World Journal of Social Science and Humanities
www.worldsocialjournal.com
Online ISSN: 3107-989X
Received: 03-12-2025, Accepted: 02-01-2026, Published: 17-01-2026
Volume 2, Issue 1, 2026, Page No. 5-19

Intelligence approaches for protecting Tanzania's path to a USD $1 trillion economy

Dr. Vitalis Mdoe
School of Security and Global Studies, American Military University, United States

Abstract
The paradigm shift in the national security posture is required by the ambitious vision of the state of attaining a USD $1 trillion economy by 2050 to be realized in the Development Vision 2050 of Tanzania. This paper will discuss the essential nature of intelligence methods in protecting such an economic path. With the United States and Europe as background on the use of intelligence frameworks, the paper examines the manner in which economic security has taken center-stage as a national security. It then puts these methodologies into the context of the Tanzanian and East African context, with an examination of the Tanzania Intelligence and Security Service (TISS) Act of 1996 and amendments of 2023. The paper assumes that an intelligence-based and proactive response is required to prevent a variety of threats, such as economic espionage, supply chain failures, critical infrastructure risks, and instability in the region. By applying a thorough examination of open-source intelligence (OSINT), systematic methods of analysis, and case analysis, the paper suggests a multi-layered intelligence framework of Tanzania. This framework focuses on the public-private partnerships, domestic intelligence cooperation in East African Community (EAC) and incorporation of economic intelligence into national policy making. The article concludes that it is only through such methodologies that Tanzania will be able to safeguard its economic development not only but also strengthen its strategic position as a regional economic superpower.

Keywords: Tanzania, USD $1 trillion economy, development vision 2050, national security posture, intelligence methods economic security

Introduction

The 21st century has seen a radical transformation of the international security environment the economic prowess ceases to be, by definition, an end but major tool of statescraft and primary object of geopolitical rivalry. There is a lack of demarcation between national security and economic policy that has led to the birth of economic security as an element of sovereignty and stability of a nation. This paradigm shift is especially relevant to the emerging economies such as Tanzania that have paved the way with a bold plan to become a USD $1 trillion economy by 2050. This vision as embodied in Tanzania Development Vision 2050 (Dira 2050) is an upfront project that will need not only sound economic planning and implementation but also an advanced and progressive security system to protect its development.

Fig 1: Tanzania Development Vision 2050 - Economic Transformation Goals

The path of the trillion-dollar economy would be full of a complicated list of threats going beyond regular military issues. These are, but not limited to, economic spying to steal proprietary technology and trade secrets, the weaponization of supply chains to form chokepoints and dependencies, cyberattacks against critical infrastructure and the destabilizing power of regional conflicts and terrorism. The safety of economic viability is currently becoming a key national security objective of advanced economies as the 2025 National Security Strategy of the US and the 2025 Economic Security Doctrine of the European Union indicate. In the case of Tanzania, which is endowed with a lot of natural resources and is well placed strategically as an entry point to East and Central Africa, the stakes are even greater. The capacity of the Tanzania Intelligence and security service (TISS) and other national security agencies to detect, predict and counter these multi-dimensional economic threats determines the successful implementation of the Vision 2050.

This paper will contend that an offensive, intelligence driven strategy is invaluable in safeguarding the economic rise of Tanzania. It will examine the ways of modifying and implementing the proven intelligence practices in the US and Europe to the specifics of the situation in Tanzania and the East African region. The paper will evaluate the present capability of the intelligence community in Tanzania to cope with the economic security issues by analyzing the legal framework of the TISS Act of 1996 and its amendments in 2023. Moreover, it will also explore the urgent need of regional collaboration in the East African Community (EAC) in order to combat transnational threats that may drive down the economic stability. This article will provide a detailed examination of intelligence tradecraft, such as open-source intelligence (OSINT) and organized analytic processes, to suggest an extensive intelligence model that will serve the economic interests of Tanzania.

Such a framework will make clear the need of all partnerships between the state and the business, building of special economic intelligence services, and the intervention of smooth incorporation of intelligence evaluations into national economic policy-making. Finally, this paper argues that strategic use of intelligence is not only a defensive action but also an enabler of the economic transformation of Tanzania and that this way to the trillion-dollar economy is not only safe but also sustainable.

