts. The principle of *jus ad bellum* outlines the criteria that must be met to ethically justify entering into armed conflict (Blanchard & Taddeo, 2022). Traditional warfare typically involves physical aggression and territorial boundaries, yet the advent of cyberspace has blurred these lines. In the realm of cyber conflict, the application of *jus ad bellum* necessitates a reevaluation of what constitutes a legitimate reason for response.

The concept of righteous reasons remains pertinent in cyber warfare. A state's response to cyber threats must be predicated on the imminent threat to its sovereignty, security, or citizens. Assessing the proportionality of response becomes nuanced in cyberspace, as the scale of potential damage varies significantly. As this study evaluates the policies of NATO and Indonesia, it is crucial to gauge whether their cyber actions are justifiably based on imminent and serious threats in alignment with the principle of righteous reasons. The principle of *jus in bello* pertains to the ethical conduct of parties engaged in conflict. In traditional warfare, this principle encompasses minimizing harm to civilians, distinguishing between combatants and non-combatants, and avoiding unnecessary suffering. In the context of cyber warfare, these principles are equally applicable, albeit with unique challenges. The principle of discrimination mandates that cyber operations target military objectives and avoid causing undue harm to civilian infrastructure or non-combatants (Huang & Ying, 2020). Proportionality, another key aspect, stipulates that the harm caused by a cyber operation should not outweigh the potential benefits gained. These principles translate into the realm of cyber conflict by emphasizing the responsible use of cyber capabilities to minimize unintended collateral damage. As cyberspace lacks the physicality of traditional battlegrounds, the adaptation of just war theory's principles to cyber conflict demands careful consideration. The principle of discrimination translates into targeting only those digital assets directly involved in the conflict while avoiding civilian systems. Proportionality requires assessing the potential consequences of a cyber operation against the anticipated benefits. Furthermore, the notion of legitimate authority requires defining which entities have the right to engage in cyber conflict on behalf of a state. This becomes pertinent in analyzing multilateral organizations like NATO, which operate based on collective defense agreements. Just war theory's principles apply to the realm of cyber conflict, albeit with adaptations that reflect the unique nature of the digital domain. This section's exploration of these principles establishes a conceptual framework for evaluating the policies of NATO and Indonesia, shedding light on their alignment with ethical considerations in the context of international cyber conflicts.

NATO, a cornerstone of international security, has adapted its policies to address the emerging threat landscape of cyber conflict (Romaniuk, Fotescu, & Chihaia, 2021). As a prominent player in the global arena, NATO's approach to international cyber conflicts warrants thorough evaluation. This section scrutinizes NATO's policies and actions within the context of just war theory and international law, delving into the extent to which they align with ethical considerations and established norms. NATO's policies regarding cyber conflict demonstrate a commitment to the principles of proportionality and discrimination. The alliance emphasizes the necessity of cyber actions being commensurate with the threat posed, avoiding disproportionate retaliation. This aligns with just war theory's principle of proportionality, ensuring that the use of cyber capabilities does not result in excessive harm relative to the anticipated benefits. Furthermore, NATO's emphasis on targeting military objectives and avoiding civilian infrastructure is congruent with the principle of discrimination. By directing cyber operations toward legitimate targets, NATO seeks to minimize unintended harm to civilian systems or non-combatants, demonstrating ethical conduct consistent with just war theory's *jus in bello*. NATO's legitimacy in the cyber realm stems from its collective defense agreements, where member states have authorized the alliance to act on their behalf (Coffey & Kochis, 2020). This alignment with the principle of legitimate authority ensures that NATO's actions are rooted in a multilateral framework, reflecting both the ethical considerations of just war theory and the requirements of international law.

NATO's approach to international cyber conflict contributes to conflict resolution by promoting a structured and coordinated response. By adhering to principles of proportionality and discrimination, the alliance minimizes the risk of unnecessary escalation and collateral damage. Furthermore, NATO's emphasis on collective defense underscores its commitment to cooperative security practices, fostering an environment conducive to diplomatic resolutions and de-escalation of tensions. The examination of NATO's policies and actions in the realm of international cyber conflicts reveals a commitment to ethical conduct consistent with just war theory and international law. The alignment with principles of proportionality, discrimination, and legitimate authority underscores NATO's dedication to responsible state behavior in the digital age. By adhering to these principles, NATO not only safeguards its interests but also contributes to the broader discourse on ethical and lawful conduct in the international cyber landscape (Gottemoeller, Hedgecock, Magula, & Poast, 2022).

