SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 02 (2025), pp. 129-138
Research Article
doi: https://doi.org/10.70710/sitj.v2i2.41

Collaborative State Apparatus Strategy in Countering Autonomous Drone Threats to the President and Vice President of the Republic of Indonesia

Sigit Yudha Pratama[1,a,*]

[1]Sekolah Tinggi Intelijen Negara, Bogor
[a]yudhasigit12@gmail.com
*Corresponding author

Article Info
Received: 25-Mar-2025
Revised: 6-May-2025
Published: 6-Jun-2025

Keywords
AI Detection; Autonomous Threats; Counter-drone; Security Collaboration; VIP Protection

Abstract
This research aims to develop a strategic collaboration model in addressing autonomous technology threats to high-ranking state officials, focusing on the integration of the roles of the Indonesian National Armed Forces (TNI), the Indonesian National Police (Polri), and the State Intelligence Agency (BIN). Autonomous technology threats, particularly drones, are a primary concern in safeguarding the President and Vice President of the Republic of Indonesia. This study proposes the use of artificial intelligence (AI)-based technology to efficiently and swiftly detect and neutralize drone threats. Additionally, scenario-based simulations of modern threats are applied to enhance readiness and the effectiveness of security measures. The research employs a descriptive qualitative approach with a case study, involving primary data collection through in-depth interviews with relevant officials, as well as secondary data from literature studies and direct observations. The findings show that collaboration between TNI, Polri, and BIN, supported by AI technology and threat simulations, can strengthen the security system for high-ranking state officials in the digital era. This research contributes to the development of policies and strategies for more effective security measures in facing autonomous technology threats in Indonesia.

1. Introduction

Industry 4.0 has triggered rapid advancements in technology, including in the field of autonomous systems or autonomous technology. This technology enables devices or systems to operate independently without requiring direct human supervision or intervention. Examples of the implementation of autonomous technology include industrial robots, self-driving cars, drones, autonomous defense systems, and more. Initially, autonomous technology was designed to ease the human workload across various sectors, such as manufacturing, transportation, space exploration, and other fields that demand precision, efficiency, and sustainability in operations (Chen, Sun, & Wang, 2022). However, behind the promised benefits, the presence of autonomous technology also raises concerns about its potential misuse for malicious purposes, including threats to the security of state leaders. The President and Vice President of the Republic of Indonesia, as the highest figures of state leadership, play a central and crucial role in overseeing the governance process and ensuring the continuity of the nation's survival and sovereignty. Their security and safety are of utmost priority in efforts to maintain national stability. However, in today's digital era, threats to the security of the President and Vice President no longer come only in conventional

forms, such as terrorism or coups, but can also emerge through the exploitation of advanced technologies like autonomous technology (Mukhammadsidiqov & Turaev, 2020).

One of the real threats posed by autonomous technology is the use of drones or unmanned aerial vehicles (UAVs) that are remotely controlled. Drones, also known as Remotely Piloted Aircraft Systems (RPAS), have rapidly evolved in recent years. Initially designed for military purposes, drones are now used across various civilian sectors, such as area mapping, environmental surveillance, aerial photography, and goods delivery. Modern drones come in a wide range of sizes and designs, from small quadcopters for personal use to large, unmanned aircraft for military missions. Thanks to technological advancements, drones are now equipped with advanced sensors, such as high-resolution cameras, thermal sensors, radar, and precise GPS navigation systems, making them highly versatile and powerful tools for various applications (Quamar, Al-Ramadan, Khan, & Shafiulla, 2023). In terms of security, drones have proven to be handy tools for law enforcement and security teams. Drones can be utilized for surveillance of large areas, crowd monitoring, search and rescue operations, and rapid mapping of disaster sites. Their ability to cover vast terrains and provide real-time data makes drones indispensable in ensuring public safety and effectively responding to emergencies. Drones also allow security personnel to gather critical information from a safe distance, enhancing both efficiency and security during operations (Yaacoub, Noura, Salman, & Chehab, 2020). However, the same capabilities that make drones valuable also make them a serious potential threat if they fall into the wrong hands. With autonomous systems in place, drones can be infiltrated and misused for unintended purposes, such as attacking specific targets. Several incidents in various countries have demonstrated how drones can be used to disrupt airport operations, conduct illegal surveillance, or even carry dangerous payloads. This dual nature of drones, serving both as a tool for security and as a potential weapon, highlights the need for stringent control and countermeasures to prevent malicious use and ensure that drones are used only for legitimate and safe purposes (Lykou, Moustakas, & Gritzalis, 2020). The ability of drones to fly at low altitudes, move quickly, and evade detection by conventional radar makes them a threat that is difficult to anticipate (Coluccia, Parisi, & Fascista, 2020). The challenge in addressing drone threats lies not only in the technical capabilities of the drones themselves but also in the accessibility and proliferation of this technology (Calcara, Gilli, Gilli, & Marchetti, 2022). Commercial drones with advanced capabilities are now widely available in the consumer market, and components to build custom drones are also easily accessible (Kapustina, Izakova, Makovkina, & Khmel, 2021). This means that individuals or groups with limited resources now have the potential to access technology that was once only available to the military or government institutions (Kasapoğlu & Kırdemir, 2022). In response to the drone threat, many countries have started developing anti-drone defense systems or counter-UAS (C-UAS) (Popescu, 2021). These systems generally consist of multiple layers of defense, including detection, identification, tracking, and neutralization (Castrillo, Manco, Pascarella, & Gigante, 2022). Detection technologies can include specialized radar, acoustic sensors, and optical/thermal camera systems (Dudczyk, Czyba, & Skrzypczyk, 2022). For neutralization, various methods have been developed, ranging from signal control and GPS jamming, the use of nets or projectiles to capture drones, to the use of high-power lasers to damage critical components of the drone (Martins, Michel, & Silkoset, 2020).

