(Online) ISSN 2744-1741
Original Research

Defense and Security Studies
Vol. 5, No. 1, 2024, pp. 1-9
https://doi.org/10.37868/dss.v5.id255

Enhancing awareness of cyber crime: A crucial element in confronting the challenges of hybrid warfare in Indonesia

Ihsania Karin Azzani[1*], Susilo Adi Purwantoro[2], Hikmat Zakky Almubarok[3]
[1,2,3] Defense Managment, Defense University of The Republic of Indonesia

*Corresponding author E-mail: ihsania.broto@mp.idu.ac.id

Received: Dec. 7, 2023.
Revised: Jan. 5, 2024.
Accepted: Jan. 6, 2024.
Online: Jan. 13, 2024.

Abstract

The Cyber Defense Center, abbreviated as Pushansiber, is an institution responsible for carrying out the duties and functions of the Defense Strategic Installation Agency. Pushansiber has an important role in implementing governance, cooperation, operations, and ensuring cyber defense security. However, this year there has been an increase in problems related to cyber attacks, such as phishing, malware, ransomware, spam. These cyber attacks are included in the concept of hybrid warfare which is believed to be a form of conflict that involves the utilization of various elements, one of which is cyber attacks, military, political, economic, and information aspects. This causes conflict situations to be complicated and demands a comprehensive approach in terms of defense and handling, with digital literacy and cybersecurity awareness which has an important role in defense management, the need for awareness and training, simulation, and certification to strengthen cybercrime awareness in every organization. The success of other countries that have established specialized cybersecurity teams and invested in advanced technology can serve as an example for Indonesia. For Indonesia, the cooperation between National Cyber and Crypto Agency (BSSN) and the Ministry of Defense in strengthening cybersecurity capabilities is an important step to safeguard infrastructure, protect sensitive data, and reduce potential disruptions from malicious cyber activities with the aim of strengthening cybersecurity capabilities.

Keywords: cyber crime awareness, cyber crime, digital literacy, hybrid war, cyber defense

1. Introduction

The phenomenon of hybrid warfare reflects a paradigm shift in the conduct of international conflict, that previously the main attention was focused on conventional military combat alone, however, over time with the advancement of increasingly sophisticated technology, especially in the field of cyber and information, the structure of conflict has undergone substantial changes that hybrid warfare involves a variety of activities, comprehensive and highly diverse military resources, programs, and application [1] all of which are carefully designed to achieve the maximization of persuasive political and economic influence without involving violence, with the goal being to reform a hostile government or group and simultaneously reverse political,

social, and economic instability [2] hybrid warfare also involves more than direct military action, but also includes elements such as propaganda, cyberattacks, and attempts to manipulate public opinion, from diversity to the purpose of making the political dimension more complex, especially since the parties involved can use digital platforms and social media to influence perceptions globally [3].

Cybersecurity is currently the main focus for all countries in the world since information and communication technology began to be applied in various aspects of our lives today[4] in the use of technology in the era of rapidly growing digitalization, that the use of technology involves various fields, in terms of advances in information technology bring a positive impact on the ease of human life, but also bring potential that can endanger humans [5] regarding the use of technology in the era of increasingly rapid digitalization, the use of technology involves various fields, in terms of advances in information technology it has a positive impact on the ease of human life, but also carries the potential to be detrimental to humans.

The influence of globalization and technological advances that enter the state and nation brings various impacts of change, from the influence of globalization now, it can be seen and cannot be denied anymore because the many technological advances that enter the state and nation involve various fields of legal certainty, social, economic, organizational, health, education, culture, government, security, defense, and so on Along with the increase in the level of adoption of information technology and communication, risks and threats to misuse of this technology have also increased significantly, are high, and are increasingly complex [6] now, it can be seen and cannot be denied because of the many technological advances that have entered the state and nation involving various fields of legal certainty, social, economic, organizational, health, education, culture, government, security, defense, and so on. Along with increasing levels of adoption of information and communication technology, the risks and threats of misuse of this technology have also increased significantly, are high, and increasingly complex.