Research Questions

This article seeks to answer the following key research questions:

1. What are the primary economic security threats facing Tanzania on its path to achieving a USD $1 trillion economy by 2050?
2. How can foundational intelligence methodologies from the United States and Europe be adapted to the Tanzanian and East African context to enhance economic security?
3. To what extent does the existing legal and institutional framework of the Tanzania Intelligence and Security Service (TISS) and its 2023 amendments equip the agency to address contemporary economic security challenges?
4. What is the role of regional intelligence cooperation within the East African Community (EAC) in mitigating transnational threats to Tanzania's economic development?
5. What are the components of a comprehensive, intelligence-led framework that can effectively protect Tanzania's critical infrastructure, supply chains, and strategic industries from both state and non-state actors?

Empirical Literature Review

The concept of economic security and the way it can be combined with national intelligence is a widely discussed academic and policy issue. The frameworks and methodologies that have been established in the United States and Europe will be discussed at the beginning of this literature review because the nexus between economic vitality and national security has long been a subject of concern in these regions. It will then proceed to explore the context of the Tanzania and the wider East African region, and the ways in which these concepts are being adapted and applied to solve unique regional challenges and desires.

Foundational Frameworks: The US and European Experience

This paradigm shift in perceiving economic security as one of the central elements of national security is an outstanding characteristic of statecraft in the 21 st century. This development in the United States is clearly expressed in the major policy documents of the country. The 2025 National Security Strategy, in its turn, makes it clear that economic strength is at the heart of national power and that a robust economy is a requirement of a robust military and diplomatic presence on the international level [1]. The 2023 National Intelligence Strategy also supports this viewpoint by outlining the increasing role of the intelligence community in comprehending and curbing the threats to the economic security and prosperity of the country [2]. In the 2025 report, U.S. Economic Security: Winning the Race to Technologies of the Future, the Council on Foreign Relations gives an in-depth account of the vulnerabilities in critical supply chains and especially in the areas such as semiconductors, rare earth minerals, and biotechnology as well as recommends an active and intelligence-focused onshoring and protection of these important resources [3].

The European Union has also adopted an inclusive view of the economic security as was reflected in its December 2025 Economic Security Doctrine.

This framework is a major move towards a concerted European policy, where many policy tools are combined, trade, competition, cybersecurity, anti-coercion, and sanctions to name a few [4]. One of the main principles of the EU strategy is the so-called concept of de-risking that presupposes the necessity to eliminate the risks of being dependent on one supplier and avoid the threat of economic blackmail without the need to wholesale decouple. The creation of dedicated centers by the UK, e.g., Supply Chain Centre, Critical Minerals Intelligence Centre, and the future European Critical Raw Materials Centre, is an indication of the fact that the use of market forces is not enough to provide resilience to supply chains [5]. The aim of these initiatives is to equip them with the requisite intelligence and analytical power to map their vulnerabilities, track supply chains and organize strategic responses to disruptions.

The intelligence methodology literature provides varying tools and techniques that can be used in economic security. A set of structured analytic techniques given by the CIA in the so-called Tradecraft Primer is also a helpful guideline that intelligence analysts should follow to reduce the impact of mental biases and enhance the quality of judgment [6]. Such techniques include Analysis of Competing Hypotheses (ACH), Devil's Advocacy, and Red Teaming, which are aimed at testing assumptions and covering as many possible outcomes as possible. Regarding economic security, one can utilize these methodologies to determine the probability and consequences of the diverse threats, starting with the state-sponsored economic espionage all the way to the interference with the vital infrastructure. Moreover, the rise in the significance of Open- Source Intelligence (OSINT) in economic analysis is indescribable. Collecting, analyzing and distributing the information in the publicly available sources means a potent means of learning about the trends in the market, possible weaknesses in the supply chain, and the actions of the state and non-state actors.

The Tanzanian and East African Context

Although the principles of economic security and intelligence are universal, they should be applied in the Tanzanian and the East African conditions, according to the geopolitical and economic situation peculiar to the region. The strategic drive toward the sound economic security framework can be obtained through the Development Vision 2050 of Tanzania, which is ambitious to have its USD dollar trillion economy [7]. The Tanzania Intelligence and Security Service (TISS), the leading intelligence agency in this country, is leading in this mission. The TISS Act of 1996 that created the agency vests certain extensive capabilities in the agency to gather, analyze, and share intelligence pertaining to the national security [8]. The recent amendments to the Act also highlight the dynamic character of security threats as it has been designated TISS as a national security and defense institution and extended its scope to cover a broader spectrum of issues [9].