Indonesia, a sovereign nation navigating the complexities of international cyber conflicts, adopts strategies to safeguard its interests and national security (Desiana & Prima, 2021). This section explores Indonesia's approach within the ethical framework of just war theory and the boundaries set by international law. By evaluating whether Indonesia's cyber policies uphold ethical standards and legal parameters, this study gains insights into its commitment to responsible conduct and conflict resolution in the realm of cyberspace. Indonesia's approach to international cyber conflicts emphasizes ethical conduct by prioritizing proportional responses. By avoiding undue escalation and harm, Indonesia's policies reflect a commitment to minimizing collateral damage, in line with the principle of proportionality. This approach aligns with just war theory's emphasis on responsible conduct during conflict, ensuring that the use of cyber capabilities remains measured and targeted. Indonesia's participation in regional frameworks like the ASEAN Cyber Norms demonstrates its commitment to international law and regional diplomacy (Priyono, Swastanto & Pramono, 2023). By engaging in discussions on responsible state behavior in cyberspace, Indonesia contributes to a stable and secure digital environment.

This alignment with international law fosters trust among states and facilitates conflict resolution through dialogue and cooperation.

Indonesia's emphasis on ethical conduct and regional cooperation in its cyber policies contributes to conflict resolution in several ways. Firstly, by adhering to principles of proportionality and ethical conduct, Indonesia minimizes the risk of escalation and unintended consequences, fostering an environment conducive to negotiation and dialogue. Secondly, by engaging in multilateral discussion, Indonesia promotes the establishment of shared norms and rules in the realm of cyberspace, fostering trust among states and reducing the potential for conflict. The examination of Indonesia's approach to international cyber conflicts reveals a commitment to ethical conduct and adherence to international law. By prioritizing proportional responses and engaging in regional diplomacy, Indonesia demonstrates its dedication to responsible state behavior in the digital realm. Through these policies, Indonesia contributes not only to its national security but also to broader conflict resolution efforts by fostering trust and promoting a secure international digital landscape. This condition supports and strengthens previous research conducted by Desiana & and Prima (2021).

Just War-Theoretic Evaluation and Resolving Conflicts Arising from Cyber Threats

In the realm of international relations, the application of just war theory provides a moral and ethical framework for evaluating the legitimacy and conduct of armed conflict (Hjorthen & Pattison, 2023). As cyber threats and conflicts continue to escalate globally, it becomes imperative to apply these principles to the domain of cyberspace. Indonesia, a sovereign nation grappling with its share of cyber threats, has the responsibility to address these challenges while adhering to just war theory principles. By assessing Indonesia's approach to cyber conflicts within this framework, this study can elucidate the extent to which its policies align with ethical considerations and contribute to conflict resolution. The first tenet of the just war theory, *jus ad bellum*, emphasizes the moral justification for resorting to war (Simon, 2018). Translating this principle to the realm of cyber conflict, it becomes essential to assess whether Indonesia's response to cyber threats is grounded in righteous reasons. Are the threats imminent and serious enough to warrant a cyber response? Indonesia's cyber defense strategy in mitigating the risk of cyber warfare threats must prioritize the protection of its citizens and national interests while minimizing unnecessary harm to other states (Permana, 2021).

Indonesia's response to cyber threats should exhibit a proportional and justifiable reaction, mirroring the principle of proportionality. A measured response would avoid exacerbating conflicts and limit collateral damage to third parties. Through a just war-theoretic lens, Indonesia must justify its cyber actions as necessary means to protect its sovereignty and ensure national security. The second aspect of just war theory, *jus in bello*, underscores the ethical conduct during the course of conflict (Joo, 2019). In the context of cyber conflicts, this principle emphasizes discrimination and proportionality in the use of cyber capabilities. Indonesia's cyber landscape report acknowledges Indonesia's comprehensive cyber policies but raises concerns about the lack of transparency and public oversight regarding their implementation. It also highlights the potential for discrepancies between official pronouncements and actual cyber operations (Safitra, Lubis, & Fakhrurroja, 2023). Indonesia's policies must ensure that its cyber operations are directed solely at legitimate targets and that the potential harm caused is commensurate with the intended goal. Non-combatant immunity remains essential, as attacks on civilian infrastructure can result in widespread harm and violate international law. Respecting the principles of *jus in bello* can facilitate conflict resolution by