The author conveys in this article that it is felt that there is a need for better attention to policy and awareness as well as expanding ideas related to awareness for individuals and for ministries/institutions in dealing with cyber crime, especially in the context of hybrid warfare which is actually happening in Indonesia at the moment, and could even become a war trend in the future writer too provide recommendations for overcoming the challenges posed by cybercrime for the two organizations in the Ministry/Institution, both Bainstrahan, Ministry of Defense and BSSN. This can be discussed in research in this field.

This paper was written to address the specific need for increased awareness and understanding of the scope and methods of cybercrime, particularly in the context of hybrid warfare in Indonesia, this is important for individuals, households and organizations because cybercrime is a significant and growing threat and has the potential to cause major losses and even business closures.

The uniqueness of this paper lies in its focus on the unique challenges of cybercrime in the context of hybrid warfare in Indonesia and provides a specific analysis of the impact of cybercrime in this context.

The added value of this paper lies in the detailed analysis of the impact and challenges of cybercrime in the context of hybrid warfare in Indonesia, as well as the practical recommendations offered to overcome these challenges.

The author's contribution is to analyze the impact and challenges of cyber crime in Indonesia, especially in the defense context, as well as valuable recommendations provided to mitigate challenges including increasing awareness about cyber security, providing training programs and educational tools regarding cyber security challenges and the consequences of information crime, and increase knowledge about the risk of loss of sensitive information.

1.1 Definition and characteristics of „Hybrid War“

Hybrid warfare is a military strategy that combines conventional and unconventional tactics [1] to achieve strategic objectives through a combination of military, economic, diplomatic, and informational actions,

involving regular military force, cyberattacks, propaganda, and economic pressure, with the goal being to exploit the opponent's weaknesses and create confusion, difficult for states to target in an effective response, complex and dynamic, increasingly prominent in global security due to technological advances and geopolitical changes [7] from the increasing prevalence of hybrid warfare, to achieve political objectives, then, emphasizing the importance of cybercrime awareness in national defense is essential.

Hybrid warfare often includes cyber terrorism and cyber warfare [8] so it is important for states to be ready to address the threats, the use of the internet in cyberspace to execute or control hybrid threats has become a common tactic, and its role in hybrid threat scenarios is huge. States, therefore, need to devise strategies to counter cybercrime and raise awareness of the threat posed by hybrid warfare itself.

This requires a comprehensive approach, including enhanced civilian and military readiness [9], innovative resilience and response strategies, and the development of new policies and doctrines hence states need to foster situational awareness of multidimensional joint campaigns for the long term and use active sensing to engage the perception of entities in the environment, understand their meaning, and project their status in the near future on the urban environment to mitigate subversive action [10], one of the measures by which states can increase their capacity to face the challenges of hybrid warfare and protect their critical infrastructure and institutions from cyberattacks and other hybrid threats

1.2 Cybercrime as critical component

The term "cybercrime" is used widely by governments, businesses, and the general public to refer to a variety of criminal activities and dangerous behavior involving the use of computers, the internet, or other forms of information and communications technology [11]. It is a growing social phenomenon in the information age. Cyberspace has raised concerns globally due to its potential for significant damage and far-reaching effects, to avoid potential threats, the implementation of effective and reliable defense management is important, which ensures the optimality of the national defense system [12].

Indonesia's universal national defense system (Sishanta) [13] aims to maintain and protect sovereignty, maintain territorial integrity, and ensure the safety of the entire nation from various challenges and threats [14].

In the direction of this universal defense system includes the use of various national resources, natural resources and human resources, on this basic principle the benchmark that national defense is all efforts made to defend sovereignty, territorial integrity, and ensure the safety of the nation from various threats and disturbances that can threaten the integrity of the nation and state, including in the form of certain issues [15].

Figure 1. Annual Report BSSN 2022 of Global Security Index (GCI's last assessment was in 2020, the latest assessment update will be released in 2023

Defense management has a very significant role in the formation of defense policy, requiring accurate and sustainable planning mechanisms [2] and refers to a country's capacity to manage its resources effectively and efficiently to meet national defense interests in a strategic and holistic manner, in accordance with applicable management principles, this includes short and long term strategic planning aimed at improving overall performance [3].

Based on the annual report containing cyber threat projections for 2023, Indonesia's National Cyber and Encryption Agency (BSSN) is placed in 24th place with a score of 94.88 in the Global Security Index (GCI), based on the document confirms that its function is not only limited to providing an overview of the national cybersecurity situation in 2022 and cyber threat trends in 2023, but also acts as a form of accountability to the public for BSSN's performance.