In Indonesia, awareness of the potential drone threat has begun to increase. Several incidents, such as the appearance of unidentified drones around the presidential palace or other vital areas, have triggered serious discussions about the need for stricter regulations and defense systems (Chamola, Kotesh, Agarwal, Gupta, & Guizani, 2021). The Indonesian government, through various relevant agencies, has begun taking steps to address this threat. The National Cyber and Crypto Agency (BSSN), for example, has started developing capabilities to detect and mitigate drone threats. The Indonesian National Armed Forces (TNI) and the National Police (Polri) have also conducted training and procured equipment to address small-scale air threats, including drones (Siswoputro, Suseto, Widjayanto, & Prakoso, 2024). However, given the complexity and rapid development of drone technology, a more comprehensive and collaborative approach is needed (Masyhar & Emovwodo, 2023).

In an era of rapid technological advancements, threats to the security of high-ranking state officials, particularly the President and Vice President of the Republic of Indonesia, have become increasingly complex and diverse. One of the latest challenges is the potential threat posed by autonomous technology. To address the threat of autonomous technology to the President of the Republic of Indonesia, effective collaboration among various state instruments is required. State instruments, as outlined in the 1945 Constitution and other relevant laws and regulations, refer to the institutions that play a crucial role in safeguarding the security and sovereignty of the nation. The 1945 Constitution explicitly mentions two main state instruments: the Indonesian National Armed Forces (TNI) and the Indonesian National Police

(POLRI) (Satria & Efendi, 2021). The Indonesian National Armed Forces (TNI) is responsible for defending, protecting, and maintaining the integrity and sovereignty of the nation. At the same time, the Indonesian National Police (Polri) is tasked with maintaining public security and order, protecting, serving, and assisting the public, as well as enforcing the law. In addition, although not directly mentioned in the 1945 Constitution, the State Intelligence Agency (BIN) is also a state instrument established by law. Article 10, paragraph (1) of Law No. 17 of 2011 on State Intelligence emphasizes that BIN is a state instrument that carries out intelligence functions both domestically and internationally. Therefore, strategic collaboration between TNI, Polri, and BIN becomes crucial in addressing the increasingly complex threat posed by autonomous technology to the security of the President of the Republic of Indonesia.

In an era of rapid technological advancement, threats to the security of state leaders have become increasingly complex, including autonomous technology that could potentially be used for malicious purposes. One critical aspect in ensuring the security of the President of the Republic of Indonesia is airspace management, particularly around strategic areas such as airports. Research by Supriyadi et al. (2023) shows that Research modeling no-fly zones at Halim Perdanakusuma Airport using remote sensing data shows that the density of buildings around takeoff and landing areas can increase the risk of aviation accidents. Therefore, collaboration between various state instruments in formulating spatial planning policies that consider aviation safety becomes crucial. This policy is not only relevant to flight safety but also serves as part of a strategy for protecting against autonomous technology threats that could jeopardize the security of the President. Thus, this research provides a strong foundation for developing collaborative strategies to address such threats through effective management of the environment around strategic areas.

2. Literature Review

2.1. Autonomous Technology

Autonomous technology or autonomous systems is a significant breakthrough in the world of modern technology. At its core, this technology refers to devices or systems that can operate independently without requiring direct human control or intervention. These autonomous systems are equipped with capabilities for environmental perception, decision-making, and actuation or the execution of actions independently, without human involvement (Singh & Saini, 2021). The environmental perception capability of autonomous systems enables them to collect and process information from their surroundings through various sensors, such as cameras, radar, lidar (light detection and ranging), and other sensors. This collected information is then processed and analyzed by the system to build a comprehensive understanding of the situation and the surrounding environmental conditions (Chen, Sun, & Wang, 2022).