minimizing unnecessary harm and promoting accountability. By adhering to ethical norms in the use of cyber capabilities, Indonesia can demonstrate its commitment to resolving conflicts without unduly escalating hostilities.

Just war theory not only provides a philosophical framework but also aligns with the principles of international law. Indonesia, as a member of the global community, must respect established international norms and conventions related to cyber conflict. Through multilateral cooperation, nations can collectively work towards conflict resolution and the establishment of common rules in cyberspace. Indonesia's adherence to international legal frameworks in its cyber policies contributes to conflict resolution by fostering trust among states and ensuring a stable environment for dialogue and negotiation. Engaging in diplomacy and seeking peaceful resolutions to cyber conflicts demonstrates a commitment to responsible behavior in the digital realm (Egenschwiler & Kulesza, 2020). In the context of Indonesia's approach to resolving conflicts arising from cyber threats, the application of just war theory provides a valuable ethical framework. By evaluating its cyber policies through the lenses of *jus ad bellum* and *jus in bello*, Indonesia can align its actions with moral principles that promote responsible conduct and minimize unnecessary harm. Furthermore, Indonesia's commitment to international law and multilateral cooperation enhances the prospects of conflict resolution by fostering an environment of trust and stability. Ultimately, by integrating just war theory principles into its cyber policies, Indonesia can demonstrate its dedication to ethical behavior, responsible conflict resolution, and the establishment of a secure digital environment for itself and the global community. This condition supports and strengthens previous research conducted by Hjorthen & and Pattison (2023). Hjorthen & Pattison's research supports this notion by emphasizing the importance of proportionality and providing a valuable framework for applying just war principles to cyber warfare.

Just war theory's principle of *jus ad bellum* requires that any use of force is justified by legitimate reasons (Simon, 2018). In the context of cyber conflict, this principle demands a careful assessment of the imminent and serious nature of cyber threats before resorting to a response. NATO's cyber defense policy reflects a proactive stance on cyber defense, emphasizing the importance of preventing cyberattacks through collective action (Arnold, 2020). This aligns with the notion of righteous reasons, as preemptive measures are justified to safeguard national security and the stability of member nations. Indonesia's approach, too, emphasizes self-defense against cyber threats, underlining the necessity of responding to protect its sovereignty and citizens. By assessing the imminence and gravity of cyber threats, both NATO and Indonesia exhibit an alignment with the principle of *jus ad bellum*, emphasizing responsible and justified actions in the face of cyber conflicts. The principle of *jus in bello* mandates ethical conduct during conflict, focusing on proportionality and discrimination. NATO regularly conducts cyber defense exercises that simulate attacks on critical infrastructure. These exercises emphasize the importance of protecting civilian targets and minimizing collateral damage (Arnold, 2020). NATO's policies reflect a commitment to these principles by employing cyber capabilities that target military objectives rather than civilian infrastructure. This ensures that harm is limited to combatants and legitimate targets, minimizing unnecessary collateral damage. NATO's adherence to the principle of discrimination exemplifies a responsible approach, underscoring its dedication to resolving conflicts without inflicting undue harm. NATO's actions also reflect the principle of legitimate authority, an essential component of just war theory (Evans, 2005). The organization operates under the framework of collective defense, providing a

