Formosa Journal of Multidisciplinary Research (FJMR)
Vol. 3, No. 6 2024: 1875-1884

Strategies and Challenges for Economic Resilience in the Era of Asymmetric Warfare

Achmad Mirza Apriansyah[1*], Mhd. Halkis[2], Rudy Sutanto[3]
Asymmetric Warfare Study Program, Faculty of Defense Strategy, The Republic of Indonesia Defense University, Indonesia
Corresponding Author: Achmad Mirza Apriansyah mirza.april13@gmail.com

A R T I C L E I N F O

Keywords: Asymmetric Warfare, Economics, Technology Information

Received : 18, April
Revised : 19, May
Accepted: 18, June

A B S T R A C T

The research, titled "Strategies and Challenges for Economic Resilience in the Era of Asymmetric Warfare," is motivated by the fact that technological developments and economic globalization promote economic growth in various countries, but as this infrastructure grows, it also creates vulnerabilities that can be exploited, especially in the era of asymmetric warfare. Asymmetric warfare in the economic sector is due to the fact that many aspects of the economy depend on information technology. Digital infrastructure, such as communications networks and information systems, is vulnerable to attacks. These attacks can be physical, such as sabotage of vital facilities, or digital, such as cyber-attacks on energy networks or financial systems, which are part of asymmetric warfare. This is what gives rise to the need for an economic defense strategy to face the challenges that exist in the era of asymmetric warfare. So, it is necessary to identify and analyze the role of the economy in facing current challenges.

DOI: https://doi.org/10.55927/fjmr.v3i6.9248
ISSN-E: 2829-8896
https://journal.formosapublisher.org/index.php/fjmr

INTRODUCTION

In general, asymmetric warfare is a war in which there is an inequality in strength or strategy between the parties involved. According to the National Research Council (DRN) in 2008, Asymmetric War is a form of conflict that originates from an unconventional way of thinking, outside the accepted norms of war and includes various aspects such as geography, demography, natural resources (SDA), as well as ideological, political, economic, social and cultural elements. In asymmetric warfare, there is always a confrontation between two or more parties with a marked power inequality. Since ancient times, a country's defense has not only been limited to military aspects but has also involved economic defense efforts. However, in the modern era, warfare has evolved, resulting in new challenges, especially with the emergence of asymmetric warfare. At the beginning of the introduction, convey the circumstances and background of the problem being discussed and the existing phenomena. Avoid conveying research results.

In the current global context, the economic aspect has found itself at the forefront of asymmetric warfare. Unlike traditional conflicts that focus on physical combat and demonstrations of military power, asymmetric warfare often exploits economic vulnerability as a means of gaining strategic advantage. Actors in asymmetric warfare, both state and non-state, have identified the economy as a vulnerability that can be exploited. By exploiting loopholes in financial, trade, and investment systems, as well as through tactics such as economic sanctions, sabotage, or cyberattacks on critical infrastructure, these actors seek to create instability, reduce investor confidence, and ultimately influence the policies or positions of an organization or country without the need for open military conflict. In the era of information and globalization, a deep understanding of the relationship between economics and asymmetric warfare is key to developing comprehensive defense strategies.

With technological developments and economic globalization, the world has become increasingly interconnected. Physical and digital infrastructure plays an important role in supporting and driving economic growth in various countries. However, as reliance on this infrastructure increases, so do the vulnerabilities that can be exploited, especially in the era of asymmetric warfare.

As previously explained, asymmetric warfare, in contrast to conventional warfare, usually involves fights between parties who have disproportionate strength and resources. In this context, the weaker party will look for and exploit its opponent's weak points, and one way of doing this is through attacks on infrastructure. These attacks can be physical, such as sabotage of vital facilities, or digital, such as cyber-attacks on energy networks or financial systems. In today's digital era, communications networks and information systems support business operations, government, and daily activities. Many aspects of the economy depend on information technology. Cyberattacks against this infrastructure can damage data, steal sensitive information, or even halt business operations (Lewis, 2018).

Unfortunately, even though the importance of this infrastructure has been recognized, public awareness regarding the threat of asymmetric warfare is still low. Many do not yet understand how vulnerable their infrastructure is to

attacks and what impact this will have on the economy. Therefore, increasing public awareness is one of the keys to strengthening infrastructure resilience (Fran H. Norris and et.al. 2008).

In a national context, Indonesia's rapid growth makes it a potential target for various threats, both physical and cyber. Attacks on vital infrastructure can hinder economic growth, disrupt social stability, and damage a country's international image (A. Sudaryanto, 2017). The government, private sector, and society, as well as stakeholders, need to collaborate to overcome this challenge. They need to identify vulnerabilities, develop defense strategies, and ensure that the infrastructure can recover quickly after an attack. Apart from that, education and training for the community are also needed to increase awareness and readiness to face various threats that occur.

