International Journal Administration, Business & Organization

Vol. 5 (No.2), 2024: 27-46 | E-ISSN 2721-5652

Available at https://ijabo.a3i.or.id/index.php/ijabo

The Impact of Intelligence Gathering, Risk Analysis, and Scenario Planning on Defense Policy Formulation

Aris Sarjito

Faculty of Defense Management,
Republic of Indonesia Defense University,
Jakarta, Indonesia
E-mail: arissarjito@gmail.com

ABSTRACT

In the evolving landscape of global security, the integration of intelligence gathering, risk analysis, and scenario planning is paramount for effective defense policy formulation. This study aims to underscore the critical role of these elements in contemporary defense strategies. Employing qualitative research methods, particularly secondary data analysis, this research investigates the transformative impact of artificial intelligence (AI) and machine learning (ML) on threat assessments, the benefits and challenges of big data analytics in risk analysis, and the value of interdisciplinary perspectives in scenario planning. The findings reveal that AI and ML significantly enhance the accuracy and reliability of threat assessments by enabling real-time data processing and predictive analytics. However, challenges such as data privacy and algorithmic biases persist. Big data analytics offers substantial benefits in identifying and mitigating emerging threats but requires robust data management frameworks to address issues of data quality and integration. Additionally, scenario planning is highlighted as a strategic tool that enhances defense strategies by anticipating various future scenarios and enabling proactive measures. Furthermore, the integration of interdisciplinary perspectives in scenario planning fosters more robust and adaptable defense policies, ensuring a comprehensive approach to security challenges. In conclusion, the integration of advanced technologies and interdisciplinary methods in intelligence gathering, risk analysis, and scenario planning is crucial for developing resilient and adaptive defense policies.

Keywords: Artificial Intelligence, Defense Policy Formulation, Intelligence Gathering, Risk Analysis, Scenario Planning

Received: 28 June, 2024
Accepted: 13 July, 2024
Available online: 26 August, 2024

DOI: 10.61242/ijabo.24.396

JEL Classifications: H56, D74, C63, O32, M15

INTRODUCTION

In the contemporary geopolitical landscape, defense policy formulation is a complex and dynamic process that necessitates the integration of intelligence gathering, risk analysis, and scenario planning. These components are crucial for developing robust defense strategies that can effectively address emerging threats and uncertainties. This research explores the current state of the art in these areas, highlighting recent advancements and their implications for defense policy.

Advancements in technology, particularly artificial intelligence (AI) and machine learning (ML), have significantly enhanced intelligence capabilities for better threat anticipation. AI and ML revolutionize data processing and analysis, enabling more accurate and timely threat assessments by analyzing vast amounts of data to identify patterns and anomalies (Johnson, 2019). AI's predictive analytics allow for accurate forecasting of security threats by processing historical data to detect trends not immediately apparent to human analysts, thereby enabling policymakers to anticipate and mitigate threats before they materialize (Sayler, 2020). Machine learning, a subset of AI, enhances this process by continuously learning from new data and adapting its models to improve accuracy. ML algorithms analyze social media feeds, news reports, and other sources to detect emerging threats in real-time, enhancing the responsiveness and effectiveness of intelligence operations (Plastiras et al., 2018). These technologies also facilitate the integration of disparate data sources, providing a comprehensive understanding of the threat landscape essential for informed and strategic defense policy decisions (Maddireddy & Maddireddy, 2020).

Intelligence gathering is the cornerstone of defense policy formulation, providing the necessary information to understand and anticipate potential threats. Modern advancements in technology have significantly enhanced intelligence capabilities. For instance, the use of artificial intelligence (AI) and machine learning (ML) algorithms has revolutionized the processing and analysis of vast amounts of data. AI-driven systems can identify patterns and anomalies in data that may indicate security threats, allowing for more proactive measures (Hoadley & Lucas, 2018).

Additionally, the integration of cyber intelligence has become increasingly important (Masruroh et al., 2024; Yuniawan, 2020). Cyber intelligence involves monitoring and analyzing digital communications to detect cyber threats and espionage activities. The growing reliance on digital infrastructure for both civilian and military operations make cyber intelligence a critical component of national security (Clarke & Knake, 2020). Risk analysis involves assessing the likelihood and potential impact of various threats. This process is essential for prioritizing resources and developing strategies to mitigate risks. Recent advancements in risk analysis methodologies have improved the accuracy and reliability of threat assessments (Syamfithriani et al., 2021; Katuk et al., 2022; Yusuf et al., 2024).

Quantitative risk analysis models, such as Bayesian networks, are now being used to predict the probability of different threat scenarios. These models incorporate a wide range of variables, including historical data, current intelligence, and expert judgments, to provide a comprehensive assessment of risks (Riley & Venables, 2020; Darmawan et al., 2021). Moreover, the use of big data analytics has enhanced the ability to identify and assess emerging threats. By analyzing large datasets from diverse sources, defense agencies can gain insights into potential risks that may not be immediately apparent. This approach allows for a more nuanced understanding of the threat landscape and supports more informed decision-making (Jain et al., 2021; Yusuf et al., 2021). Recent innovations in scenario planning have focused on the incorporation of advanced simulation techniques. These techniques use sophisticated models to simulate the outcomes of

 DOI: https://doi.org/10.61242/ijabo.24.396

different scenarios, allowing policymakers to test the effectiveness of various strategies in a virtual environment (Baiocchi et al., 2018; Akhmaddhian, 2020; Budiman & Akhamddhian, 2023). This approach provides a more dynamic and interactive means of exploring potential futures and their implications for defense policy.

Additionally, scenario planning has increasingly incorporated a broader range of perspectives, including those from non-military sectors. By considering economic, political, and social factors, scenario planning can provide a more holistic view of potential threats and their impacts (Nurhandika & Manalu, 2023; Rachmawati et al., 2018). This interdisciplinary approach ensures that defense policies are not only robust but also adaptable to a wide array of challenges (Webster et al., 1989; Budiman et al., 2024). The integration of intelligence gathering, risk analysis, and scenario planning has significant implications for defense policy formulation. By leveraging advanced technologies and methodologies, defense agencies can develop more informed and effective strategies. These tools enable a proactive approach to security, allowing for the anticipation and mitigation of threats before they materialize.

Furthermore, the ability to conduct comprehensive and accurate threat assessments supports more efficient allocation of resources. By prioritizing the most significant risks, defense agencies can ensure that their efforts are focused on the areas of greatest need (Akhmaddhian et al., 2021). This approach not only enhances security but also maximizes the return on investment for defense spending (Flynn, 2004; Budiman et al., 2022). Incorporating perspectives from non-military sectors into scenario planning is essential for developing robust and adaptable defense policies. This approach ensures strategies consider various potential threats and opportunities. Insights from economics, technology, health, and environmental science help policymakers understand the complex factors influencing national security. Economic trends affect resource availability and stability, while technological advancements and cybersecurity threats require tech expertise (Singh et al., 2022; Toops et al., 2021; Wibowo & Rahmantya, 2023). Health experts highlight pandemics' impact on military readiness, and environmental scientists address climate-related security issues (Braun III & Allen, 2014; Moudy et al., 2014). Interdisciplinary planning promotes innovative problem-solving by combining diverse expertise, leading to more effective strategies (Yang et al., 2014; Manalu & Adzimatinur, 2024). Addressing challenges in data integration and expert coordination is crucial for ensuring strategies are realistic and actionable, ultimately enhancing defense policies' robustness (Kröger & Schäfer, 2016).

Intelligence gathering, risk analysis, and scenario planning are critical to defense policy formulation. Intelligence gathering provides foundational data to understand and anticipate threats. Recent technological advancements, like artificial intelligence (AI) and machine learning (ML), have notably bolstered intelligence capabilities. AI-driven systems efficiently process vast data volumes, pinpointing patterns and anomalies indicative of security threats (Hoadley & Lucas, 2018). Additionally, cyber intelligence, essential for monitoring digital communications to detect cyber threats and espionage, has grown in significance with increased reliance on digital infrastructure (Clarke & Knake, 2020). Risk analysis assesses threat likelihood and impact to prioritize resources and formulate mitigation strategies (Wiharno et al., 2021; Manalu et al., 2023). Recent advances, like Bayesian networks, enhance accuracy by integrating historical data, current intel, and expert insights (Riley & Venables, 2020). Big data analytics further enhances threat identification and assessment through comprehensive dataset analysis (Jain et al., 2021).