multilateral mandate for its actions. This aligns with international law by operating within the established norms of cooperation among sovereign states. NATO's adherence to legitimate authority contributes to conflict resolution by promoting a structured and lawful approach to cyber conflict management. Indonesia's policies mirror the just war theory's emphasis on ethical conduct during conflict. Although attributing responsibility remains complex, Indonesia's response to alleged cyberattacks targeting its critical infrastructure by APT29 (Russia) reportedly focused on defensive measures and international cooperation rather than immediate escalation (Mahira, Rohmahwatin, & Suciningtyas, 2020). By employing a proportional response framework, Indonesia strives to limit the scope and impact of its cyber actions, avoiding unnecessary escalation. This approach showcases the country's commitment to conflict resolution by minimizing harm while still addressing cyber threats effectively. In various international forums, particularly within the Association of Southeast Asian Nations (ASEAN) framework, Indonesia has actively emphasized the importance of regional cooperation. One notable initiative is the ASEAN Cyber Norms. In this context, Indonesia has demonstrated its commitment to upholding international law and engaging in multilateral diplomacy. Indonesia's emphasis on regional cooperation, through mechanisms like the ASEAN Cyber Norms, illustrates its dedication to international law and multilateral diplomacy. By engaging in dialogue and collaboration with neighboring states, Indonesia contributes to conflict resolution by fostering trust and shared understanding in the complex landscape of cyber conflict. The analysis of NATO and Indonesia's policies through the lens of just war theory and international law reveals a concerted effort towards responsible and ethical conduct in the face of international cyber conflicts. Both entities' alignment with principles such as righteous reasons, ethical conduct, and legitimate authority underscores their commitment to conflict resolution. By incorporating these principles into their policies, NATO and Indonesia contribute to the broader discourse on responsible state behavior in the digital age, ultimately fostering a secure and stable international environment. This condition supports and strengthens previous research conducted by (Simon, 2018).

This section explores how a just war theoretic evaluation facilitates the identification and application of best practices in addressing international cyber conflicts. By reviewing case studies of cyber conflicts and their resolutions, Indonesia can gain valuable insights into effective strategies employed by other states. For instance, the Stuxnet incident, a well-known cyberattack on Iran's nuclear facilities, provides a case study where a cyber operation was executed with precision to achieve a specific objective (Kaminska, Broeders, & Cristiano, 2021). Analyzing such instances allows Indonesia to understand how the principles of proportionality, discrimination, and legitimate authority were applied effectively to resolve conflicts and attain strategic goals. A just war theoretic evaluation enables Indonesia to extract key lessons from case studies and past incidents, identifying practices that have yielded positive outcomes. For instance, the use of diplomatic channels and multilateral cooperation to address cyber incidents, as observed in the agreement between the United States and China to curb cyber espionage, exemplifies successful conflict resolution. By drawing parallels between these cases and Indonesia's context, the nation can learn from strategies that emphasize dialogue, cooperation, and responsible state behavior. While drawing insights from case studies is invaluable, it is crucial to adapt best practices to Indonesia's unique geopolitical, cultural, and technological landscape. Just war theory's flexibility allows for the integration of successful strategies within a framework that aligns with Indonesia's values and national interests. For instance, while a specific strategy might have been effective for one nation,

Indonesia's circumstances may require adjustments to account for local considerations and geopolitical dynamics (Komalasari & Mustafa, 2023). The identification and application of best practices through a just war theoretic evaluation contribute significantly to Indonesia's conflict resolution efforts. By incorporating successful strategies into its policies, Indonesia can enhance its cyber defenses, minimize harm, and promote diplomatic solutions (Gottemoeller, Hedgecock, Magula, & Poast, 2022). Moreover, demonstrating a willingness to learn from the experiences of others fosters a culture of responsible behavior in the digital realm and paves the way for collaborative efforts in addressing cyber threats collectively (Komalasari & Mustafa, 2023). A just war theoretic evaluation not only evaluates the ethical and legal dimensions of policies but also serves as a valuable tool for identifying and applying best practices in resolving international cyber conflicts. By analyzing case studies, extracting lessons, and adapting strategies to its unique context, Indonesia can enhance its conflict resolution efforts, contribute to responsible state behavior, and create a secure and stable digital environment on a global scale (Mustafa, 2021). The realm of international conflict has extended its boundaries to encompass cyberspace, posing unique challenges that demand novel solutions. This essay has examined the policies of NATO and Indonesia through the ethical framework of just war theory and the lens of international law, providing a comprehensive evaluation of their approaches to combatting international cyber conflicts. The application of just war theory 's principles, encompassing righteous reasons for cyber response and ethical conduct during conflict, has revealed the commitment of both NATO and Indonesia to responsible actions in the face of cyber threats. Their adherence to principles of proportionality, discrimination, and legitimate authority showcases their dedication to minimizing harm while pursuing conflict resolution. Furthermore, both entities' respect for international law and engagement in regional diplomacy underscore their commitment to a stable and secure digital environment. This condition supports and strengthens previous research conducted by (Priyono, Swastanto & Pramono, 2023)