Nonetheless, the implementation process of an economic intelligence system has been associated with a number of challenges in Tanzania. Natural resources such as gold, tanzanite, and critical minerals are richly endowed in the country thus making it the major target of illicit flow of finances, illegal mining, and other economic exploitation [10]. This natural wealth is an important element of economic security and needs advanced intelligence machinery to detect and overcome these threats. Moreover, the security of the critical infrastructure of Tanzania, such as the port of Dar es Salaam which is the key point of entry to several landlocked nations is critical. Cyber Security Strategy 2022-2027 is the document by the Tanzanian Government that recognizes the increasingly serious threat of cyberattacks and provides a roadmap to secure the necessary services and establish a reliable cyber environment [11].

Also of serious importance in determining the economic security situation of Tanzania are the regional security dynamics of East Africa. The risk of terrorism, especially by such organizations as Al-Shabaab, is a major threat to stability in the region and economic growth [12]. East African Community (EAC) has built a peace and security cooperation framework that it employs to share intelligence and undertake mutual operations to deal with transnational threats [13]. The success of these regional security arrangements is a crucial element in establishing a favourable environment in economic growth and investment. The porous nature of the borders, as well as the existence of cross-border criminal networks, make the security calculus even more complex, thus a coordinated and intelligence-led border management and law enforcement would be necessary.

Finally, the literature demonstrates that there is a strong tendency towards economic security being incorporated into national security policies in the developed world, and the emerging economies. The way to the trillion-dollar economy in the case of Tanzania is the proactive and intelligence-driven approach to security, which is designed specifically to suit the national and regional setting. This literature review will be expanded in following sections of this article to come up with a holistic framework of intelligence to safeguard an economic future of Tanzania.

Methodology

In this research, the qualitative, descriptive, and analytical research methodology has been used to examine the role of intelligence in safeguarding the economic development path of Tanzania. The study is based upon the thorough analysis of the literature and the official government policies, legal standards and the opinions of experts of the reputable think-tanks and academic institutions. The methodology process will synthesize information obtained through various sources and build a consistent and evidence-based argument that will answer the research questions at the heart of the study.

The study methodology is one-case study, with a special regard to the specific situation in Tanzania. The method enables a deep and comprehensive study of the intricate nature of the relationship between economic momentum, national security and intelligence. The time frame within which the case study falls is that of the vision of Tanzania Vision 2050, its inception to the projected time in which it should end. The Tanzanian intelligence community and specifically the Tanzania Intelligence and Security Service (TISS) is the unit of analysis.

Various primary and secondary sources were used to gather data to use in this study. The official government documents are the primary sources, including the Tanzania Development Vision 2050, the TISS Act of 1996, and the amendment of the Act of 2023. The secondary sources can be academic books and journal articles, reports issued by international organizations and non-governmental organizations, and articles in a reputable news source. The research questions informed the data collection process, in which the most emphasis was placed on gathering data that would possibly help to illuminate the primary themes and concepts of the study.

The thematic analysis was used to analyze the data. This entailed procedures of identifying, analyzing, and reporting patterns (themes) in the data. The theoretical framework of the study is what led to the analysis as it refers to concepts of the covered areas of intelligence studies, international political economy, and security studies. The process of analysis was repetitive in that the researcher alternated between the research subject and the theoretical paradigm to come up with a deep and detailed sense of the research subject.

There are a number of limitations of this study. To begin with, because of the utilization of open-source data, the study cannot get the classified information required to conduct a thorough and comprehensive review of the intelligence capability in Tanzania. Second, the single-case study design implies that the results can not be applied to other countries. Nevertheless, the detailed and contextualized nature of the study is an insight that can be utilized in other developing economies in developing economic intelligence capabilities. Conclusively, the research on the role of intelligence in safeguarding economic development implies that it is not related to the social and political aspects of the Tanzania vision 2050 generally.

The three stages of the research are designed, following the same steps of the article written in phases. The first step will consist of comprehensive review of the early literature on the topic of economic security, as well as intelligence methods in the United States and Europe. It involves critical evaluation of national security policies, the intelligence community policies, and scholarly works that have reshaped the current concept of economic intelligence. This stage aims at identifying a theoretical and conceptual framework, which will be utilized in the Tanzanian context.