Scenario planning is a strategic tool used to envision and prepare for possible future events. It involves developing a range of plausible scenarios based on current trends and

 DOI: https://doi.org/10.61242/ijabo.24.396

potential disruptors. Recent innovations in scenario planning have focused on the incorporation of advanced simulation techniques, which use sophisticated models to simulate the outcomes of different scenarios, allowing policymakers to test the effectiveness of various strategies in a virtual environment (Baiocchi et al., 2018). Moreover, scenario planning has increasingly incorporated a broader range of perspectives, including those from non-military sectors, ensuring that defense policies are robust and adaptable to a wide array of challenges (Webster et al., 1989).

In today's digital age, cyber intelligence plays a critical role in national security by monitoring and analyzing digital communications to detect cyber threats and espionage activities, essential for effective defense policy formulation. It involves collecting and interpreting data from various digital sources like email traffic, social media, and network activity to identify hacking, phishing, and data breaches swiftly (Kasowaki & Alp, 2024). Real-time insights provided by AI and machine learning tools enable rapid detection of patterns and anomalies that signal potential cyber espionage or attacks, supporting preemptive defense measures (Labu & Ahammed, 2024). This capability enhances strategic decision-making by offering a comprehensive understanding of the threat landscape, enabling the development of robust cybersecurity policies to bolster digital infrastructure resilience (Brown et al., 2015). Integrating cyber intelligence into defense policy also improves risk analysis and scenario planning, helping policymakers mitigate risks and coordinate responses effectively (Marotta & McShane, 2018).

Conceptual Issues and Research Gaps

Understanding the interplay between intelligence gathering, risk analysis, and scenario planning is essential for effective defense policy formulation. Intelligence serves as the foundation for assessing risks and developing scenarios; deficiencies in intelligence can undermine these processes, while robust risk analysis and scenario planning identify gaps in intelligence, guiding further data collection efforts. However, significant research gaps remain, such as the impact of AI and ML integration on intelligence quality and subsequent risk and scenario analysis, requiring resolution of ethical and operational concerns (Hoadley & Lucas, 2018). Additionally, advanced simulation techniques in scenario planning show promise but require more empirical validation for practical application in defense policy formulation (Baiocchi et al., 2018). The literature underscores the need for comprehensive studies on interdisciplinary scenario planning and further research on big data analytics in risk analysis, particularly addressing challenges like data quality, privacy, and security (Jain et al., 2021).

Statement of the Problem

In an era of rapid technological advancement and evolving geopolitical threats, formulating effective defense policies has become increasingly complex. Integrating intelligence gathering, risk analysis, and scenario planning is crucial for developing robust defense strategies to tackle dynamic challenges. However, gaps persist in understanding how these components interact and contribute to overall policy effectiveness. Specifically, the roles of advanced technologies like artificial intelligence (AI) and big data analytics in intelligence gathering and risk analysis, along with the integration of interdisciplinary perspectives in scenario planning, are areas requiring further exploration. Closing these gaps is vital for enhancing defense agencies' strategic capabilities and safeguarding national security in today's rapidly changing landscape.

 DOI: https://doi.org/10.61242/ijabo.24.396

Research Objectives

This study aims to analyze the role of artificial intelligence and machine learning in enhancing intelligence gathering for defense policy formulation, evaluate the effectiveness of big data analytics in risk analysis for identifying and mitigating emerging threats, and examine the integration of interdisciplinary perspectives in scenario planning and its impact on the robustness of defense policies.

Research Questions

1. How does the application of artificial intelligence and machine learning in intelligence gathering impact the accuracy and reliability of threat assessments for defense policy formulation? This research question explores how AI and ML technologies enhance intelligence gathering by processing vast data volumes, identifying patterns, anomalies, and improving threat assessment accuracy. Understanding these impacts enables policymakers to effectively utilize AI and ML for informed, proactive defense strategies (Hoadley & Lucas, 2018).

2. What are the benefits and challenges of using big data analytics in risk analysis for defense policy formulation, particularly in identifying and mitigating emerging threats? This question explores how big data analytics enhances risk analysis by analyzing large, diverse datasets to uncover emerging threats and improve risk mitigation strategies. It also examines critical challenges such as data quality, privacy, and security, which are crucial for ensuring the reliability and effectiveness of big data analytics in defense contexts (Jain et al., 2021).

3. How does the integration of interdisciplinary perspectives in scenario planning enhance the robustness and adaptability of defense policies? This research question investigates integrating economic, political, and social factors into scenario planning to enhance understanding of potential threats and their impacts on defense policies. By examining the benefits and challenges of this interdisciplinary approach, the research aims to show how it can improve the robustness and adaptability of defense policies, addressing diverse challenges effectively (Webster et al., 1989).

LITERATURE REVIEW

The application of artificial intelligence (AI) and machine learning (ML) in intelligence gathering leverages the Data-Information-Knowledge-Wisdom (DIKW) hierarchy. This framework illustrates how raw data is processed into actionable wisdom through successive stages of transformation. AI and ML technologies enhance this process by efficiently analyzing vast datasets, using algorithms to detect patterns and anomalies that improve the accuracy of threat assessments (Russell & Norvig, 2016). By automating data analysis, these technologies mitigate human error and bias, thereby enhancing the reliability of intelligence. Signal Detection Theory further explains how AI and ML distinguish relevant signals from noise in data, improving the identification of potential threats (Wickens et al., 2004).

The benefits and challenges of using big data analytics in risk analysis for defense policy can be understood through the Technology Acceptance Model (TAM), emphasizing the importance of perceived usefulness and ease of use in technology adoption (Davis, 1989). Big data analytics enhances defense policy by integrating diverse data sources to identify emerging threats and improve situational awareness, supporting

 DOI: https://doi.org/10.61242/ijabo.24.396

proactive risk mitigation strategies. However, challenges outlined by the Theory of Constraints (TOC), such as data quality, privacy, and security concerns, must be addressed to fully realize the technology's potential (Goldratt, 1990). Big data analytics in risk analysis provides real-time insights, enhances decision-making accuracy through advanced algorithms, and supports continuous surveillance to respond swiftly to threats (El Khatib et al., 2023; More et al., 2017). Yet, challenges include ensuring data accuracy across sources, navigating algorithm complexity, addressing privacy and security issues, managing financial investments, and overcoming resistance to change (Bates et al., 2014; Becker et al., 2015; Djouzi & Beghdad-Bey, 2019; Gahi et al., 2016; Verma et al., 2018; Wiharno et al., 2021).

The integration of interdisciplinary perspectives in scenario planning, analyzed through Systems Theory, enhances defense strategies by integrating insights from fields like economics, politics, and social sciences. This approach considers how these factors interconnect and influence defense policies, improving the ability to anticipate and address complex security challenges dynamically (Gheorghe et al., 2017). Systems Theory offers a framework to optimize defense strategies by examining systemic behaviors and feedback loops across various domains (Derbyshire, 2019). By incorporating economic, political, and social dimensions into scenario planning, defense policymakers can develop resilient strategies that account for diverse contingencies and align with broader national objectives (Balarezo & Nielsen, 2017).

RESEARCH METHOD

Qualitative research methods provide a thorough approach to studying intricate topics such as the influence of intelligence gathering, risk analysis, and scenario planning on defense policy formulation. Qualitative research focuses on understanding human experiences and behaviors through detailed data analysis (Creswell & Creswell, 2017; Chaniago et al., 2023). Utilizing secondary data in qualitative research involves examining existing datasets originally collected for other purposes, offering valuable insights into the research topic. This study examines the application of qualitative research methods using secondary data to explore these specific areas.

The methods section details a qualitative research design based on Creswell & Creswell (2017) and recent literature. Research Design: The study utilizes a qualitative approach with secondary data to examine how intelligence gathering, risk analysis, and scenario planning influence defense policy formulation, leveraging its flexibility to explore complex interactions (Creswell & Creswell, 2017). Data Collection: Secondary sources include government reports, defense white papers, academic literature, media, and expert opinions, accessed through public databases and governmental websites to provide historical and contemporary insights (Johnston, 2014). Data Analysis: The study employs content analysis for systematic coding (Krippendorff, 2018), thematic analysis to identify recurring themes (Braun & Clarke, 2021), and narrative analysis to reveal underlying narratives and accounts (Riessman, 2008).