Based on this introduction, the problem is how to increase the resilience of physical and digital infrastructure to ensure that economic operations continue despite disruptions or attacks, and how to increase public awareness of the challenges of economic resilience in the era of asymmetric warfare, as well as the most effective strategies for increasing awareness and preparedness. Society in facing these threats. Through this article, the above problems will be discussed, with the aim that readers can understand the role of the economy in the context of economic defense strategies and challenges in the era of asymmetric warfare.

LITERATURE REVIEW

Expalantive Theory

Explantive theory is an approach in science that is used to explain, predict, and develop something based on phenomena that occur. Current developments show changes in various sectors of social life, resulting in relations between international communities developing. In the context of international relations, the explanatory theory will explain the causes of events to build a causal picture between two or more variables, as well as expand the understanding of contemporary international politics. (Linklater, 1996).

Human events or situations can often be explained best based on cause-and-effect relationships. However, the complexity and dynamics of these events and situations often require a broader explanation than just a cause-and-effect relationship. Clandestine and degree of publicity provide perceptions and narratives regarding modern terrorist activity that are complex. Therefore, constructs are needed that help understand complex and confusing events or situations through the source of testable causal theories (Davidoff, 2019).

Peace Education Theory

The dynamics of Indonesian society, the structure and relationships of society are not static entities, but are shaped and constantly reshaped by social interactions. The process of interaction that takes place places an obligation on society to create peace. In the scientific field, education can be used as development so that individuals can be globally responsible and able to create peace, this is called peace education (Reardon, 1988)

The theory of peace education proposes that education can be employed as a tool to promote peace, reduce conflict, and build more just and inclusive societies. Peace education, as an inquiry-based endeavour, is not about providing definitive answers, but rather about generating new questions and processes at every stage. (Bajaj, 2015). This means that peace education emphasizes the importance of generating new questions and undergoing a dynamic process at each stage, which can assist individuals in a more comprehensive understanding of phenomena, the identification of sustainable solutions, and the encouragement of positive change in society. Consequently, social conflict will be regarded in education as an integral component of the process of fostering critical thinking, reflection, and innovation in the context of conflict and peace.

METHODOLOGY

According to Hillway, quoted by Kaelani, research is nothing other than a study method that is carried out by someone through careful, perfect research into a problem, so that an appropriate solution to the problem is obtained (H. Kaelani, 2012). Basically, the research consists of a series of scientific activities that can be either qualitative or quantitative, or both.

The type of research used in this research is qualitative research methods and a descriptive approach. Descriptive qualitative research is research to explain a phenomenon or event based on observations on the problems studied, namely those related to the use of economics in determining strategies and facing the challenges of economic resilience in the era of asymmetric warfare.

The data collection used in this research is a literature study that will use library data as a source of information, such as books, journals, articles, and other sources that are relevant to the research subject. However, the data in the literature is a secondary source, so researchers obtain information that is not original data from the field. Therefore, data collection in this research was carried out by examining and searching for several books, journals, documents from print media, or other information relevant to the subject matter.

RESEARCH RESULT

Discussion about economic growth and national development, physical and digital infrastructure are two crucial components that support the wheels of the economy. In the Indonesian context, infrastructure has become one of the main priorities in national development, as stated in Rencana Pembangunan Jangka Menengah Nasional (RPJMN) (Bappenas, 2020). However, along with the growth and expansion of infrastructure, various vulnerabilities also emerge.

In this context, the challenges of economic defense are becoming increasingly complex. A country's economy, including its physical infrastructure such as transportation and energy, as well as its digital infrastructure such as communications networks and information systems, is a potential target in asymmetric warfare. Therefore, it is crucial to develop effective strategies to protect these vital components of a nation's infrastructure. A country's economy, including its physical infrastructure such as transportation and energy, as well as its digital infrastructure such as communications networks and information systems, is a potential target in

asymmetric warfare. The main challenges for economic defense in the era of asymmetric warfare:

1. Cyber Threats: With increasing reliance on digital technology, cyber attacks are becoming a very real threat to a country's economy. Enterprises and government institutions are equally vulnerable to these attacks, which can hinder operations, steal sensitive data, or damage critical infrastructure (Ben Buchanan, 2016).
2. Disinformation and Propaganda: In the information age, the ability to manipulate information and public opinion becomes a weapon in asymmetric warfare. Disinformation can cause panic, damage reputations, or even influence economic policy (Christopher Paul & Miriam Matthews, 2016).
3. Geopolitical Instability: Threats to trade routes, economic sanctions, and sudden policy changes by major powers can disrupt a country's economy (Joseph S. Nye, Jr 2011).
4. Terrorism and Sabotage: Physical attacks on vital economic infrastructure or assets, such as ports, stations, or energy facilities, can have long-term impacts on the economy (Walter Enders & Todd Sandler, 2012).