The second phase of the study is the consideration of a particular case of Tanzania and the East African region in general. It includes the actual examination of primary source materials, such as Tanzania Development Vision 2050, the Tanzania Intelligence and Security Service (TISS) Act of 1996, and the amendment to the Act of 2023. The review of reports and analyses conducted by the international organizations, including the World Bank and the United Nations, and regional institutions, such as the East African Community (EAC), accompany these documents. The purpose of this step is to have an in-depth insight into the economic aspirations and current security architecture of Tanzania and threats and vulnerabilities that it is currently exposed to.

The third and last phase of the research is the synthesis and analysis of the information collected during the earlier phases. It is an analytical process that employs a structured qualitative analysis to find major themes, patterns, and relationships in the data. The study takes a comparative format in the comparison of the established intelligence framework of the US and Europe with the new demands and capabilities of Tanzania. This analysis is then applied to come up with a proposed intelligence framework of economic security of Tanzania. This framework is not just a piece of theory but rather it is based on the realities of the Tanzanian context and is set so as to be practical and flexible.

In this study, the triangulation of data on numerous sources will be used (policy documents, legal texts, scholarly literature, and commentaries of experts): it is expected that by such means the validity and reliability of the research results will be ensured. The descriptive part of the methodology offers a detailed and substantial account of the present circumstances of economic security intelligence whereas the analytical aspect offers a critical evaluation of the problematic issues and prospects of Tanzania. The ultimate aim of this methodology approach is to generate a thorough and analytical practice that can be discussed as adding value to the academic knowledge of economic security as well as practical formulation of effective intelligence strategies in new economies.

Analysis and Findings

This section entails a comprehensive assessment of the intelligence procedures needed to secure the economic aspiration of Tanzania based on the theoretical frameworks laid down in the literature review and implementing them in the particular setting of Tanzania and the East African region. The discussion is organized around the main research questions, including the analysis of the nature of the threat, the evolution of the intelligence tradecraft, the role of the Tanzania Intelligence and Security Service (TISS), the role of regional cooperation, and the elements of the holistic intelligence structure.

Threat Analysis for Tanzania's Economic Security

The journey that has taken Tanzania to a trillion-dollar economy has not been without any threats. The country experiences a multi-layered and dynamic threat environment that needs a multi-faceted and active intelligence reaction. The major threats to the economic security can be divided into the following:

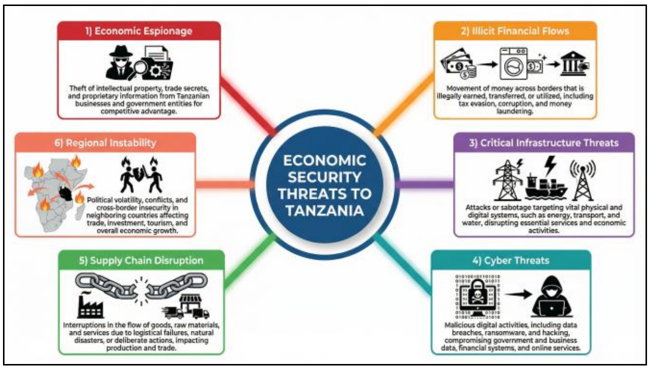

Fig 2: Economic Security Threats to Tanzania

Economic Espionage and Intellectual Property Theft: With the economy of Tanzania diversifying and scaling up the value chain, especially in fields such as manufacturing, technology and agro processing, the country will be more appealing to economic spies. State and non-state foreign actors can be interested in acquiring proprietary technology, trade secrets, and other sensitive business information to obtain a competitive edge. Such a risk is especially severe with regards to foreign direct investment (FDI), where alliances and joint ventures may be used as channels of transferring illicit technology. The intelligence problem is recognizing who is doing it, how they are doing it, and whom they are targeting, and coming up with an effective use of intelligence to counter the activities of these actors in an attempt to safeguard the growing innovation ecosystem in Tanzania.

Supply Chain Vulnerabilities: The COVID-19 pandemic and the war in Ukraine have provided a clear picture of how weak global supply chains and excessive dependence on one supplier can be. In the case of Tanzania that wants to become more part of the global economy, the issue of supply chain security is a burning issue. The level of reliance of the country on the imported capital goods, intermediate goods and technology poses vulnerability that can be exploited by the enemies. An effective point of reference to gauge the extent of risks that should be considered high by the Tanzania Government can be found in the Economic Security Doctrine of the EU where a 60-percent reliance on one supplier is considered to be a high level of risk [4]. The intelligence community should also be mandated to map vital supply chains, identify possible chokepoints and give early alerts of possible disruptions, be it due to geopolitical tensions, natural disasters or any other unexpected occurrences.