It has been stated in the presidential regulation of the republic of indonesia number 47 of 2023 on national cyber security strategy and cyber crisis management the importance of realizing that technological advances can trigger cyber attacks that have the potential to cause social and economic losses, and threats to state sovereignty. It is emphasized that the need to develop a cyber security strategy and cyber crisis management at the national level including the development of a cyber security culture and the implementation of emergency response handling is part of the government's responsibility to protect the public interest from various forms of disturbance caused by misuse of electronic information and electronic transactions; it is necessary for steps to be taken seriously to maintain national integrity and security in the current new digital era.

When viewed from the scope of cyber threat ranking in Indonesia can be a very complex problem[16] in the future if not anticipated early, then the country's defense strategy plays a very important role in the sense of maintaining sovereignty, integrity, and safety from threats both traditional and non-traditional which are massively integrated that the essence of national defense is all universal defense actions, organized based on awareness of the rights and obligations of citizens, as well as belief in strength from within, the administration of national defense is carried out by the government and prepared with the state defense system anticipatory or can recognize risks and all forms of uncertainty [17] plays a very important role in terms of maintaining sovereignty, integrity, and safety from threats both traditional and non-traditional in nature

Figure 2. Screenshot of Ministry of Defense data stolen by hackers and sold on StealthMole

In October, there was a serious incident threatening Indonesia's national security, in which classified data in a Ministry of Defense work unit was leaked and can be accessed through stealthmole web [4]

A hacker with special skills managed to gain access without permission. The hacker then marketed his services on the black market via Twitter (X), with the intention of selling access to confidential documents and administrative rights on the website, backed up with various evidence of misconduct.

In an attempt to prove access, the hacker shared screenshots and stated that the server stored about 1.64 TB of data, from screenshots showing the possibility of hackers successfully hacking the Ministry of Defense website including personnel management information kemhan web backup components, electronic procurement services and digital scripting.

Analysis from the Ministry of Defense suspected the presence of *stealer malware on* the personal computer (PC) of the document administrator, this loss of data can provide significant benefits to irresponsible parties, result in harm to Indonesia's national interests, and potentially worsen the state of national security while increasing the risk of cybercrime.

This study seeks to explore the effectiveness of world crime awareness prevention management techniques in responding to increasingly complex cyber threat dynamics, the aim of this study is to increase public and stakeholder awareness of cyber threats, with the hope of reducing cybercrime incidents.

Therefore, it is necessary to implement a national defense system [18] every institution or organization that has the capacity to respond anticipatively to these threats, and can raise awareness to staff and personnel about cybersecurity risks and increase cybercrime awareness in human resources as well as to prevent data leaks and address cybersecurity threats and build cooperation with other parties to strengthen efforts to prevent and handle cybercrime[19] this complex and multidimensional threat is significantly influenced by changes in the strategic environment and has a major impact on national defense capabilities.

This article can provide valuable policy recommendations for the government and produce effective results for stakeholders in the field of cyber defense, The results of the research can also be a guide for myself, academics and defense practitioners to improve their understanding of the discipline of defense management. So as to strengthen Indonesia's defense capability on national cyber security strategy and cyber crisis management to protect the whole nation and national interests.

2. Research method

This research applies descriptive qualitative research methods, which aim to explain the phenomena that occur in the field through direct observation or observation [18] as well as secondary data collection through literature study, documentation, and interpretation. Data collection through literature study in this research includes document collection, including journals, books, articles, and news contained in newspapers and magazines [19] The data analysis process consists of data collection, data reduction (data condensation), data presentation (data display), and conclusion drawing/verifying [20].