Armed with this understanding, autonomous systems are then able to make decisions independently based on algorithms and logic that have been programmed into them. This decision-making process involves data analysis, risk evaluation, and selecting the most appropriate action to achieve a goal or complete a specific task. Autonomous systems can learn and adapt to new situations, allowing them to make the right decisions even in complex or unpredictable conditions. After making a decision, the autonomous system then performs actuation or executes actions independently. This can be done through various mechanisms, such as motor drivers, actuators, or even weapon systems, depending on the specific purpose and function of the autonomous system. This actuation process is carried out without the need for direct human intervention or control, allowing the autonomous system to operate independently and efficiently.

2.2. Autonomous Technology Threats

According to the Republic of Indonesia Law No. 34/2004, a threat is any effort or activity carried out, either domestically or internationally, that can pose a danger to the unity, sovereignty, integrity, and safety of a country and its people. Meanwhile, Law No. 17 on State Intelligence states that a threat can be understood as any action, effort, work, or activity originating from both domestic and foreign sources, which is perceived or proven to endanger the safety of the nation, security, sovereignty, territorial integrity of the Republic of Indonesia, and national interests in various aspects such as ideology, politics, economy, socio-culture, and defense and security.

Although autonomous technology was created with the aim of helping to lighten human workload and improve efficiency in various sectors, its existence also raises concerns about its potential misuse for malicious purposes. With the ability to operate independently without human intervention, this technology could be exploited by certain parties to carry out actions that threaten the security and safety of the public (Felski & Zwolak, 2020). In facing these threats, it becomes crucial to develop strict regulations and policies regarding the use of autonomous technology. Additionally, collaboration between the government, security agencies, and the technology community is necessary to ensure that this technology is used responsibly and not misused for malicious purposes that could threaten public security and safety.

2.3. State Instruments Collaboration Strategy

In facing the increasingly complex and rapidly evolving threats posed by autonomous technology, a solid and coordinated collaborative strategy is required among all state instruments. Collaboration between institutions such as the Indonesian National Armed Forces (TNI), the Indonesian National Police (POLRI), the State Intelligence Agency (BIN), and other relevant agencies is key to optimizing resources, capabilities, and authorities in efforts to prevent and address these threats. State instruments, as outlined in the 1945 Constitution and various laws and regulations, include the Indonesian National Armed Forces (TNI), the Indonesian National Police (Polri), and the State Intelligence Agency (BIN). These three institutions play complementary roles in the national security system for protecting the head of state.

TNI, through the Presidential Security Force (Paspampres), is directly responsible for the physical protection of the President, Vice President, and their families within the framework of military operations other than war (OMSP). Polri plays a crucial role in maintaining security in the surrounding areas and handling threats of a criminal nature. Meanwhile, BIN, which operates based on Law No. 17 of 2011 on State Intelligence, plays a strategic role in gathering and analyzing intelligence related to potential threats, including its duty to coordinate efforts to protect national leaders from threats, challenges, obstacles, and disturbances, especially those originating from autonomous technology.

Collaboration between TNI, Polri, and BIN becomes very important in facing the threats posed by autonomous technology. TNI can implement physical security based on information provided by BIN, and Polri can enhance surveillance in high-risk areas. In contrast, BIN provides real-time intelligence and technological support for swift and precise action. However, given that autonomous technology threats are new and continuously evolving, a more effective and adaptive collaboration strategy is needed. Therefore, this research aims to analyze and formulate a collaboration strategy between state institutions in addressing the autonomous technology threats to the President of the Republic of Indonesia, to strengthen the head of state's security system in the digital age.

2.4. Regulations and Policies Related to Autonomous Technology

The rapid development of autonomous technology demands clear regulations and policies to govern its use. Several countries and international organizations have developed guidelines, particularly in the fields of military and weaponry. Globally, the UN Convention on Conventional Weapons (CCW) prohibits the use of fully autonomous weapon systems that are completely detached from human control. The Government Group of Experts (GGE) under the CCW is formulating rules and ethical principles for the use of autonomous weapon systems, although no binding agreements have been reached. At the regional level, the European Union has issued ethical guidelines for the development of artificial intelligence (AI) technology, emphasizing the importance of human control. Meanwhile, Indonesia does not yet have specific regulations related to autonomous technology. Still, several laws and regulations may serve as a basis, such as the National Defense Law, the Defense Industry Law, Minister of Transportation Regulation No. 63 of 2021 on drones, the Electronic Information and Transactions Law (ITE Law), and cybersecurity regulations.