Critical Infrastructure Protection: The economic growth in Tanzania cannot be sustained without the security of the critical infrastructure of the country. The port of Dar es Salaam, the national energy grid, telecommunications networks, and financial systems are some of the key assets that can be targeted during physical and cyberattacks. Any successful attack of any of these assets would be catastrophic to the economy, as it would interrupt the trade, lead to mass power outages, and destroy the trust of the population. The Cyber security Strategy 2022-2027 of the Tanzanian Government is a good move in the right direction in dealing with these threats, but it should be backed up by a sound intelligence capability that would help to detect and thwart the threats before they become real [11]. This needs a multi-layered intelligence that integrates technical intelligence, human intelligence, and open source intelligence in order to give a holistic view of the threat environment.

Regional Instability and Terrorism: Tanzania is a poor country located in a shifting region, and economic opportunities of this country directly depend on the security situation of the neighbors. The current terrorism threat posed by the Al-Shabaab group, alongside the possibility of spillover the effects of conflicts of other countries in the region, is a major threat to the stability of the region and investor confidence [12]. Even terrorist attacks with no direct effect on the economic assets, may have a chilling impact on the tourism, foreign investment and trade. The intelligence problem is to keep track of the activities of terrorist groups and other military actors in the area, disorganize their funding and recruitment channels, and give early notices of the possibility of attacks.

Illicit Financial Flows and Natural Resource Exploitation: The fact that Tanzania is highly endowed in natural resources is a blessing and curse. Though these resources can drive economic development, they are also a target to the illicit actors who aim at exploiting them to their benefit. Smuggling, illegal mining, and other types of economic crime does not only deny the government the much needed revenue it destroys the rule of law and breeds a culture of corruption and instability [10]. The intelligence community has a major role to play in ensuring that these networks behind such illegal activities are not only detected but also broken down, both in Tanzania and outside its borders.

Localization of Western Intelligence Methodologies to a Tanzanian scenario.

TISS needs to be flexible and institutionalize various contemporary intelligence approaches to deal with such multidimensional threats effectively. The experience of the United States and Europe could be a hard-learned lesson in that respect, yet the latter methodologies should be adjusted to the particular needs and limitations of the situation in Tanzania.

Structured Analytic Techniques (SATs): The CIA in its Tradecraft Primer is a good guide to SATs, which may be applied to enhancing the quality and rigor of the intelligence analysis [6]. The risk of confirmation bias and groupthink can be reduced with the help of such techniques as Analysis of Competing Hypotheses (ACH), which presupposes that analysts should explicitly consider and debate alternative explanations of events. Devil advocacy, where an analyst gets the task of criticizing the mainstream narrative, can assist in finding the flaws in the arguments and concealed assumptions. Red Teaming, or the process of emulating the behavior of an adversary, may be a useful way of learning more about the possible vulnerabilities and attack vectors. These techniques would be important steps in the institutionalization of an analytical and evidence-based method of intelligence in TISS.

Open-Source Intelligence (OSINT): Information gathering, analysis and sharing of information that is publicly available is a very important intelligence asset in an ever-integrating world. OSINT may be utilized to trace the trends in the global economy, the risks in supply chains, the new technologies, as well as evaluate the potential and motivation of the state and non-state actors. In the case of Tanzania that might not be able to afford conventional intelligence gathering, OSINT provides an affordable means of propping up its situational awareness and complementing its other sources of intelligence. Creation of a specialized OSINT division in TISS, including the required educational resources and technologies, must be one of the priorities.

Public-Private Partnerships: The government and the private sector share the responsibility of safeguarding the economic security. Businesses tend to be the ones to notice new threats and vulnerabilities and their collaboration is critical to successful related intelligence gathering and analysis. Tanzania can use the Economic Security Doctrine developed by the EU, which places much emphasis on the trusted teams of advisors and secure information exchange systems [4]. TISS also needs to put in place official methods to interact with the private sector such as regular briefings, risk assessments, and a secure way of reporting suspicious occurrences. This would not only improve the intelligence community in their understanding of the threat environment, but it would also enable the businesses to be more proactive in their security.