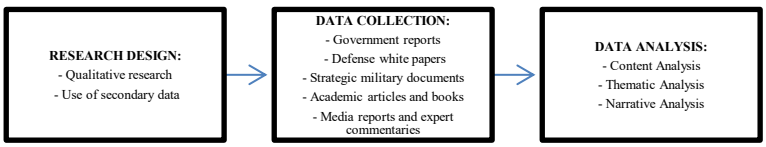

Figure 1. Methods
Source: Creswell & Creswell, 2017

 DOI: https://doi.org/10.61242/ijabo.24.396

Addressing Research Questions

Using Creswell's qualitative research framework, this study employs secondary data analysis to investigate key research questions. For instance, researchers explore the impact of artificial intelligence and machine learning on threat assessments by analyzing existing reports and studies (Hoadley & Lucas, 2018), providing insights into their effectiveness and challenges in defense contexts. Examining government publications and academic research on big data analytics in defense assesses its benefits and challenges in mitigating emerging threats (Jain et al., 2021). Additionally, analyzing policy documents and interdisciplinary studies illuminates how integrating diverse perspectives in scenario planning enhances defense policies' robustness and adaptability (Webster et al., 1989), highlighting the practical implications of interdisciplinary collaboration in shaping effective defense strategies.

RESEARCH RESULTS

1. Impact of Artificial Intelligence and Machine Learning on Threat Assessments for Defense Policy Formulation

AI and ML have significantly enhanced intelligence gathering and threat assessment in defense policy formulation by efficiently processing vast amounts of data using the DIKW hierarchy. They improve the identification of threats by distinguishing relevant signals from background noise across diverse sources like social media and satellite imagery. These technologies automate data processing tasks, reducing human error and bias while identifying correlations and trends that enhance analytical capabilities. However, challenges such as data privacy, algorithmic bias, and the interpretability of AI-driven decisions remain significant, necessitating collaboration among government agencies, industry partners, and academia to develop ethical frameworks for responsible AI use in defense intelligence.

2. Benefits and Challenges of Using Big Data Analytics in Risk Analysis for Defense Policy Formulation

Big data analytics (BDA) plays a crucial role in defense policy formulation by integrating diverse data sources to provide real-time insights into emerging threats, enhancing decision-making, and enabling proactive risk mitigation (TAM). BDA's advanced analytics algorithms improve the accuracy of risk assessments and support predictive modeling for preemptive risk management (TOC). However, challenges such as ensuring data privacy and addressing algorithmic bias must be addressed to fully exploit its potential. Despite these challenges, BDA aids in resource allocation and strategy prioritization based on anticipated risks, contributing to enhancing strategic decision-making and safeguarding national security interests responsibly.

3. Integration of Interdisciplinary Perspectives in Scenario Planning for Defense Policies

Interdisciplinary perspectives in scenario planning enhance defense policies by integrating economic, political, and social factors to create more adaptive strategies for complex threats (Wachjuni et al., 2024; Nirmala et al., 2021; Djuniardi et al., 2022). Economic insights provide critical understanding of resource availability and geopolitical stability, preparing defense agencies for potential disruptions (Alizadeh et al., 2016). Political analyses illuminate international relations dynamics, guiding strategic alignment amidst evolving policies (Passeri & Marston, 2022), while social factors like

 DOI: https://doi.org/10.61242/ijabo.24.396

demographics and public sentiment influence defense initiatives and societal stability (Glenn et al., 2014). This holistic approach fosters innovative problem-solving and ensures policies are robust and responsive (Polk, 2014; Rijal et al., 2023), though effective data integration and expert coordination are essential to maximize these benefits and strengthen policy adaptability (Djalante et al., 2013; Djuniardi, et al., 2022).

DISCUSSION

1. Impact of Artificial Intelligence and Machine Learning on Threat Assessments for Defense Policy Formulation

The application of artificial intelligence (AI) and machine learning (ML) in intelligence gathering significantly impacts the accuracy and reliability of threat assessments for defense policy formulation. Utilizing the Data-Information-Knowledge-Wisdom (DIKW) hierarchy, AI and ML enhance the transformation of raw data into actionable wisdom by efficiently processing vast amounts of data. These technologies employ sophisticated algorithms to identify patterns and anomalies in large datasets, automating the data analysis process, reducing human error and bias, and leading to more precise intelligence outputs (Russell & Norvig, 2016).

Artificial intelligence (AI) and machine learning (ML) play a pivotal role in enhancing intelligence gathering and actionable insights through the Data-Information-Knowledge-Wisdom (DIKW) hierarchy, particularly in threat assessments for defense policy formulation. AI and ML algorithms excel at processing vast amounts of data (data) collected from diverse sources such as surveillance systems, social media, and satellite imagery, transforming this raw data into structured and meaningful information (information). This process involves pattern recognition and anomaly detection, allowing for the identification of potential threats and trends that may not be immediately apparent to human analysts (knowledge) (Sayler, 2020). By continuously learning from new data inputs, ML algorithms refine their models over time, enhancing the accuracy and reliability of threat assessments (wisdom) (Plastiras et al., 2018). This hierarchical approach enables defense policymakers to make informed decisions and formulate proactive strategies based on comprehensive and nuanced insights derived from AI and ML technologies.

Additionally, AI and ML enhance threat detection by efficiently distinguishing relevant signals from background noise, as explained by Signal Detection Theory. These technologies excel at analyzing diverse data sources like social media and satellite imagery, continually improving their ability to detect patterns and anomalies indicative of threats (Wickens et al., 2004). Integrating AI and ML in intelligence gathering significantly enhances its efficiency and effectiveness, forming a solid basis for defense policy formulation.

Cyber intelligence is crucial for defense policy formulation as it enhances the ability to monitor, analyze, and respond to cyber threats and espionage activities, which is essential for national security given the increasing reliance on digital infrastructure (Borum et al., 2015). AI and ML technologies process vast amounts of data from network traffic, social media, and communication channels to detect malicious activities in real-time, enabling quicker and more accurate threat detection and response (Herring & Willett, 2014; Labu & Ahammed, 2024). These technologies also provide insights into adversaries' tactics, aiding the development of robust cybersecurity policies and proactive measures to safeguard critical infrastructure (Sabillon et al., 2017). Integrating cyber intelligence into defense policy formulation ensures a holistic approach to addressing the complex and evolving landscape of cyber threats.

 DOI: https://doi.org/10.61242/ijabo.24.396

Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized intelligence gathering and threat assessment in defense policy formulation. These technologies enable defense agencies to process and analyze vast amounts of data rapidly and accurately, enhancing real-time threat detection and assessment (Maddireddy & Maddireddy, 2020). This discussion explores their profound impact on improving the accuracy and reliability of threat assessments, thereby shaping defense strategies globally.

AI and ML significantly enhance defense policy by improving threat assessments through advanced data analysis and predictive capabilities. These technologies allow defense agencies to rapidly process vast data from sources like satellite imagery and social media, identifying patterns and anomalies that enhance the accuracy and timeliness of threat assessments (De Spiegeleire et al., 2017). Predictive analytics enable AI and ML models to forecast threats based on historical data, supporting proactive risk mitigation strategies (Roff, 2020). This approach boosts national security preparedness and response capabilities. Additionally, AI and ML facilitate real-time monitoring, providing defense policymakers with current situational awareness for informed decision-making (Dalkıran et al., 2021). Integrating these technologies into defense policy ensures a comprehensive strategy to address evolving security challenges effectively.

Enhancing Data Processing and Analysis

AI and ML technologies are adept at processing large datasets and uncovering meaningful insights that human analysts might miss (Ghavami, 2020). These technologies can analyze diverse data sources, such as satellite imagery and intercepted communications, to detect patterns indicative of potential threats (Hao, 2020). By automating data processing tasks, AI reduces the workload on human analysts and speeds up the generation of actionable intelligence. Moreover, AI and ML enhance data analysis by identifying hidden correlations and trends, leading to more accurate threat assessments and a deeper understanding of risks (Kaloudi & Li, 2020). Continuously learning from new data, AI algorithms improve intelligence gathering efficiency over time, enabling defense policymakers to make informed decisions and allocate resources effectively to counter emerging threats (Jensen et al., 2020).