National policies are also needed to address the ethical aspects, security standards, monitoring mechanisms, and limitations on the use of autonomous technology in both civilian and military sectors. The government, through the Ministry of Defense and relevant agencies, needs to develop comprehensive rules to ensure that this technology is used responsibly, safely, and not misused. Strong regulations will provide a clear legal foundation, encourage positive technological development, and strengthen international collaboration in the global governance of autonomous technology.

3. Method

This research employs a descriptive qualitative method with a case study approach to explore the threats of autonomous technology to the President and Vice President of the Republic of Indonesia, as well as the collaborative strategies of state instruments in addressing these threats. Primary data is collected through in-depth interviews with officials from relevant agencies, academics, and cybersecurity experts, while secondary data is gathered from literature studies, journals, regulations, and official reports. Data collection techniques include semi-structured interviews, literature review, and direct observation, which are analyzed inductively using a thematic approach. The validity of the data is ensured through source and method triangulation. At the same time, ethical principles such as confidentiality, informed consent, non-harm, and objectivity are applied to maintain the integrity of the research. The findings of this study are expected to provide strategic recommendations for enhancing the collaboration of state instruments to address the threats posed by autonomous technology.

4. Results and Discussion

4.1. Threats of Autonomous Technology to the President and Vice President of the Republic of Indonesia

The research reveals that autonomous technology, particularly drones, is increasingly being utilized by both state and non-state actors worldwide for various purposes such as direct attacks, surveillance, sabotage, and spreading disinformation. This technology is highly flexible and operationally capable, enabling its use in diverse contexts, both military and non-military. In Indonesia, officials from the Indonesian National Army (TNI), the Indonesian National Police (POLRI), the National Intelligence Agency (BIN), and the Presidential Security Force (Paspampres) have shared through in-depth interviews that the threat of this technology is grave, especially considering the global trend of drone utilization in military operations and unconventional tactics. Drones, as autonomous technology, can be operated remotely or autonomously with pre-programmed commands. These drones can be modified to carry payloads such as surveillance cameras, firearms, explosives, or even chemical and biological weapons. Their autonomous capabilities allow them to avoid radar detection by flying at low altitudes or through routes that are difficult to reach by traditional monitoring technologies. TNI notes that the threat has intensified with advances in drone technology, enabling precision strikes on specific targets, including presidential convoys or state events.

TNI also refers to the use of drones in military operations by countries such as Russia, the United States, and Iran, where drones are used for precision strikes against both military and civilian targets. A concrete example is the drone attack on the Saudi Arabian airport and oil facilities, which crippled vital infrastructure at a relatively low operational cost. This demonstrates that both state and non-state actors can exploit drones for attacks that cause significant damage but are difficult to trace. The threat is even more relevant due to the growing use of drones in urban areas and sensitive regions. Reports from Paspampres mention incidents of drones approaching the president's location without official authorization, which, although not always resulting in direct attacks, could be used for gathering strategic intelligence that threatens the safety of the head of state. One of the main challenges in countering this threat is the difficulty in detecting and preventing it. Many modern drones can fly at low altitudes that are hard to detect with conventional radar, and their small size adds to the complexity of tracking them. Incidents of commercial drones flying without authorization in no-fly zones highlight the limitations of existing detection systems. To address this, the Ministry of Transportation has implemented regulations such as PM 37 of 2020, which governs no-fly zones and drone operator registration procedures. However, implementation still requires improvements in technology and personnel.

The study also finds that non-state actors, such as terrorist groups and criminal organizations, can modify drones to attack military facilities, smuggle weapons, or spread propaganda. BIN highlights that drones are frequently used for reconnaissance, especially at borders and other critical areas. POLRI mentions that several cases of drone misuse have been found, and unregistered drones are often difficult to track due to advanced technology designed to evade detection. This threat underscores the need for stronger regulations and expanded detection and monitoring capabilities. As a mitigation measure, Paspampres and the TNI have developed anti-drone technologies, such as jamming systems to disrupt drone signals and specialized radar to detect small objects at low altitudes. In VVIP security simulations,

this technology has successfully turned off several drones, although its effectiveness remains limited to certain areas. Expanding the coverage of anti-drone technology is crucial to protecting high-ranking officials in remote regions. Further development is also necessary to tackle advanced drones operating without control signals.