3. Results and discussion

3.1 Increased cyber threat awareness

Digital awareness is very important in preventing cybercrime, in this digital era, internet users must strengthen digital literacy to avoid cybercrime, that this shows the importance of digital awareness in dealing with threats in cyberspace, increased internet usage has led to a significant increase in cybercrime, so knowledge and learning about cybersecurity awareness is very important. Understandingome both from outsiders, such as Web Phishing due to clicking on links carelessly, as well as from within (insiders) [21], we can explore where very worrying condition occurs if the perpetrator of cybercrime is also an expert in anti-cybercrime actions as well, so that the new mode of cybercrime is difficult to detect and solve with cybersecurity [22]. The

escalating frequency of cybercrime attacks poses a pressing issue, demanding swift resolution and immediate implementation of robust cybersecurity measures. Addressing this challenge entails a proactive approach, including the enhancement of digital awareness through training programs, simulations demonstrating the causes and effects of cybercrime, and certification processes to elevate human resource competency in the realm of cyber defense [2] addition, caution and understanding are also required when using apps and digital payments.

By improving and strengthening digital literacy at all levels of society and in all organizations, internet users will more easily avoid cybercrime and protect their personal data from misuse [22] and have taken proactive measures to protect their digital assets. Some countries have even established dedicated cybersecurity teams and invested resources in advanced technologies to mitigate the risks associated with cyberattacks. From the various considerations of the evolving threat, Indonesia needs to quickly realize the significance of cybersecurity and take immediate action to strengthen its defenses.

Among them, through cooperation in strengthening cybersecurity capabilities, Indonesia can safeguard critical infrastructure, protect sensitive data, and reduce potential disruptions that may be caused by malicious cyber activities

Realizing the increasing prevalence of cybercrime in Indonesia, and the many interrelated risks, the need to raise cyber security awareness is a must for individuals and organizations. This requires education of employees and the general public regarding various threats in the digital world, as well as responsible and responsive actions to mitigate these risks [23].

It can be seen how gaining knowledge about current security threats, including implementing best practices, and understanding the potential dangers of activities such as clicking on malicious links or downloading infected attachments will empower individuals to contribute to a safer digital environment both mandatory in an organization then Awareness Cyber security not only plays a role in financial security but also functions to protect sensitive information, thereby reducing the possibility of becoming a victim of cyber threats [24] for organizations, the need to implement a comprehensive security awareness training program is essential. Encouraging a culture of vigilance within the organizational structure further strengthens the security posture, providing protection against the potential adverse impacts of cybercrime.

3.2 Educational programs and skill development

Educational nitiatives and skill development [25] in the field of cyber security awareness in an organization play an important and very useful role in safeguarding sensitive information and mitigating the risk of falling victim to cyber threats, this includes recognizing cyber threats, understanding the associated risks, and implementing safe practices. If the individual employee does not pass certification in global crime awareness, then the use of rewards and punishments in cybersecurity awareness training can have varying impacts on individual behavior and the overall security culture within an organization.

The main goal is to instill a culture of security awareness in the organization [26], enforce regulations to prevent errors if something goes wrong and equip all employees with the knowledge and tools to defend against cyber attacks.

Cybersecurity awareness training typically covers a variety of topics, including recognizing phishing attacks, emphasizing password security, addressing physical security issues, and ensuring the security of mobile devices/computers used is safe from malware.

The importance of cyber security awareness arises from the enormous growth of cybercrime, where cyber attacks pose financial risks and disruption to businesses and individuals, recognizing the human factor as a significant vulnerability, businesses must address potential employee errors and knowledge gaps that can expose organizations to cyber threats, regularly promoting a culture of conversation and awareness through

end-user security awareness training ensures that employees stay informed about the steps necessary to secure personal and business information [27].

In short, educational programs and skills development in cyber security awareness are necessary for both individuals and organizations, serving to protect sensitive information and reduce the likelihood of succumbing to cyber threats. Implementing a comprehensive security awareness training program, coupled with cultivating a vigilant organizational culture, contributes to improving security posture and reducing the risk of falling victim to cyber threats.

4. Conclusions

The conclusion that can be drawn reminds us that increasing cyber security awareness will play an important role in implementing national defense strategy policies as stipulated in Minister of National Defense Regulation Number 14 of 2023 if it is implemented effectively from cyber crime awareness starting with Educational Programs and Skill Development so as to provide benefits for individuals and the Indonesian state and its stakeholders.

Those well-versed in cyber risks are more likely to comply with security policies, thereby minimizing potential security vulnerabilities and promptly reporting suspicious activity within an organization.

In the field of hybrid warfare, digital awareness is becoming increasingly important, especially in combating the wave of cybercrime that accompanies the surge in internet use, a concrete form of overcoming these complex cyber attacks is the need to increase digital literacy and increase awareness of cyber security is very important for individuals and countries, because this can serve as a shield against threats in the vast cyber world.