Improving Accuracy in Threat Detection

AI and ML improve threat assessments by adapting algorithms with new data, minimizing errors, and enhancing reliability for defense policy (Hao, 2020). They analyze vast datasets swiftly, identifying subtle patterns and threats, aiding proactive defense strategies (Nassar & Kamal, 2021). Automated threat detection frees analysts to focus on strategic responses, enhancing national security and safeguarding critical infrastructure (Adewusi et al., 2024; Sayler, 2020).

Identifying Patterns and Anomalies

AI and ML excel at detecting subtle patterns and anomalies in datasets, such as flagging unusual activities that may indicate emerging threats or changes in adversary tactics (Khan et al., 2021). This proactive capability enables defense agencies to anticipate threats, enhancing preparedness and response. Leveraging AI and ML, defense agencies analyze vast data volumes in real-time to swiftly identify risks and vulnerabilities, continually improving their adaptive threat detection abilities (Maddireddy & Maddireddy, 2020). This dynamic approach is essential in today's security landscape, complementing traditional methods and automating routine tasks to focus human analysts on strategic challenges (Sarker, 2024).

Challenges and Considerations Sarker

 DOI: https://doi.org/10.61242/ijabo.24.396

Despite their transformative potential, AI and ML technologies in defense intelligence face significant challenges, including data privacy, algorithmic bias, and the interpretability of AI-driven decisions (T. M. Chen & Jøsang, 2020). Concerns also arise around the ethical and legal implications of relying on AI for critical decision-making in defense policy formulation. Organizations must implement robust safeguards to mitigate these risks and ensure accountability and transparency. Additionally, the integration of AI and ML technologies requires careful consideration to prevent unintended consequences or misuse. Collaboration among stakeholders—government agencies, industry partners, and academia—is crucial to developing ethical frameworks that guide the responsible use of AI in defense intelligence (Board, 2019). Addressing these challenges effectively will enable organizations to leverage AI and ML technologies fully, enhancing national security and strategic decision-making capabilities.

AI enhances threat assessments in defense policy by improving data processing, predictive analytics, and decision-making accuracy. AI algorithms analyze vast amounts of data from sources like social media and satellite imagery at unprecedented speeds, transforming raw data into actionable intelligence (De Spiegeleire et al., 2017). This enables the identification of subtle patterns and anomalies, leading to more accurate threat detection (Rashid et al., 2023). AI-powered predictive analytics forecast potential threats by identifying emerging risks, allowing proactive measures (Bouchama & Kamal, 2021). AI also supports real-time monitoring, providing up-to-the-minute threat assessments and alerts for swift decision-making (Dalkıran et al., 2021). Additionally, AI integrates diverse data sources for a comprehensive view of the threat landscape, crucial for effective defense policies (Koch, 2021).

The diagram below illustrates how Artificial Intelligence (AI) and Machine Learning (ML) enhance threat assessments and inform defense policy (Freeman, 2020). AI and ML algorithms enable defense agencies to analyze extensive data to identify threats and predict risks more accurately. These technologies automate tasks, improve response times, and enhance national security measures. As AI and ML progress, they will increasingly shape defense strategies, safeguarding nations in a complex security landscape.

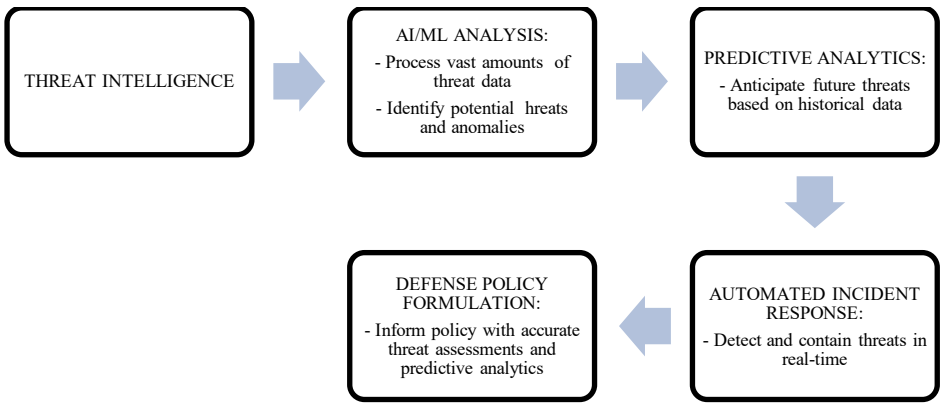

Figure 2: The Impact of Artificial Intelligence and Machine Learning on Threat Assessments for Defense Policy Formulation
Source: *researcher, 2024*

By integrating AI and ML into threat assessments, defense policies can be more effective in addressing emerging cyber threats, thereby strengthening national security (Shah, 2021). These technologies analyze vast amounts of data in real-time, identifying patterns and anomalies indicative of potential cyber-attacks. Automating threat detection

 DOI: https://doi.org/10.61242/ijabo.24.396

processes allows defense agencies to preemptively thwart breaches and stay ahead of cybercriminals. Furthermore, AI improves incident response times by offering actionable insights and recommendations to security teams, enabling a proactive and targeted approach to cybersecurity.

2. Benefits and Challenges of Using Big Data Analytics in Risk Analysis for Defense Policy Formulation

The benefits and challenges of using big data analytics in defense policy formulation can be understood through the Technology Acceptance Model (TAM), which emphasizes perceived usefulness and ease of use as critical adoption factors (Davis, 1989). In defense contexts, big data analytics integrates and analyzes diverse data sources to identify emerging threats, enhancing situational awareness and enabling proactive risk mitigation strategies. This capability improves decision-making processes and facilitates the formulation of more effective and timely defense policies by providing comprehensive, real-time insights into potential threats (H. Chen et al., 2020).

The Theory of Constraints (TOC) identifies key challenges in implementing big data analytics in defense contexts. These include ensuring data quality—accuracy, completeness, and relevance are crucial for reliable outcomes. Privacy concerns are significant, requiring careful management of sensitive information to protect individual rights and comply with legal regulations. Security issues are paramount to safeguarding the integrity of big data systems against cyber threats and unauthorized access. Addressing these constraints is essential to fully harness the potential of big data analytics in defense policy formulation, as any lapses in these areas can undermine its effectiveness and reliability (Goldratt, 1990; Rehman et al., 2022).

Big Data Analytics (BDA) plays a pivotal role in risk analysis for defense policy by providing deep insights into emerging threats and supporting proactive mitigation strategies. BDA enhances situational awareness by processing vast amounts of data from sources like social media, satellite imagery, and financial transactions, enabling swift detection and response to risks (Al-Zahrani & Al-Hebbi, 2022). Advanced analytics improve threat assessment accuracy by identifying subtle patterns, reducing uncertainty, and informing decision-making (Symon & Tarapore, 2015). BDA also supports predictive modeling to anticipate future threats and implement preemptive measures, optimizing resource allocation and enhancing national security (Berlin & Neskovic, 2018). However, challenges include ensuring data quality, infrastructure scalability, and addressing ethical issues like data privacy and algorithmic bias (Petrozzino, 2020).

Big data analytics enhances risk analysis for defense policy formulation by providing insights into emerging threats and supporting effective mitigation strategies. It allows defense agencies to utilize vast amounts of structured and unstructured data from diverse sources, facilitating deeper insights and informed decision-making processes (Akhgar et al., 2015).

Enhancing Insight through Data Integration

Big data analytics integrates data from diverse sources like sensor networks, social media feeds, satellite imagery, and financial transactions (M. Chen et al., 2014). This approach enables defense analysts to detect patterns and correlations that reveal potential threats early on. For instance, combining social media data with geospatial information can offer insights into civil unrest or geopolitical tensions, informing preemptive defense strategies. Additionally, data integration provides a comprehensive view of security challenges, connecting disparate pieces of information to uncover hidden insights (Unver, 2018). By

 DOI: https://doi.org/10.61242/ijabo.24.396

leveraging varied datasets, including open-source intelligence and historical data, analysts gain a nuanced understanding of evolving threats, enhancing situational awareness and supporting proactive risk mitigation efforts for national security.