To address these challenges, it is necessary to update economic defense strategies. Some steps that can be taken include improving detection and response capabilities to cyber attacks, collaborating with other countries to share intelligence information and best practices, developing infrastructure that is more resilient and resistant to attacks, and educating the public about potential threats and how to protect themselves.

The strategies outlined above demonstrate the close relationship between the use of the economy in developing strategies and addressing economic defense challenges in the era of asymmetric warfare, and Infrastructure Resilience, Education, and Public Awareness.

Infrastructure Resilience

In the era of asymmetric warfare, state infrastructure, both physical and digital, has become a strategic target. Vulnerable infrastructure can impact economic operations, cause trade disruptions, and undermine investor confidence. A country's economic strength is often measured by its ability to recover from a crisis, and this requires a resilient infrastructure.

Rothkopf (2014) argues that threat-resistant infrastructure involves not only good physical security but also the ability to adapt quickly to changing threats. Infrastructure, whether physical or digital, is the backbone of the modern economy. In a world that is increasingly connected and dependent on technology, infrastructure resilience is crucial to ensuring the continuity of economic operations in the face of various threats.

1. Physical Infrastructure Resilience:

   physical infrastructure, which includes transportation networks (such as roads, bridges, and ports), energy systems (such as power plants and power grids), and other facilities that support the daily functioning of the economy and society, must be designed with potential threats in mind, such as natural disasters or terrorist attacks, to increase endurance.

- Planning and design are crucial for achieving this goal. Select durable materials, designs that minimize vulnerabilities, and ensure redundancy in the system (Yacov. Y. Haimes, 2009).
- Perform routine maintenance and inspections on existing infrastructure to identify and fix potential vulnerabilities before they become serious problems.
- Conduct emergency training for personnel and response teams to minimize the impact of possible disasters or attacks and speed up recovery.

2. Digital Infrastructure Resilience:

Digital Infrastructure Resilience refers to the ability of communications networks, data centers, cloud services, and other information systems to support business operations, government, and daily life.

- Cybersecurity is a key aspect of digital infrastructure resilience, which involves implementing firewalls, intrusion detection systems, data encryption, software updates, and patching to protect against known vulnerabilities (Ben Buchanan, 2016).
- Identity and Access Management is essential for providing control over who has access to critical systems and data. To prevent unauthorized access, multi-factor authentication, user rights management, and access monitoring can be employed (William Stallings, 2017).
- Additionally, a system must have backup copies and a disaster recovery solution in place to ensure continuity of operations in the event of a failure or an attack. Regular data backup and fast recovery solutions are included.

Cybersecurity awareness among employees and users is the first line of defense against attacks when they occur. Regular training and attack simulations can improve preparedness and response to incidents.

Education and Public Awareness

In the era of asymmetric warfare, public awareness and readiness play a crucial role in facing threats. Public awareness of potential threats and ways to protect oneself from them can determine a country's ability to face and recover from attacks. According to Paul and Matthews (2016), disinformation and propaganda can influence public perceptions. Therefore, public education is key in countering false narratives.

Asymmetric warfare has transformed the global defense and security paradigm.Modern warfare encompasses multidimensional threats that are often challenging to detect and anticipate, extending beyond conventional military power. Economic defense is one of the critical aspects affected by asymmetric warfare. However, to what extent will society understand this challange.

1. Public understanding of asymmetric warfare.

Asymmetric warfare, which often involves non-state actors and unconventional tactics, may be less understood by the general public than conventional warfare, which involves fighting between two military forces. This type of warfare often exploits psychological vulnerabilities, including by attacking the economy to create fear, uncertainty, and financial loss.

2. Importance of Public Awareness

Unaware people can become easy targets for asymmetric warfare tactics. For example, they may be more susceptible to disinformation or cyberattacks designed to damage the economy (David Rothkopf, 2014). Second, an unaware public may not support or understand government policies aimed at addressing the threat.