The Indonesian government has implemented security policies through regulatory and operational approaches, including the establishment of no-fly zones around VVIP areas and strategic facilities. The Ministry of Transportation works with the TNI, POLRI, and Paspampres to ensure that all drone activities are monitored and can be halted if necessary. However, inter-agency coordination remains a challenge, particularly in sharing information in real-time. Enhanced communication and intelligence technologies are required to support rapid responses to threats. Domestic technology development is a priority to strengthen national security. The TNI has collaborated with local defense industries to create anti-drone technologies tailored to Indonesia's operational needs, while also reducing reliance on foreign technologies. The Ministry of Transportation is also active in international forums such as JARUS to align national regulations with global standards, ensuring the adoption of the best technologies to handle drone threats.

4.2. Collaboration of State Apparatus Roles in Addressing Autonomous Technology Threats

This research highlights the growing complexity of threats posed by autonomous technology, particularly in the context of national security and the safety of high-ranking officials like the President and Vice President of the Republic of Indonesia. As these technological advancements evolve, it is essential to develop more robust intelligence strategies and better coordination among key security agencies such as the Indonesian National Army (TNI), the Indonesian National Police (POLRI), and the National Intelligence Agency (BIN). These institutions play integral roles in safeguarding national security, and their effective collaboration is necessary to address the diverse threats posed by autonomous systems, such as drones. Coordination between these agencies is critical to ensure a seamless and effective response to emerging threats. Through strategic collaboration, they can share intelligence, coordinate actions, and pool resources to prevent or mitigate risks. The main challenge, however, lies in optimizing the use of intelligence across multiple institutions. As each agency specializes in different areas of security, effective communication, data sharing, and real-time coordination are essential to prevent any gaps in protection.

BIN, as the lead intelligence agency, has a critical role in early detection and continuous monitoring of activities that may pose a threat to national security. With autonomous technology becoming increasingly accessible, especially in the form of drones, there is an urgent need for advanced monitoring systems to detect and identify these threats. BIN can leverage technologies such as airspace dashboards, which integrate flight data from both manned aircraft and unmanned aerial vehicles (UAVs), supported by cutting-edge artificial intelligence (AI). This system allows for real-time tracking and identification of drones, even in sensitive and high-risk areas such as presidential palaces, airports, and critical infrastructure facilities. By utilizing AI algorithms, BIN can identify unusual flight patterns, detect rogue drones, and trace the location of operators, significantly improving early warning capabilities.

Moreover, improving coordination between agencies is vital to enhance operational readiness. Joint exercises involving TNI, POLRI, and BIN are essential for testing preparedness to respond to various threat scenarios, particularly drone attacks targeting key personnel, such as the President. These exercises allow the agencies to refine their Standard Operating Procedures (SOPs), ensuring that each agency understands its role in securing high-profile individuals and sensitive areas. Paspampres, which is responsible for the direct security of the President, has updated its SOPs to include anti-drone protocols in response to the evolving nature of the threats. However, challenges remain in terms of real-time communication and the seamless coordination of efforts on the ground. Units in the field need to have access to up-to-date intelligence and actionable data to respond promptly and effectively to threats.

The research also identifies obstacles in the flow of intelligence, particularly related to delays in processing and distributing data due to technical and bureaucratic constraints. The differing communication systems and technologies across agencies often hinder the speed of decision-making and response times. To address these issues, the development of an integrated communication system based on real-time networking is crucial. Such a system would allow agencies to exchange information quickly, enabling a coordinated response to threats as they arise. In addition, streamlining the bureaucratic

processes involved in intelligence processing and data distribution would expedite the sharing of vital information, ensuring that decision-makers have access to the intelligence they need when they need it. In order to address the rapidly evolving nature of autonomous threats, particularly those involving drones, BIN has proposed investing in AI-based technologies to accelerate data analysis and improve threat detection accuracy. AI can enhance the speed and precision of identifying potential threats, allowing security agencies to respond proactively rather than reactively. However, in order to maximize the effectiveness of these technologies, personnel across all relevant agencies must be adequately trained. Intensive training programs should be implemented to ensure that security officers are proficient in using AI tools and systems, thereby enabling them to analyze and respond to emerging threats quickly.