Supporting Real-Time Decision Making

Big data analytics processes information swiftly, enabling defense agencies to respond rapidly to evolving threats. Real-time analytics platforms monitor data streams continuously, triggering alerts based on predefined thresholds or anomaly detection algorithms (M. Chen et al., 2014). This capability enhances situational awareness and facilitates proactive risk mitigation measures before security challenges escalate. Moreover, real-time decision-making allows agencies to adapt quickly to changing circumstances (Fraga-Lamas et al., 2016). By leveraging big data analytics, agencies can make informed decisions based on the latest information, crucial in navigating a dynamic threat landscape. Additionally, real-time analytics uncover hidden patterns and trends, aiding agencies in anticipating and preventing potential security breaches before they materialize (Rassam et al., 2017).

Improving Predictive Capabilities

Predictive analytics, a subset of big data analytics, uses historical data to forecast future trends and potential threats. Machine learning algorithms analyze historical conflict data, predicting the likelihood and severity of future conflicts in specific regions (Xu et al., 2020). This capability enables defense policymakers to allocate resources effectively and prioritize response strategies based on anticipated threats, enhancing overall security readiness and reducing the impact of security incidents. Continuous refinement of predictive capabilities strengthens defense mechanisms, enabling real-time monitoring and agile response to emerging threats (McCue, 2014; Sharma & Barua, 2023).

Challenges in Implementation

Implementing big data analytics in defense risk analysis presents significant challenges. Firstly, ensuring data quality and integrity is crucial to prevent erroneous conclusions and decisions (M. Chen et al., 2014). Secondly, managing the volume and velocity of data requires robust infrastructure and scalable analytics platforms capable of real-time processing. Thirdly, safeguarding data privacy and security is essential when integrating sensitive information from multiple sources. Additionally, the complexity of harmonizing and analyzing data from diverse sources and formats poses logistical hurdles (C. L. P. Chen & Zhang, 2014). Addressing these challenges demands specialized skills in data analytics and cybersecurity. Despite these complexities, the potential benefits of big data analytics in defense risk analysis justify the effort to enhance strategic decision-making capabilities (Eastman et al., 2015).

Ethical and Legal Considerations

The use of big data analytics raises ethical and legal concerns regarding privacy infringement, algorithmic bias, and decision-making accountability (T. M. Chen & Jøsang, 2020). Maintaining transparency and adhering to ethical guidelines in data collection, analysis, and use are essential to preserve public trust and protect civil liberties. Organizations must navigate these challenges carefully to ensure that their use of big data analytics is effective, ethical, and compliant with legal standards. Balancing the need for data-driven insights with privacy protection requires robust data governance

 DOI: https://doi.org/10.61242/ijabo.24.396

frameworks and compliance measures to prevent unauthorized access and misuse of sensitive information (Ghavami, 2020). Addressing concerns about algorithmic bias is also critical to ensure fair and unbiased decision-making outcomes. By actively managing these ethical and legal considerations, organizations can foster trust among stakeholders and demonstrate their commitment to responsible data practices.

3. Integration of Interdisciplinary Perspectives in Scenario Planning for Defense Policies

Integrating interdisciplinary perspectives in scenario planning enhances defense policies by using Systems Theory, which highlights the interconnectedness of system components (Bertalanffy, 1968). By incorporating economic, political, and social factors, scenario planning becomes more comprehensive and adaptable. This approach ensures that defense strategies consider potential threats from multiple angles, enabling more effective policy responses. For instance, analyzing how economic downturns or political instability affect security threats enhances the robustness of defense strategies.

Interdisciplinary scenario planning is crucial for defense policies as it integrates diverse perspectives from economics, politics, sociology, and technology to develop comprehensive and adaptive strategies (Gheorghe et al., 2017). This holistic approach ensures consideration of a wide range of variables and potential impacts that traditional single-discipline planning might miss (Abewardhana et al., 2020). By identifying interdependencies and cascading effects within the global security environment, incorporating various disciplines enhances the robustness of defense strategies (Fjäder, 2018). For instance, understanding the economic implications of political conflicts aids in formulating effective responses. Furthermore, interdisciplinary planning fosters innovative problem-solving by leveraging diverse expertise to generate novel strategies (Porkoláb & Zweibelson, 2018). Addressing challenges such as data integration, expertise coordination, and scenario validation is essential to maximize the effectiveness of interdisciplinary planning, ensuring that developed strategies are realistic and actionable for enhancing defense policies' adaptability (Kröger & Schäfer, 2016).

The Complex Adaptive Systems (CAS) Theory suggests that systems with diverse interacting agents can adapt to changing environments (Holland, 1992). Integrating interdisciplinary perspectives in scenario planning enhances this adaptability in defense policy formulation, crucial for addressing evolving threats. Insights from various disciplines make defense policies more flexible and responsive, improving strategies to mitigate risks and capitalize on opportunities in a dynamic global landscape (Page, 2008). For example, integrating environmental science enhances responses to climate-related security threats, while technological insights strengthen cyber defense measures.

The integration of diverse perspectives in scenario planning, guided by Complex Adaptive Systems (CAS) Theory, enhances defense strategies by addressing a broad spectrum of challenges. CAS Theory underscores the dynamic and interconnected nature of systems, where components continually adapt to environmental changes (Gheorghe et al., 2017). Incorporating interdisciplinary perspectives—spanning economics, politics, social sciences, and technology—enables scenario planning to account for the complex interdependencies within defense systems (Derbyshire, 2019). This holistic approach allows defense policymakers to develop robust strategies capable of responding to unforeseen events. For example, economic factors influence resource allocation, political dynamics shape threat perceptions, and social factors impact military readiness and public support (Balarezo & Nielsen, 2017). By integrating these elements, scenario planning ensures that defense strategies are comprehensive and adaptable to a wide range of potential challenges.

 DOI: https://doi.org/10.61242/ijabo.24.396

Moreover, CAS Theory advocates for resilient defense systems capable of self-organization to confront complex threats effectively (Dobson et al., 2019). Collaborating across disciplines fosters innovation and facilitates the development of nuanced defense strategies that can withstand the uncertainties of the modern security landscape.

Scenario planning is a strategic tool used in defense policy formulation to anticipate and prepare for future uncertainties. This discussion explores how the integration of interdisciplinary perspectives—from economic, political, and social domains—enhances the robustness and adaptability of defense policies. By incorporating diverse viewpoints, scenario planning can provide a more comprehensive assessment of potential threats and their impacts on national security.

Defense policies must navigate complex and evolving geopolitical landscapes, where traditional military perspectives alone may not suffice in anticipating all potential threats. Interdisciplinary scenario planning integrates insights from various fields, offering a holistic approach to understanding and preparing for diverse security challenges (Sarjito, 2023). This discussion critically examines the benefits of incorporating economic, political, and social perspectives into scenario planning for defense policy formulation.

Comprehensive Understanding of Threats

Integrating economic perspectives into scenario planning allows defense policymakers to evaluate how economic factors such as trade dynamics, resource scarcity, and economic stability affect national security (Cetorelli, 2017). Economic downturns or disruptions in global supply chains can significantly impact defense capabilities and strategic priorities. By incorporating economic scenarios, defense planners can anticipate vulnerabilities and develop resilient strategies to mitigate risks. This holistic approach provides a comprehensive understanding of threats beyond traditional military considerations, highlighting the interconnectedness of security and economic issues (Otaiku, 2018). By integrating economic perspectives into scenario planning, defense policymakers can better prepare for diverse threats and uncertainties, enhancing strategic decision-making effectiveness.

Political Dynamics and Strategic Interactions

Political factors such as international alliances, diplomatic tensions, and governance structures play a pivotal role in shaping defense policies and strategic decision-making. Scenario planning that integrates political perspectives enables policymakers to simulate geopolitical scenarios and assess their impact on national defense (Frieden et al., 2019). Understanding political dynamics aids in identifying allies, adversaries, and diplomatic leverage points, enhancing preparedness and response capabilities. Additionally, political factors influence defense budgets and resource allocation, necessitating careful navigation of competing funding demands across sectors (Steinbock, 2014). By monitoring political developments closely and engaging in strategic diplomacy, policymakers can effectively address security threats and foster stability amid global uncertainties.