3. Strategies to Increase Awareness and Readiness
    a. Public Education. Including the topic of asymmetric warfare and its impact on the economy in the school curriculum can build understanding from an early age (Paula Smith, 2011). In addition, the government and civil society organizations can conduct campaigns to educate the public about the threat of asymmetric warfare to the economy (Lilie Chouliaraki, 2010).
    b. Simulation and Exercise. Conducting simulations or exercises in a community can prepare the community for the possibility of economic disruption due to asymmetric warfare. In addition, workshops can be held to provide communities with the skills and knowledge to protect themselves and their communities.
    c. Work with the media. The media plays an important role in disseminating information. Collaboration between the government and the media to provide accurate and relevant information can increase public awareness (Denis McQuail, 2010).
    d. Building resilient communities. Developing resilient communities, where community members support each other, can increase preparedness for the threat of asymmetric warfare (Fran H. Norris and et.al. 2008).
    e. Leverage technology. Technology can be used to disseminate information, detect threats, and respond quickly. For example, applications that inform the public about threats or actual economic disruptions.

Private Sector Involvement. Business plays an important role in the economy and can be a strategic partner in raising public awareness. Employee training, CSR campaigns, and other initiatives can be implemented (David Chandler & Jon Coaffee, 2016).

CONCLUSIONS AND RECOMMENDATIONS

In the era of asymmetric warfare, a nation's economic defense depends not only on the physical and digital strength of its infrastructure, but also on the awareness and preparedness of its people. As the backbone of economic activity, infrastructure is often the primary target of asymmetric attacks due to the widespread impact it can have on the economy and society. Therefore, the importance of improving the resilience and redundancy of these systems cannot be ignored. This requires the integration of advanced security technologies, personnel training, and cross-sector collaboration to address ever-changing threats.

But a strong infrastructure alone is not enough. Society plays a critical role as the first line of defense against asymmetric threats. Public awareness of potential threats and how to recognize and respond to them is key to

minimizing the impact of an attack. Unfortunately, there is often a gap in this awareness at various levels of society.

Public education and community training strategies are important to overcome these challenges. Collaboration between governments, NGOs, the private sector and the media can ensure that the information disseminated is accurate and relevant. Through educational campaigns and public awareness initiatives, individuals can be empowered to act as protectors of themselves and their communities in the face of threats.

Thus, effective economic defense in the context of asymmetric warfare is a combination of resilient infrastructure and an informed and prepared society. These two aspects must be strengthened and improved so that the country can protect itself from potential disruptions that could affect its economic growth and stability.

REFERENCES

Bappenas (Badan Perencanaan Pembangunan Nasional). (2020). Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020-2024. Jakarta: Bappenas

Buchanan, Ben. (2016). The cybersecurity dilemma: network intrusions, trust, and fear in the international system. King's College London (University of London).

Chandler, David, & Jon Coaffee. (Eds.). (2016). The Routledge Handbook of International Resilience. Routledge.

Chouliaraki, L. (2010). Post-humanitarianism: Humanitarian communication beyond a politics of pity. International Journal of Cultural Studies.

Davidoff, F. (2019). Understanding contexts: How explanatory theories can help. *Implementation Science*, *14*(1), 1–9. https://doi.org/10.1186/s13012-019-0872-8

Enders, Walter & Todd Sandler. (2012). The Political Economy of Terrorism. Cambridge University Press.

H. Kaelani, (2012). Metode Penelitian Kualitatif Interdisipliner Bidang Sosial, Budaya, Filsafat, Seni, Agama dan Humaniora, Yogyakarta : Penerbit Paradigma.

Haimes, Y. Y. (2009). On the Complex Definition of Risk: A Systems-Based Approach. Risk Analysis

Kompas. (2023) Perang Asimetris, Bentuk Perang Baru. Retrieved from https://tekno.kompas.com/read/2008/07/10/21091857/perang.asimetris.bentuk.perang.baru accessed on April 18th, 2023

Lewis, J. A. (2018). The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations. Oxford University Press.

Linklater, S. B. dan A. (1996). *Theories of International Relation*.

Norris, F. H., et al (2008). Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. American Journal of Community Psychology.

Nye, J. S. (2011). The Future of Power. PublicAffairs.

Paul, Christopher & Miriam Matthews (2016). The Russian "Firehose of Falsehood" Propaganda Model. RAND Corporation.

Paula Smith. (2012). Teaching Controversial Issues in the Classroom: Key Issues and Debates. Continuum

Rothkopf, David. (2014). National Insecurity: American Leadership in an Age of Fear PublicAffairs.

Smith, P. (2011). Teaching Controversial Issues in the Classroom: Key Issues and Debates. Continuum.

Stallings, William. (2017). Network Security Essentials. Prentice Hall

Indrawan, R. M., & Widiyanto, B. (2016). Offset Policy in Building State Defense Independence. Jurnal Pertahanan, 6(2), 29–50.

Moleong, L. J. (2017). Metodologi Penelitian Kualitatif. Jakarta: PT Remaja Rosdakarya.

Tickner, J. A. (1995). "Re-visioning Security", in Ken Booth and Steve Smith. In International Relations Theory Today. Oxford.