Furthermore, fostering collective learning among agencies is crucial. Sharing knowledge and experiences from joint exercises can help agencies refine their strategies and enhance their capabilities in addressing autonomous technology threats. TNI and POLRI, for example, can benefit from BIN's expertise in intelligence gathering and threat analysis, while BIN can gain valuable insights into operational security practices from TNI and POLRI. This cross-agency collaboration can help develop a more comprehensive approach to countering autonomous threats. To facilitate this, it is essential to establish an integrated training center where personnel from TNI, POLRI, BIN, and Paspampres can train together. Such a center would provide an environment for joint training, where agencies can practice coordinated responses, learn best practices, and refine their procedures for dealing with threats. Through these exercises, personnel can enhance their readiness, improve interagency communication, and develop better strategies for addressing the growing threat of autonomous technology. Finally, as autonomous technology continues to advance, there is a need for greater investment in domestic technology development. Relying solely on foreign technologies may expose national security to risks, such as vulnerabilities in foreign-made systems or geopolitical tensions that could limit access to critical technologies. Therefore, TNI has been working closely with local defense industries to develop anti-drone technologies tailored to Indonesia's specific needs. This not only strengthens Indonesia's ability to defend against autonomous threats but also reduces its dependence on foreign technologies, ensuring greater national security autonomy. Similarly, the Ministry of Transportation has been actively participating in international forums like JARUS (Joint Authorities for Rulemaking on Unmanned Systems) to align Indonesia's regulations with global standards, ensuring that the country is adopting the best practices in countering autonomous technology threats.

4.3. Development of Domestic Technology and Implementation of Collaborative Strategies

In facing increasingly complex autonomous technology threats, the Indonesian government has prioritized the development of domestic technology as a strategic move. This step aims to reduce dependency on foreign technology and strengthen the national security system by utilizing local innovations and resources. This study shows that the development and application of domestic technology, particularly in drones and anti-drone systems, is crucial to ensure Indonesia's capacity to counter autonomous technology threats effectively. The Indonesian National Armed Forces (TNI) plays an active role in local drone technology development, collaborating with domestic defense industries and academic institutions to create technology suited to national defense and security needs. This project includes the development of various types of drones, including reconnaissance drones for area monitoring and surveillance operations, as well as defense drones designed for combat air missions. The goal is to enhance national air surveillance capabilities and reduce dependency on imported drones that are vulnerable to security breaches and availability issues.

In addition to operational drones, TNI is also developing domestic anti-drone systems utilizing radar and jamming technology. These systems are designed to detect drones entering no-fly zones and neutralize them before they pose a threat. Radar technology is developed to detect small objects flying at low altitudes. In contrast, jamming technology focuses on disrupting the communication signals between the operator and the drone, thereby forcing the drone to land safely or be controlled. However, the development of this technology faces several significant challenges. The Ministry of Transportation (Kemenhub) and the Indonesian National Police (POLRI) note that the process of developing local drone and anti-drone technology requires considerable time and resources. This is due to the complexity of technology that must be adapted to Indonesia's geographical and operational conditions, as well as the need to meet high-performance and security standards. Additionally, the development of new technology requires extensive testing and adjustments to ensure reliability and effectiveness in the field.

Kemenhub and POLRI emphasize the importance of cross-sector collaboration in accelerating the development of this technology. They encourage collaboration with private industries, research institutions, and universities to leverage existing knowledge and research capacity. This collaborative effort is seen as vital to speeding up technological innovation and ensuring that the results of the development can be swiftly implemented into national security strategies. The domestic defense industry is also encouraged to take a larger role in the development and production of anti-drone technology so that it can be rapidly integrated into the operational systems of TNI and POLRI. Inter-agency collaboration is a key foundation in responding to autonomous technology threats, particularly in terms of policy implementation and oversight. Kemenhub, as the authority responsible for regulating airspace and aviation regulations, continues to coordinate with TNI and POLRI to ensure that surveillance in critical areas such as airports, vital national assets, and sensitive airspace operates effectively. Kemenhub is also actively involved in drafting new, more comprehensive policies related to drone use and monitoring in Indonesia, focusing on improving regulations and law enforcement against violations involving unregistered or unauthorized drones.

TNI and POLRI, in their efforts to address threats more effectively, have formed specialized task forces trained to handle drone threats and carry out VVIP security with high standards. These task forces are designed to integrate TNI's operational expertise, which has experience in military security and anti-drone technology, with POLRI's law enforcement and rapid-response capacity. This synergy aims to create operational units that can act quickly and effectively in the field, particularly in situations involving drone threats. The formation of these specialized task forces is based on the need to integrate the capabilities and technologies possessed by each agency. TNI, which has access to advanced anti-drone technology and military operational strategies, focuses on securing rings 2 and 3 in the layered security system protecting the president and senior officials. POLRI, on the other hand, is responsible for law enforcement and quick responses to violations in civilian areas. POLRI also ensures that drone surveillance in public areas complies with the regulations set by Kemenhub.