The diverse nature of cyber threats, both external and internal, adds to the complexity of detection and mitigation efforts. Addressing cybersecurity challenges requires immediate attention from institutions and organizations. Given the increasing frequency of cyberattacks, the authors advocate increasing digital awareness through initiatives such as training, simulations, and certification. This approach aims to increase human resource competency in cyber defense, which ultimately strengthens digital literacy at various levels of society and organizational structures. Such measures can enable more effective use of the internet, reduce the risk of cybercrime and protect personal data.

If seen from neighboring countries (Singapore) that they involve the formation of special cyber security teams and large investments in advanced technology. This success model states the importance of strategic steps for Indonesia. Strengthening cybersecurity capabilities through collaborative efforts is critical to safeguarding critical infrastructure, protecting sensitive data, and mitigating potential disruptions stemming from malicious cyber activity. Recognizing the importance of cyber security, Indonesia must proactively take steps to strengthen its defenses against ever-growing cyber threats.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Acknowledgements

Many thanks are extended to Col. TNI AU Dr. Ir. Hikmat Zakky Almubaroq, S.Pd., M.Si., CIQaR . as Head of the Defense Management Study Program, for his guidance and inspiration in the completion of this article.

Gratitude is also extended to Dr.Ir. Susilo Adi Purwantoro, S.E., M.Eng.Sc., CIQnR., CIQaR., IPU., CIPA., ASEAN Eng, Mayor Jenderal TNI, Mayjen TNI (Purn) Dr. Agung Risdhianto, M.D.A, Brigjen TNI (Purn) Makmur Supriyatno, B.Sc., S.Pd., M. Pd, Kolonel Caj (K) (Purn) Dr. Dra. Herlina Tarigan, MPPM as a mentor acted as a guide for me in completing the final project of the lecture and this article.

References

[1] A. Sarjito, "Hybrid war: fourth generation war," *Defense Management*, vol. 8, no. 1, pp.1-21, 2022.

[2] E. Sebastian, "Increasing the role of human resources in national defense to face fourth-generation warfare," *Defense Journal*, vol 5, no 1, pp. 109-128, 2015.

[3] R. Rachma Kurnia G. Eko Saputro, and S. Murtiana, "Management of human resources in national defense depend on defense economics point of view," *International Journal on Social Sciences, Economics and Arts,* vol. 13, no. 1, pp. 1-11, 2023.

[4] Y. Ginanjar, "Indonesia's strategy to form cyber security in facing cyber crime threats through the country's cyber and encryption agency," *Journal of Global Dynamics*, vol. 7, no. 2, pp. 291-312, 2022, DOI: 10.36859/JDG. v7i02.1187.

[5] A. Razzaq, M. Aditya, A. Widya, O. Kuncoro Putri, D. L. Musthofa, and P. Widodo, "Hacking Tools Attack as a Cyber Threat in the State Defense System (Case Study: Predator)," *Global Political Studies Journal*, Vol. 6, 2022, DOI: 10.34010/GPSCedjournal.v6i1.

[6] M. Christmartha, et al., "The policy strategy of national cybersecurity human resources development to support national defense (a case study at the national cyber and crypto agency 2019)," *Journal of Defense Management*, vol. 6, no. 2, pp. 85-127, 2020.

[7] E. Reichborn-Kjennerud and P. Cullen, "What is hybrid warfare?" [online]. Norwegian Institute for International Affairs (NUPI) is collaborating with JSTOR, 2016.

[8] A. Anggono and M. Riskiyadi, "Cybercrime and cybersecurity at fintech: a systematic literature review," *Journal of Management and Organization (JMO)*, vol. 12, no. 3, pp. 239-251, 2021.

[9] M. James, "Strategic Readiness," in *The International Encyclopedia of Strategic Communication*, Wiley, 2018, pp. 1-5. DOI: 10.1002/9781119010722.IESC0178.

[10] A. Munir, A. Aved, and E. Blasch, "Situational awareness: techniques, challenges, and prospects," *AI (Switzerland)*, vol. 3, no. 1, pp. 55-77, 2022, DOI: 10.3390/AI3010005.