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

In conclusion, resolving disputes emerging from cyber threats requires strict adherence to ethical behavior during cyber conflict, righteous motives for cyber reaction, and international legal standards. Entities may enhance their ethical stance, reduce needless damage, and create a space that is favorable to resolving conflicts by integrating ideas of just war theory into their policies. With this strategy, Indonesia and NATO, together with the rest of the world, can help build a more secure and reliable internet. Unique to this work is its examination of NATO and Indonesian policy as a whole, with an eye on the ethical and legal considerations raised by international law and just war theory.

One significant limitation lies in the subjective interpretation of the just war theory's principles. The application of principles such as proportionality and discrimination in the context of cyber warfare can be challenging due to the intangible nature of digital assets and the difficulty in measuring potential harm accurately. This subjectivity could lead to varying interpretations and potential disagreements among different stakeholders. To address the limitation of subjective interpretation, policymakers and scholars should collaborate to develop standardized guidelines that apply the just war theory's principles to cyber conflicts. This effort could involve creating a set of criteria for assessing cyber threats, measuring potential harm, and determining

appropriate responses. Such guidelines could help mitigate ambiguity and provide a common basis for evaluating the ethical and legal dimensions of cyber defense policies.

REFERENCES

Arnold, R. (2020). The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, edited by Michael N. Schmitt. *International Criminal Law Review*, *20*(1), 155–159. https://doi.org/10.1163/15718123-02001008

Barboza, A. R. (2020). *The Irish Republican Army: An Examination of Imperialism, Terror, and Just War*. California Polytechnic State University, San Luis Obispo.

Berglund, O. J . B ., Dunlop , C ., Koebele , E . A ., & Weible, C. M. (2022). *Transformational Change through Public Policy. Policy and Politics, 50(3)*, 302–322. https://doi.org/10.1332/030557322X16546739608413

Blanchard, A., & Taddeo, M. (2022). Autonomous Weapon Systems and Jus Ad Bellum. *AI & Society*. https://doi.org/10.1007/s00146-022-01425-y

Coffey, L., & Kochis, D. (2020). *NATO in the 21st Century: Preparing the Alliance for the Challenges of Today and Tomorrow*. Washington DC: The Heritage Foundation.

Desiana, R., & Prima, S. C. (2021). Cyber Security Policy in Indonesian Shipping Safety. *Journal of Maritime Studies and National Integration*, *5*(2), 109–117. https://doi.org/https://doi.org/10.14710/jmsni.v5i2.13673

Eggenschwiler, J., & Kulesza, J. (2020). Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace. In D. Broeders & B. Van Den Berg (Eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy*. London: Rowman & Littlefield.

Evans, M. (2005). *Just War Theory: A Reappraisal*. United Kingdom: Edinburgh University Press.

Gottemoeller, R., Hedgecock, K., Magula, J., & Poast, P. (2022). Engaging with Emerged and Emerging Domains: Cyber, Space, and Technology in the 2022 NATO Strategic Concept. *Defence Studies*, *22*(3), 516–524. https://doi.org/10.1080/14702436.2022.2082955

Hjorthen, F. D., & Pattison, J. (2023). Proportionality in cyberwar and just war theory. *Ethics and Global Politics*, *16*(1), 1–24. https://doi.org/10.1080/16544951.2023.2179244

Huang, Z., & Ying, Y. (2020). The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective. *International Review of the Red Cross*, *102*(913), 335–365. https://doi.org/10.1017/S1816383121000023

Joo, M. Y. (2019). *The Principle of Proportionality in the Law and Ethics of War: Steps Toward a Unified View of Proportionality in Jus Ad Bellum and Jus in Bello by Moving from Subjective Political to Objective Legal Criteria* (American University). American University, Washington D.C.