Social and Technological Trends

Social factors like demographic shifts, public opinion changes, and advancements in technology significantly influence defense policies. Integrating social perspectives into scenario planning helps defense agencies anticipate how these trends such as public attitudes towards defense spending or developments in cyber capabilities affect national

 DOI: https://doi.org/10.61242/ijabo.24.396

security (Bracken, 2012). By proactively adapting to societal and technological changes, defense agencies can enhance their ability to address emerging threats effectively. For instance, increasing public awareness of cyber threats prompts agencies to bolster cyber defenses (Choucri et al., 2014). Demographic changes, like aging populations or immigration patterns, may also necessitate adjustments in defense strategies to address new security concerns. By staying abreast of these dynamics, defense planners can better anticipate and respond to evolving threats in today's global landscape.

Challenges and Considerations

Interdisciplinary scenario planning in defense policy formulation offers significant benefits but also presents challenges in data integration, expertise coordination, and scenario validation (Schoemaker, 1993). Integrating diverse data sources and coordinating experts from various disciplines require effective communication and collaboration (Sutrisno, 2023). Ensuring scenarios align with real-world developments and assessing the feasibility of proposed strategies are critical to enhancing the credibility and utility of scenario planning. Coordinating experts from different fields can be complex due to varied methodologies and priorities, necessitating careful management of communication and collaboration efforts (Michael et al., 2013).

The diagram below illustrates the integration of interdisciplinary perspectives in scenario planning for defense policies, highlighting the importance of considering various viewpoints and methods to inform strategic decision-making.

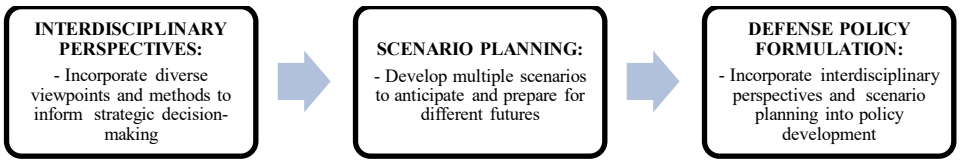

Figure 3: Integration of Interdisciplinary Perspectives in Scenario Planning for Defense Policies
Source: *researcher, 2024*

Integrating interdisciplinary perspectives into scenario planning enhances defense policies' effectiveness in addressing complex strategic challenges, ultimately bolstering national security (Weigand et al., 2014). By exploring diverse scenarios and collaborating with experts across various fields, defense policies become more adaptable to dynamic environments and emerging threats. This proactive approach improves strategic decision-making and promotes innovation within the defense sector, ensuring national security and resilience in an uncertain world.

CONCLUSIONS

The integration of AI and ML technologies has revolutionized intelligence gathering and threat assessment in defense policy formulation, enhancing accuracy and reliability through advanced data processing and predictive analytics. Ongoing research is crucial to address data privacy, bias mitigation, and ethical challenges. By fully harnessing AI and ML while tackling these issues, defense agencies can better safeguard national security and adapt to evolving geopolitical threats.

Big data analytics enhances defense policy risk analysis by providing deep insights into emerging threats and supporting proactive mitigation strategies. Advanced analytics improve situational awareness, predictive capabilities, and resource allocation. However, challenges related to data quality, infrastructure scalability, and ethical considerations must be addressed to maximize benefits and mitigate risks. Continued research and

 DOI: https://doi.org/10.61242/ijabo.24.396

innovation will strengthen defense risk analysis, emphasizing the importance of data integration, expertise coordination, and scenario validation for comprehensive and actionable intelligence.

Integrating interdisciplinary perspectives in scenario planning enriches defense policy by providing a comprehensive understanding of potential threats and opportunities. By incorporating economic, political, and social insights, defense agencies can develop more adaptive and resilient strategies. Addressing data integration, expertise coordination, and scenario validation is crucial for effectiveness. Effective data integration ensures all relevant information is considered, coordinated expertise synthesizes diverse insights, and scenario validation ensures strategies are realistic and actionable, enhancing policy robustness and adaptability.

REFERENCES

Abewardhana, A., Karunarathne, N. C., Dayarathne, H., Gamage, R., Lakmali, N., & Genovese, P. V. (2020). *A Holistic Approach to National Security of Sri Lanka*.

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews*, *21*(1), 2263–2275.

Akhmaddhian, S., Supartono, T., Yuhandra, E., Budiman, H., & Rahmat, D. (2021, July). The government policy on the covid-19 handling viewed from environmental and biodiversity perspectives. In *IOP Conference Series: Earth and Environmental Science* (Vol. 819, No. 1, p. 012044). IOP Publishing.

Akhmaddhian, S. (2020). Discourse on Creating a Special Environmental Court in Indonesia to Resolve Environmental Disputes. *Bestuur*, *8*(2), 129-138.

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of big data for national security: a practitioner's guide to emerging technologies*. Butterworth-Heinemann.

Alizadeh, R., Lund, P. D., Beynaghi, A., Abolghasemi, M., & Maknoon, R. (2016). An integrated scenario-based robust planning approach for foresight and strategic management with application to energy industry. *Technological Forecasting and Social Change*, *104*, 162–171.

Al-Zahrani, A., & Al-Hebbi, M. (2022). Big data major security issues: challenges and defense strategies. *Tehnički Glasnik*, *16*(2), 197–204.

Baiocchi, D., Blum, I., & Richardson, A. (2018). *Defining and Assessing Adversary Threats to Space: Toward a Research Agenda.* RAND Corporation.

Balarezo, J., & Nielsen, B. B. (2017). Scenario planning as organizational intervention: an integrative framework and future research directions. *Review of International Business and Strategy*, *27*(1), 2–52.

Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. (2014). Big data in health care: using analytics to identify and manage high-risk and high-cost patients. *Health Affairs*, *33*(7), 1123–1131.

Becker, D., King, T. D., & McMullen, B. (2015). Big data, big data quality problem. *2015 IEEE International Conference on Big Data (Big Data)*, 2644–2653.

Berlin, G., & Neskovic, D. (2018). Bayesian Predictive Threat Modeling in Border Security. *Phalanx*, *51*(4), 24–27.

Bertalanffy, L. von. (1968). *General system theory: Foundations, development, applications*. G. Braziller.

Board, D. I. (2019). AI principles: recommendations on the ethical use of artificial intelligence by the department of defense: supporting document. *United States Department of Defense*.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, *23*(3), 317–332.

Bouchama, F., & Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. *International Journal of Business Intelligence and Big Data Analytics*, *4*(9), 1–9.

Bracken, P. (2012). *The second nuclear age: Strategy, danger, and the new power politics*. Macmillan.

Braun III, W. G., & Allen, C. D. (2014). Shaping a 21st Century Defense Strategy. *Joint Forces Quarterly*, *73*(2), 54.

Braun, V., & Clarke, V. (2021). Adapting Defense Doctrines to Hybrid Threats: Lessons from Recent Conflicts. *Defense Studies*, *22*(4), 512–528.

 DOI: https://doi.org/10.61242/ijabo.24.396

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43–49.

Budiman, H., Barokah, T., Harjadi, D., Fathanudien, A., & Anugrah, D. (2022, August). The Application of Legal System Theory in Handling Consumer Dispute by the Consumer Dispute Settlement Agency (BPSK) Of Kuningan Regency. In *UNISET 2021: Proceedings of the 2nd Universitas Kuningan International Conference on System, Engineering, and Technology, UNISET 2021, 2 December 2021, Kuningan, West Java, Indonesia* (p. 52). European Alliance for Innovation.

Budiman, H., Suwari Akhmaddhian, S., & Erga Yuhandra, E. (2024). Conservation-Based Spatial Planning Policy Formulation to Strengthen Tourism Districts. *Pena Justisia*.

Budiman, H., & Akhmaddhian, S. (2023). The Implications of Law No. 11 2020 Concerning Job Creation on Regional Spatial Planning and Watershed Management. *Pena Justisia: Media Komunikasi dan Kajian Hukum*.

Cetorelli, V. (2017). Scenario planning for military strategy: A methodological exploration. *Military Psychology*, *29*(5), 359–371.