The Role of TISS and the Legal Framework The key to the economic security system of the country is the Tanzania Intelligence and Security Service (TISS). The legal basis of the agency operations is the TISS Act of 1996 that gives the agency comprehensive authority to gather, analyze, and share intelligence that is sensitive to national security [8]. The amendments to the Act of 2023 also enhance the mandate of the agency where it is a national defense and security institution and has its mandate broadened to deal with a broader set of threats of the modern era [9].

Nevertheless, the efficacy of TISS in terms of economic security will not be based on its legal imperative only but also its institutional ability. The agency should train professional skills in economic analysis, financial intelligence, cybersecurity and supply chains management. This will involve a huge cost in training and recruitment, and the design of a career path that will appeal best talent and retain them in these areas. Moreover, TISS needs to develop a culture of teamwork and information exchange, both in the agency and other government departments, including the Ministry of Finance, the Bank of Tanzania, and Tanzania Revenue Authority.

Its legal system is strong, but should also be enforced in a way that will not violate the rule of law and safeguard the rights of citizens. TISS act has clauses to avoid keeping an eye on people just because they are participating in a lawful protest or dissent and the protection should be followed to the latter [8]. The issue facing TISS is balancing between its security mandate and its duty to act within the limits of the law. This necessitates the existence of powerful oversight procedures, both at the executive level and the legislative level to make sure that the authorities of the agency do not get in the wrong hands.

Regional Intelligence Cooperation in East Africa

Considering that many economic security threats in this region are transnational, the need to cooperate on regional levels is not a luxury but a necessity. East African Community (EAC) offers a platform to coordinate efforts on various issues of security such as terrorism, inter-country criminal activities, and money laundering [13]. Tanzania has a self-interest in enhancing such regional security agreements because the stability and prosperity of its neighbors cannot be separated by its prosperity.

Cooperation among regional intelligence demands a lot of trust and readiness to pass sensitive information. EAC has created a mechanism where leaders of the intelligence and security services meet and share information frequently, however, this mechanism only works based on the political will of the member states. Tanzania should be in the forefront of encouraging more intelligence sharing in the EAC especially in matters of mutual interest like counter-terrorism and maritime security and the interdiction of illegal financial flows.

Another potent tool that can be used to improve the security of a region is joint intelligence operations, which has specific transnational threats. On a case in point, an interagency task force may be formed to combat the smuggling of minerals and other natural resources, with intelligence officers of all the EAC member states collaborating to find out and destroy the criminal networks of the smugglers. Equally, a regional cybersecurity center may be developed to distribute awareness on the emergent cyber threats besides organizing responses to significant occurrences. The EAC member states are able to share their resources and experience which would result in a measure of security which would not be realized otherwise.

A Proposed Intelligence Framework for Tanzania's Economic Security

According to the discussion in this paper, four main pillars of the intelligence system to be used in ensuring the economic security of Tanzania are:

Pillar 1: Proactive Threat Identification: This pillar indicates the importance of having a proactive intelligence posture that preempts the occurrence of future threats by not merely responding to prevailing threats. This necessitates a methodical horizon scanning, trend analysis and scenario planning to determine the emerging risks and opportunities. TISS ought to create a special strategic analysis wing which will be charged with the responsibility of generating longitudinal analysis of the economic security environment.

Pillar 2: Integrated Intelligence Collection: This pillar would support a multi-disciplinary intelligence collection approach that integrates conventional intelligence collection techniques, including human intelligence (HUMINT) and signals intelligence (SIGINT), with more open-source intelligence (OSINT) and financial intelligence collection (FININT). This is aimed at providing an enriched and endowed intelligence picture, which might be applied in both strategic and operational decision-making.

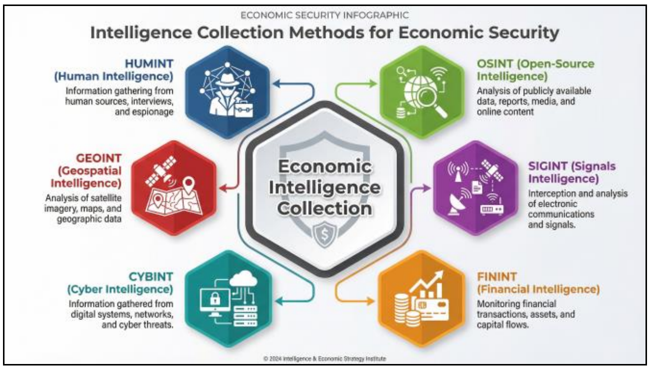

Fig 3: Intelligence Collection Methods for Economic Security

Pillar 3: Collaborative Analysis and Assessment: This pillar emphasizes the need of inter-agency coordination, and the importance of partnerships between the government and industries in the analysis process. The intelligence community is not the only one to provide economic intelligence; it is an activity that must be contributed to by various stakeholders, such as ministries of various governments, regulatory bodies, and the business industry. TISS must emerge as a hub of integration and correlation of economic intelligence, using the experience of all interested players.