[11] S. Chen *et al.*, "Exploring the global geography of cybercrime and its driving forces," *Humanit Soc Sci Commun,* vol. 10, no. 1, 2023, DOI: 10.1057/S41599-023-01560-X.

[12] A. Sarjito and Z. Almubaroq, "Defense management and its implications on state sovereignty." *Journal of Defense Management,* vol. 9, no. 1, pp. 166-187.

[13] L. Maria ulfah, A. Sudarya, N. Lelyana, and C. Sri Marnani, "Implementation of the policy of deploying the Joint Command of Defense Area I to support the national defense system." *Journal of Defense Management,* vol 7., no. 1, pp. 39-52, 2021.

[14] T. Haryono, Y. Swastanto, and S. Hadi Sumantri, "Human resource development through the collaboration of universities, professional organizations, industry, and government in the defense industry as an important part of the state defense strategy Human resources development through the collaboration of universities, professional organizations, industries, and governments in the defense industry is an important part of the state defense strategy." *National Defense & Defense Journal*, vol. 12, no. 1, pp. 62-76, 2022.

[15] A. Sarjito and Z. Almubaroq, "Defense management and its implications on state sovereignty." *Journal of Defense Management,* vol 9, no. 1, pp. 166-187, 2022.

[16] B. R. Sanjaya *et al.*, "Development of cyber security in the face of cyber warfare in Indonesia," *Journal of Advanced Research in Defense and Security Studies*, vol. 1, no.1, pp. 19-34, 2022.

[17] R. Ramadhianto, S. Lumban Toruan, S. Nefo, H. Kertopati, and Z. Almubaroq, "Analysis of presidential regulations concerning cyber security to bolster defense policy management," *Defense and Security Studies*, vol. 4, pp. 84-93, 2023, doi: 10.37868/dss.v4.id244.

[18] J.W. Creswell, D.J. Creswell, Research Design Qualitative, Quantitative, and Mixed Methods Appproaches, Fifth edition, SAGE Publications Inc., California, 2018.

[19] F. Rita Fiantika, M. Wasil, and S. Jumiyati, *Qualitative research methodology*. [online]. Publisher: PT. Global Executive Technology, IKAPI Member Number: 033/SBA/2022, West Sumatra.

[20] E. Murdianto, Qualitative Research Methods, Institute for Research and Community Service UPN "Veteran", Yogyakarta Press, April, 2022.

[21] S. Back and R. T. Guerette, "Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks," *J Contemp Crim Justice*, vol. 37, no. 3, pp. 427-451, 2021, doi: 10.1177/10439862211001628.

[22] A. Razzaq, M. Aditya, A. Widya, O. Kuncoro Putri, D. L. Musthofa, and P. Widodo, "Hacking tools attack as a cyber threat in the country's defense system (case study: predator)," *Global Political Studies Journal*, vol. 6, 2022, DOI: 10.34010/GPSCedjournal.v6i1.

[23] K. F. Mccrohan, K. Engel, and J. W. Harvey, "Influence of Awareness and training on cyber security," *Journal of Internet Commerce*, vol. 9, no. 1, pp. 23-41, 2010, doi: 10.1080/15332861.2010.487415.

[24] I. Rahmawati, "The Analysis of cyber crime threat risk management to increase cyber defense", *National Seminar on Indonesian Science Technology and Innovation (SENASTINDO AAU)*, vol. 1, no.1, pp. 299-306, 2019, ISSN 2685-899.

[25] A. Frimayasa, W. Desty Febrian, and U. Dian Nusantara, "Effect of reward and punishment on employee performance," *International journal of social and management studies (ijosmas)*, vol. 2, no. 3, pp. 179-186, 2021.

[26] D. Azwar, "Analysis the effect of reward and punishment effect on performance with working discipline as intervening variable (a case study of employee at the culture and tourism office sungai penuh city)", *American Journal of Humanities and Social Sciences Research (AJHSSR)*, ISSN:2378-703X, vol 4, no. 8, pp. 435-444, 2020.

[27] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for security education, training and awareness (seta) program effectiveness: a lifecycle model," *Information Technology and People*, vol. 36, no. 8, pp. 94-125, 2023, doi: 10.1108/ITP-07-2022-0515.