This study reveals that the collaboration between Kemenhub, TNI, and POLRI is not only focused on technology implementation but also on enhancing policies and regulations. They work together to identify gaps in existing regulations and develop new, stricter, and more effective policies. For example, they have developed a more comprehensive registration and licensing system for commercial and civilian drones, as well as introduced heavier penalties for violators involved in illegal or unregistered activities. Kemenhub also facilitates training and outreach programs for drone operators to ensure they understand the rules and procedures to be followed, especially in the context of operations near sensitive areas. They work with the drone industry and the civil aviation community to ensure that drone operators are well-informed about no-fly zones and safety protocols that must be followed. This outreach is essential to prevent unwanted incidents and ensure that any legitimate drone use can be effectively monitored and controlled.

The study also finds that the integration between domestic technology and national security policies is crucial to ensure the success of security strategies against autonomous technology threats. This integration ensures that local technology development aligns with national defense and security priorities, making the national security system more resilient and adaptable to evolving risks. Inter-agency collaboration, such as between TNI, Kemenhub, BIN, and POLRI, enables a coordinated response to autonomous technology threats, particularly drones. By combining advanced technological solutions with a robust policy framework, Indonesia aims to enhance its ability to monitor, detect, and neutralize drone-related threats efficiently.

4.4. Integrated Approach to Countering Autonomous Technology Threats

This study reveals that the threat of autonomous technology to the security of the President and Vice President is highly complex and involves various aspects such as physical security, technology, and intelligence coordination. This demonstrates that addressing this threat cannot be handled by a single agency alone but requires an integrated approach and cooperation among various security agencies, including the Indonesian National Armed Forces (TNI), the Indonesian National Police (POLRI), the National Intelligence Agency (BIN), and the Ministry of Transportation (Kemenhub). To achieve optimal results in threat mitigation, advanced technological support, an efficient communication system, and clear and coordinated operational procedures are necessary. This research also shows that although the TNI has implemented anti-drone technology in several VVIP security operations, its effectiveness still varies depending on operational conditions and the type of threat faced. The anti-drone technology currently used

is primarily based on jamming systems, which function to interfere with the signal between the drone and its operator. However, this system has limitations, particularly when facing small drones or those flying at low altitudes, which often go undetected by conventional radar. TNI is developing more advanced detection systems, combining high-frequency radar and thermal cameras, which are expected to improve detection effectiveness, especially in strategic areas.

The importance of developing real-time communication systems is also highlighted in this research. The speed of information exchange is crucial in responding to threats quickly, as drones can operate within very short time frames. BIN recommends the development of a real-time communication network system that allows seamless access to information. This will integrate the technologies used by TNI, POLRI, and Kemenhub, so that each unit can communicate directly and access intelligence data from a single control center. The development of this system will accelerate responses to drone threats and enhance interoperability among the technologies used by these agencies. However, implementing this system requires significant investment in technology and personnel training, particularly to ensure that both hardware and software can operate in various conditions, including remote areas with limited access. Additionally, practical training for personnel is crucial so they can operate this system efficiently and understand new communication protocols. The success of handling autonomous technology threats also heavily depends on coordination and collaboration among security agencies. Although there has been collaboration between TNI, POLRI, BIN, and Kemenhub, this study finds that there is still room for improvement, particularly concerning the integration of information and operational procedures. Information-sharing processes between agencies are often hampered by bureaucracy and differences in the systems used, which can slow the response to threats. Therefore, it is necessary to harmonize Standard Operating Procedures (SOPs) across agencies so that information exchange can occur rapidly, and responses to emergencies can be taken promptly. BIN recommends that the SOPs used by each agency be aligned with international standards and operational needs in facing autonomous technology threats. This includes establishing more efficient communication protocols, using integrated technologies, and conducting joint training to ensure each unit understands its role in security operations.

Collaboration between agencies should also be strengthened through regular joint exercises, where various agencies can train together to simulate threat scenarios and test the operational readiness of their units in handling these threats. This will help identify potential weaknesses in operational procedures and find solutions to address these issues before a real threat occurs. Joint exercises will also strengthen relationships between agencies, build trust among parties, and enhance the synergy needed to face increasingly complex threats. Overall, this study demonstrates that addressing the autonomous technology threats to the security of the President and Vice President requires a more integrated and coordinated approach. Only through solid collaboration between agencies, the development of innovative technologies, and efficient communication systems can Indonesia improve its ability to respond to autonomous technology threats and maintain national security more effectively.

5. Conclusion

Based on the research findings, it can be concluded that the threat of autonomous technology, particularly drones, to the security of the President and Vice President of Indonesia is a real and multidimensional threat. This threat requires an integrated response, involving various security agencies such as the Indonesian National Army (TNI), the Indonesian National Police (POLRI), the National Intelligence Agency (BIN), the Ministry of Transportation (Kemenhub), and the Presidential Security Force (Paspampres). Autonomous drones can operate without direct human control, creating serious potential threats such as surveillance, carrying hazardous payloads, and detection challenges. Although the roles of TNI, POLRI, and BIN are crucial, they face obstacles such as limited resources, reliance on foreign technology, and the lack of specific regulations related to autonomous technology. Collaboration among agencies still requires improvement due to differences in jurisdiction, communication, and intelligence limitations. Therefore, the strategy for optimizing collaboration should include enhancing inter-agency coordination, more effective information sharing, regulatory development, and increasing technological capacity and human resources to address the evolving threats.