Kaminska, M., Broeders, D., & Cristiano, F. (2021). Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone. *13th International Conference on Cyber Conflict: Going Viral*, 59–72. Retrieved from https://ccdcoe.org/uploads/2021/05/CyCon_2021_kaminska_broeders_cristiano.pdf

Komalasari, R., & Mustafa, C. (2023). A Healthy Game-Theoretic Evaluation of NATO and Indonesia's Policies in the Context of International Law. *Jurnal Pertahanan*, *9*(2), 333. https://doi.org/10.33172/jp.v9i2.16794

Lu, I. F. (2022). To Subdue the Enemies without Fighting: Chinese State-Sponsored

Disinformation as Digital Warfare. *Digital War*, *3*(1–3), 96–106. https://doi.org/https://doi.org/10.1057/s42984-022-00052-7

Mahira, D. F., Rohmahwatin, D. S., & Suciningtyas, N. D. (2020). Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat. *Lex Scientia Law Review*, *4*(1), 59–69. https://doi.org/https://doi.org/10.15294/lesrev.v4i1.38191

Maschmeyer, L. (2023). A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies*, *46*(3), 570–594. https://doi.org/https://doi.org/10.1080/01402390.2022.2104253

Mustafa, C. (2021). The News Media Representation of Acts of Mass Violence in Indonesia. *IGI Global*, 127–140. https://doi.org/https://doi.org/10.4018/978-1-7998-4957-5.ch008

Permana, A. (2021). Indonesia's Cyber Defense Strategy in Mitigating the Risk of Cyber Warfare Threats. *Syntax Idea*, *3*(1), 1–11. https://doi.org/https://doi.org/10.46799/syntax-idea.v3i1.860

Priyono, U., Swastanto, Y., & Pramono, B. (2023). Cyber Diplomacy (a Perspective from Indonesia-Australia Cyber Cooperation). *International Journal of Humanities Education and Social Sciences*, *2*(4), 1326–1333. https://doi.org/https://doi.org/10.55227/ijhess.v2i4.371

Romaniuk, S. N., Fotescu, A., & Chihaia, M. (2021). NATO's Evolving Cyber Security Policy and Strategy. In *Routledge Companion to Global Cyber-Security Strategy*. London: Routledge.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18). https://doi.org/https://doi.org/10.3390/su151813369

Simon, H. (2018). The Myth of Liberum Ius ad Bellum: Justifying War in 19th-Century Legal Theory and Political Practice. *European Journal of International Law*, *29*(1), 113–136. https://doi.org/10.1093/ejil/chy009

Solar, C. (2020). Cybersecurity and Cyber Defence in the Emerging Democracies. *Journal of Cyber Policy*, *5*(3), 392–412. https://doi.org/https://doi.org/10.1080/23738871.2020.1820546

Suryadi, K., & Komalasari, K. (2020). *Dinamika dan Tantangan Pendidikan: Senarai Pemikiran Guru Besar UPI dalam Pidato Pengukuhan Tahun 2002-2020*. Bandung: UPI Press.

Tichenor, M., Merry, S. E., Grek, S., & Bandola-Gill, J. (2022). Global Public Policy in a Quantified World: Sustainable Development Goals as Epistemic Infrastructures. *Policy and Society*, *41*(4), 431–444. https://doi.org/10.1093/polsoc/puac015

Valentini, D., Lorusso, A. M., & Stephan, A. (2020). Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.00524

Yanti, R., Aviolita, S., & Marsetio. (2020). Judicial Review of Indonesia's Position as the First Archipelagic State to Implement the Traffic Separation Scheme to Establish Maritime Safety and Security. *International Journal of Law and Political Sciences*, *14*(12), 1176–1180. Retrieved from https://publications.waset.org/10011631/judicial-review-of-indonesias-position-as-the-first-archipelagic-state-to-implement-the-traffic-separation-scheme-to-establish-maritime-safety-and-security

Yousefi, Y. (2022). Notions of Fairness in Automated Decision Making: an Interdisciplinary Approach to Open Issues. *International Conference on Electronic*

Government and the Information Systems Perspective. https://doi.org/https://doi.org/10.1007/978-3-031-12673-4_1