Chaniago, H., Muharam, H., & Efawati, Y. (2023). Metode Riset Bisnis dan Permodelan. *Bandung: Edukasi Riset Digital, PT*.

Chen, C. L. P., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences*, *275*, 314–347.

Chen, H., Chiang, R. H. L., & Storey, V. C. (2020). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, *36*(4), 1165–1188.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*, 171–209.

Chen, T. M., & Jøsang, A. (2020). The ethics of artificial intelligence and machine learning: A review and critique. *Journal of Big Data and Society*, *3*(2), 1–19.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development*, *20*(2), 96–121.

Clarke, R. A., & Knake, R. K. (2020). *The Fifth Domain: Defending our country, our companies, and ourselves in the age of cyber threats*. Penguin.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Dalkıran, E., Önel, T., Topcu, O., & Demir, K. A. (2021). Automated integration of real-time and non-real-time defense systems. *Defence Technology*, *17*(2), 657–670.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Darmawan, E., Yusuf, F., Suseno, E., Budianto, H., & Maesyaroh, S. (2021, June). Decision support system for the selection of exemplary teachers using profile matching method. In *Journal of Physics: Conference Series* (Vol. 1933, No. 1, p. 012013). IOP Publishing.

De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial intelligence and the future of defense: strategic implications for small-and medium-sized force providers*. The Hague Centre for Strategic Studies.

Derbyshire, J. (2019). Use of scenario planning as a theory-driven evaluation tool. *Futures & Foresight Science*, *1*(1), e1.

Djalante, R., Holley, C., Thomalla, F., & Carnegie, M. (2013). Pathways for adaptive and integrated disaster resilience. *Natural Hazards*, *69*, 2105–2135.

Djouzi, K., & Beghdad-Bey, K. (2019). A review of clustering algorithms for big data. *2019 International Conference on Networking and Advanced Systems (ICNAS)*, 1–6.

Djuniardi, D., Harjadi, D., & Fitriani, L. K. (2022, August). Problems, Motivation and Success of Women Entrepreneurs: a Study on the MSME Sector in Kuningan Regency, West Java During the Pandemic. In *UNISET 2021: Proceedings of the 2nd Universitas Kuningan International Conference on System, Engineering, and Technology, UNISET 2021, 2 December 2021, Kuningan, West Java, Indonesia* (Vol. 336). European Alliance for Innovation.

Eastman, R., Versace, M., & Webber, A. (2015). Big data and predictive analytics: on the cybersecurity front line. *IDC Whitepaper, February*.

El Khatib, M., Al Shehhi, H., & Al Nuaimi, M. (2023). How Big Data and Big Data Analytics Mediate Organizational Risk Management. *Journal of Financial Risk Management*, *12*(1), 1–14.

Fjäder, C. O. (2018). Interdependence as dependence: Economic security in the age of global interconnectedness. In *Geo-economics and power politics in the 21st Century* (pp. 28–42). Routledge.

Flynn, S. (2004). *America the vulnerable: How our government is failing to protect us from terrorism*. HarperCollins New York.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, *16*(10), 1644.

 DOI: https://doi.org/10.61242/ijabo.24.396

Freeman, L. (2020). Test and evaluation for artificial intelligence. *Insight*, *23*(1), 27–30.
Frieden, J. A., Lake, D. A., & Schultz, K. A. (2019). World politics: interests, interactions, institutions. *(No Title)*.
Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016). Big data analytics: Security and privacy challenges. *2016 IEEE Symposium on Computers and Communication (ISCC)*, 952–957.
Ghavami, P. (2020). *Big data management: Data governance principles for big data analytics*. Walter de Gruyter GmbH & Co KG.
Gheorghe, A. V, Tatar, U., & Gokce, Y. (2017). *Strategic Cyber Defense: A Multidisciplinary Perspective* (Vol. 48). IOS Press.
Glenn, J. C., Gordon, T. J., & Florescu, E. (2014). *2013-14 State of the Future* (Vol. 1). The Millennium Project.
Goldratt, E. M. (1990). *Theory of constraints*. North River Croton-on-Hudson.
Hao, K. (2020). *How artificial intelligence has transformed the intelligence community. MIT Technology Review. Retrieved* . MIT Technology Review. https://www.technologyreview.com/2020/07/08/1004721/how-artificial-intelligence-transformed-intelligence/](https://www.technologyreview.com/2020/07/08/1004721/how-artificial-intelligence-transformed-intelligence/
Herring, M. J., & Willett, K. D. (2014). Active cyber defense: a vision for real-time cyber defense. *Journal of Information Warfare*, *13*(2), 46–55.
Hoadley, D. S., & Lucas, N. J. (2018). *Artificial intelligence and national security*. Congressional Research Service Washington, DC.
Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, *121*(1), 17–30.
Jain, R., Chandrasekaran, A., & Sharma, R. (2021). Big Data and Artificial Intelligence in Cyber Defense. *Journal of Cyber Security Technology*, *5*(2), 67–83.
Jensen, B. M., Whyte, C., & Cuomo, S. (2020). Algorithms at war: the promise, peril, and limits of artificial intelligence. *International Studies Review*, *22*(3), 526–550.
Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147–169.
Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries*, *3*(3), 619–626.
Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1–34.
Kasowaki, L., & Alp, K. (2024). *Threat Intelligence: Understanding and Mitigating Cyber Risks*. EasyChair.
Katuk, N., Vergallo, R., Sugiharto, T., & Krisdiawan, R. A. (2022). A client-based user authentication scheme for the cloud of things environment. *Journal of Computer Science & Technology*, *22*.
Khan, A., Akhtar, N., Khan, S. U., & Jeon, G. (2021). A survey of the recent architectures of deep learning for anomaly detection. *Neural Computing and Applications*, *33*, 1–22.
Koch, W. (2021). On digital ethics for artificial intelligence and information fusion in the defense domain. *IEEE Aerospace and Electronic Systems Magazine*, *36*(7), 94–111.
Krippendorff, K. (2018). *Content analysis: An introduction to its methodology*. Sage publications.
Kröger, M., & Schäfer, M. (2016). Scenario development as a tool for interdisciplinary integration processes in sustainable land use research. *Futures*, *84*, 64–81.
Labu, M. R., & Ahammed, M. F. (2024). Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*, *6*(1), 179–188.
Maddireddy, B. R., & Maddireddy, B. R. (2020). Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 64–83.
Manalu, V. G., Rahimi, F., & Akbar, I. (2023). Entrepreneurial Orientation and Product Innovation Performance of MSMEs in West Java: Foresight Capabilities as a Mediating Variable. *Khazanah Sosial*, *5*(3), 508-519.
Manalu, V. G., & Adzimatinur, F. (2024). How Digital Transformation Can Affect Product Innovation Performance MSMEs: Evidence from West Java. *Jurnal Aplikasi Manajemen*, 22(1), 253-266.
Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435–452.
Masruroh, R., Budiman, A., Dodi, D., Komarudin, M. N., & Irawan, N. (2024). Self Control and Organizational Commitment Views of Cyberloafing Behavior. JURISMA: Jurnal Riset Bisnis & Manajemen, 14(1), 167-174.

 DOI: https://doi.org/10.61242/ijabo.24.396

McCue, C. (2014). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Butterworth-Heinemann.

Michael, O., Crowley, S., Eigenbrode, S. D., & Wulfhorst, J. D. (2013). *Enhancing communication & collaboration in interdisciplinary research*. sage publications.

More, R., Unakal, A., Kulkarni, V., & Goudar, R. H. (2017). Real time threat detection system in cloud using big data analytics. *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 1262–1264.

Moudy, R. M., Ingerson-Mahar, M., Kanter, J., Grant, A. M., Fisher, D. R., & Jones, F. R. (2014). Bridging the health security divide: Department of Defense support for the Global Health security agenda. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *12*(5), 247–253.

Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), 51–63.

Nirmala, V. W., Harjadi, D., & Awaluddin, R. (2021). Sales forecasting by using exponential smoothing method and trend method to optimize product sales in pt. zamrud bumi indonesia during the covid-19 pandemic. *International Journal of Engineering, Science and Information Technology*, *1*(4), 59-64.