The recommendations from this study cover several academic and practical aspects. Academically, contributions to the development of national security theory and inter-agency collaboration need to be strengthened, with a focus on further research examining autonomous technology threats and inter-agency cooperation in addressing these threats. On the practical side, there is a need to refine regulations related

to the use and control of autonomous technology, including restrictions on its use in public spaces, regulation of drone ownership and operations, and the implementation of sanctions for its misuse. Additionally, it is essential to increase the budget for the development of detection technologies and anti-drone defense systems to enhance early detection capabilities. Inter-agency synergy should also be improved through joint training programs that include scenarios for handling autonomous technology threats, cross-agency coordination, and crisis response. Public awareness of the potential threats posed by autonomous technology and the importance of community participation in reporting suspicious activities should also be prioritized. Finally, international cooperation in information exchange, global regulations, and the development of anti-drone defense technologies must be strengthened to enable Indonesia to leverage the experience and technology of other countries.

References

Calcara, A., Gilli, A., Gilli, M., & Marchetti, R. (2022). Why drones have not revolutionized war: The enduring hider-finder competition in air warfare. *International Security, 46*(4), 130-171.

Castrillo, V. U., Manco, A., Pascarella, D., & Gigante, G. (2022). A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones, 6*(3), 65.

Chamola, V., Kotesh, P., Agarwal, A., Gupta, N., & Guizani, M. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Networks, 111*, 102324.

Chen, J., Sun, J., & Wang, G. (2022). From unmanned system to autonomous intelligent systems. *Engineering, 12*, 16-19.

Coluccia, A., Parisi, G., & Fascista, A. (2020). Detection and classification of multirotor drones in radar sensor networks: A review. *Sensors, 20*(15), 4172.

Dudczyk, J., Czyba, R., & Skrzypczyk, K. (2022). Multi-sensory data fusion in terms of UAV detection in 3D space. *Sensors, 22*(12), 4323.

Kapustina, L., Izakova, N., Makovkina, E., & Khmel. (2021). The global drone market: Main development trends. *SHS Web of Conferences, 129*, 11004.

Kasapoğlu, C., & Kırdemir, B. (2022). *Rising drone power: Turkey on the eve of its military breakthrough*. Centre for Economics and Foreign Policy Studies.

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors, 20*(12), 3537.

Martins, B. O., Michel, A. H., & Silkoset, A. (2020). *Countering the drone threat*. Peace Research Institute.

Masyhar, A., & Emovwodo, S. O. (2023). Techno-prevention in counterterrorism: Between countering crime and human rights protection. *Journal of Human Rights, Culture and Legal System, 3*(3), 625-655.

Mukhammadsidiqov, M., & Turaev, A. (2020). Influence of US neoconservatism on formation of national security paradigm. *The Light of Islam*, (3), 7-14.

Popescu, L. R. (2021). The threat that is represented by the unauthorized flight of the RPAS and the anti-drone systems. *International Conference Knowledge-Based Organization, 27*(3), 77-82.

Quamar, M. M., Al-Ramadan, B., Khan, K., & Shafiulla. (2023). Advancements and applications of drone-integrated geographic information system technology—A review. *Remote Sensing, 15*(20), 5039.

Satria, I., & Efendi, S. (2021). Implementation of presidential power based on the 1945 State Constitution of the Republic of Indonesia. *Pranata Hukum, 16*(1), 45-59.

Singh, S., & Saini, B. S. (2021). Autonomous cars: Recent developments, challenges, and possible solutions. *Materials Science and Engineering, 1*(1).

Siswoputro, S., Suseto, B., Widjayanto, J., & Prakoso, L. Y. (2024). Fortification of civil-military cooperation through utilization of geospatial intelligence concepts in dealing with armed criminal groups in Papua. *Jurnal Pertahanan, 10*(1), 54-76.

Supriyadi, A. A., Yusdian, M. F., Putra, A. B., Anandari, A. A., Debiyanti, Bakasa, L. O., . . . Haryanto, A. (2023). Concept design of military and civilian interoperability based on sensing technology to support defense systems in the Malacca Strait region. *Remote Sensing Applications: Society and Environment, 32*(3), 101034.

Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things, 11*, 100218.