Nurhandika, A., & Manalu, V. G. (2023). How poilitical connection moderate audit committee characteristics and csr: evidence from Indonesian companies. *Jurnal Mantik*, 7(3), 1653-1660.

Otaiku, A. A. (2018). A framework for hybrid warfare: Threats, challenges and solutions. *J Def Manag*, *8*(178), 374–2167.

Page, S. (2008). *The difference: How the power of diversity creates better groups, firms, schools, and societies-new edition*. Princeton University Press.

Passeri, A., & Marston, H. (2022). The Pendulum of Non-Alignment: Charting Myanmar's Great Power Diplomacy (2011–2021). *Journal of Current Southeast Asian Affairs*, *41*(2), 188–213.

Petrozzino, C. (2020). Big data analytics: ethical considerations make a difference. *Scitech Lawyer*, *16*(3), 14–21.

Plastiras, G., Terzi, M., Kyrkou, C., & Theocharides, T. (2018). Edge intelligence: Challenges and opportunities of near-sensor machine learning applications. *2018 Ieee 29th International Conference on Application-Specific Systems, Architectures and Processors (Asap)*, 1–7.

Polk, M. (2014). Achieving the promise of transdisciplinarity: a critical exploration of the relationship between transdisciplinary research and societal problem solving. *Sustainability Science*, *9*, 439–451.

Porkoláb, I., & Zweibelson, B. (2018). Designing a NATO that thinks differently for 21st century complex challenges. *Honvédségi Szemle–Hungarian Defence Review*, *146*(1), 196–212.

Rachmawati, E., Juminawati, S., Akbar, I., Bahri, K. N., & Cakranegara, P. A. (2018). The importance of understanding the application of marketing strategy for household MSME products on social media networks. *International Journal of Business, Economics and Management*, *5*(1), 76-85.

Rashid, A. Bin, Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International Journal of Intelligent Systems*, *2023*(1), 8676366.

Rassam, M. A., Maarof, M., & Zainal, A. (2017). Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. *Journal of Information Assurance & Security*, *12*(4).

Rehman, M. H., Chang, V., Batool, A., & Wah, T. Y. (2022). Big Data Analytics in Information Systems Research: Challenges and Opportunities. *Journal of Information Technology*, *37*(2), 102–123.

Riessman, C. K. (2008). *Narrative methods for the human sciences*. Sage.

Rijal, S., Sihombing, T. M., Akbar, I. A., Desembrianita, E., & Lubis, R. F. (2023). Peran Keunggulan Kompetitif, Inovasi Produk, dan Jaringan Bisnis terhadap Kinerja Ekonomi Daerah. *Sanskara Ekonomi dan Kewirausahaan*, *1*(03), 173-185.

Riley, M., & Venables, D. (2020). The New Age of Risk Analysis in Defense. *Defense and Security Journal*, *11*(3), 34–45.

Roff, H. (2020). Uncomfortable ground truths: Predictive analytics and national security. *Brookings National Security Report*.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253–259.

Syamfithriani, T. S., Mirantika, N., Yusuf, F., & Kurniadi, E. (2021, June). M-Commerce application acceptance analysis using Technology Readiness Index (TRI) model in Kuningan Regency. In *Journal of Physics: Conference Series* (Vol. 1933, No. 1, p. 012012). IOP Publishing.

 DOI: https://doi.org/10.61242/ijabo.24.396

Sarjito, I. A. (2023). *Kebijakan dan Strategi Pertahanan*. CV Jejak (Jejak Publisher).
Sarker, I. H. (2024). *AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability*. Springer Nature.
Sayler, K. M. (2020). Artificial intelligence and national security. *Congressional Research Service*, *45178*.
Schoemaker, P. J. H. (1993). Multiple scenario development: Its conceptual and behavioral foundation. *Strategic Management Journal*, *14*(3), 193–213.
Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentacion Cientifica*, *15*(4), 42–66.
Sharma, P., & Barua, S. (2023). From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. *International Journal of Information and Cybersecurity*, *7*(9), 31–59.
Singh, A., Gupta, S. S., & Jain, M. M. (2022). Adaptation of Modern Technologies and Challenges in the Defense Sectors. *Res Militaris*, *12*(2), 1547–1566.
Steinbock, D. (2014). The challenges for America's defense innovation. *The Information Technology & Innovation Foundation*, *36*(6), 366–374.
Supriadi, A., Djuniardi, D., & Hamzah, A. (2022). Pengaruh Overconfidence Bias, Mental Accounting Dan Familiarity Bias Terhadap Pengambilan Keputusan Investasi: (Studi Kasus Terhadap Korban Investasi Ilegal Binary Option). Journal of Global Business and Management Review, 4(1), 50-65.
Sutrisno, S., Agustiani, I., & Rahmantya, Y. E. K. (2023). Systematic Literature Review: Strategi Komunikasi Dalam Pemasaran Politik Partai. *Jurnal Ilmiah Edunomika*, *8*(1).
Symon, P. B., & Tarapore, A. (2015). Defense intelligence analysis in the age of big data. *Joint Force Quarterly*, *79*(4), 4–11.
Toops, S., Peterson, M. A., Vanderbush, W., Sackeyfio, N., & Anderson, S. (2021). *International studies: An interdisciplinary approach to global issues*. Routledge.
Unver, A. (2018). Digital open source intelligence and international security: a primer. *EDAM Research Reports, Cyber Governance and Digital Democracy*, *8*.
Verma, S., Bhattacharyya, S. S., & Kumar, S. (2018). An extension of the technology acceptance model in the big data analytics system implementation environment. *Information Processing & Management*, *54*(5), 791–806.
Wachjuni, W., Oktaviani, W., & Mahsyar, J. H. (2024). Strategies To Improve The Performance Of Msme's In Kuningan Regency. Journal of Social Research, 3(2), 609-619.
Webster, J. L., Reif, W. E., & Bracker, J. S. (1989). The manager's guide to strategic planning tools and techniques. *Planning Review*, *17*(6), 4–48.
Weigand, K., Flanagan, T., Dye, K., & Jones, P. (2014). Collaborative foresight: Complementing long-horizon strategic planning. *Technological Forecasting and Social Change*, *85*, 134–152.
Wibowo, S. K., & Rahmantya, Y. E. K. (2023). Systematic Literature Review Peran Teknologi Informasi Dan Komunikasi Terhadap Kinerja. *Jurnal Ekonomi, Akuntansi & Manajemen*, *3*(1), 567-577.
Wickens, C. D., Gordon, S. E., Liu, Y., & Lee, J. (2004). *An introduction to human factors engineering* (Vol. 2). Pearson Prentice Hall Upper Saddle River, NJ.
Wiharno, H., Rahmawati, T., Martika, L., Nurhandika, A., & Dewi, R. (2021, March). Investment Risk: Empirical Evidence from Indonesia Stock Exchange. In *Proceedings of the 1st Universitas Kuningan International Conference on Social Science, Environment and Technology,* UNiSET 2020, 12 December 2020, Kuningan, West Java, Indonesia.
Xu, C., Qin, J., & Fang, Z. (2020). Predicting regional conflicts using machine learning and big data analytics. *Journal of Conflict Resolution*, *64*(9), 1789–1816.
Yang, H.-B., Wang, X.-X., Liu, T.-T., Zhang, C., & Sun, D.-B. (2014). Practice Collaborative Innovation and Promote Interdisciplinary Integration. *2014 International Conference on Management Science and Management Innovation (MSMI 2014)*, 172–175.
Yuniawan, A. (2020). Artikel: Testing the Relationships between Human Resource Competence, Financial Aspect and SMEs Performance.
Yusuf, F., Rahman, T. K. A., & Subiyakto, A. (2024). Information Technology Readiness and Acceptance Model for Social Media Adoption in Blended Learning: A Case Study in Higher Education Institutions in West Java, Indonesia. *Journal of Applied Data Sciences*, *5*(2), 382-402.
Yusuf, F., Mirantika, N., Syamfithriani, T. S., Darmawan, E., & Irawan, D. (2021, June). Technology readiness and acceptance model as a factor for the use intention of LMS e-Learning in Kuningan University. In *Journal of Physics: Conference Series* (Vol. 1933, No. 1, p. 012005). IOP Publishing.

 DOI: https://doi.org/10.61242/ijabo.24.396