Pillar 4: Intelligence-Led Policy and Action: This pillar underscores the importance of having a smooth flow of feedback between the intelligence community and policymakers to make sure that intelligence is used to inform national economic strategy. The intelligence tests must be prompt, pertinent, and operational and they must be incorporated in the decision making process of all the government departments with interest in the economic security. This would necessitate a close collaboration between the intelligence agents and the policymakers, which is based on mutual trust and respect.

Through this four-pillar approach, Tanzania will be able to develop an intelligence apparatus that is up to the test of the 21 st century. It will not just secure the economic assets of the country, but also enable the nation to have a secure and stable environment, in terms of investment, innovation, and sustainable development, long-term development.

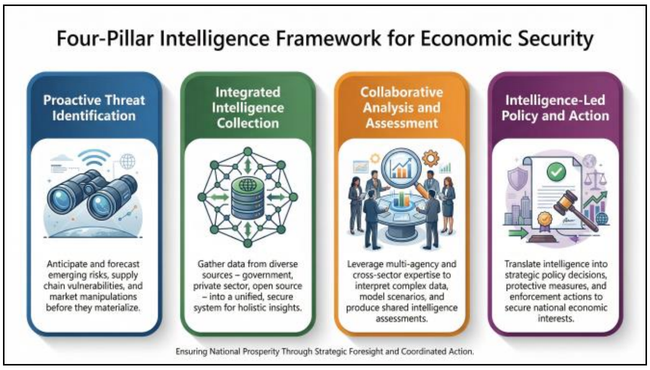

Fig 4: Four-Pillar Intelligence Framework for Economic Security

The Theoretical Foundations of Economic Intelligence

The field of economic intelligence is a relatively new phenomenon that has become prominent over the past few years; however, the endeavors of state-sponsored collection and analysis of economic information with strategic benefit have a lengthy history. The economic intelligence theoretics can be dated back to the mercantilist era in which the states considered economic competition as a zero-sum game and were vigorously trying to diminish the economic strength of their opponents. The notion of economic intelligence in the contemporary period has assumed a much wider scope of activities and it includes gathering of open-source information on business trends and hidden acquisition of trade secrets and proprietary technology.

One of the theoretical notions in economic intelligence is the concept of the so-called knowledge-based economy, according to which the competitive advantage of a nation is more and more based on the competencies of its capacity to generate, share and use knowledge. In this regard, intellectual property and technological innovation will be important national resources that cannot be lost to foreigners. The contribution of the works of scholars like Michael Porter who stressed on the significance of national competitive advantage has had an impact on the formation of the current perception of economic intelligence. The Diamond Model proposed by Porter (which defines national advantage based on four major determinants, namely: factor conditions, demand conditions, related and supporting industries, and firm strategy, structure, and rivalry) is a helpful tool in the analysis of economic strength and weakness of a country as well as in determining the possible targets of economic intelligence intelligence collection.

The other significant theoretical framework that helps to comprehend the idea of economic intelligence is the notion of economic statecraft which is the application of economic instruments and tools to obtain foreign policy goals.

Economic statecraft may be executed in various manifestations, although, as expressed by such theorists as David Baldwin and Jean-Marc F. Blanchard, it can be the imposition of sanctions and trade embargoes, foreign aid, and foreign investment. Economic intelligence is a vital part of successful economic statecraft which enables the policymakers with the information required to determine the possible effects of various policy choices; and also to oversee their actual execution. To illustrate, a government will be required to have a thorough insight of the monetary susceptibility of a foreign nation and its strategic trade connections, prior to administering sanctions to a foreign state. This demands an advanced intelligence operation that is able to gather and examine a broad scope of economic information.

The emergence of globalization and the growing interdependence of the international economy has been of significant influence to the theory and practice of economic intelligence as well. In the new fragmented and dispersed supply chains across multiple nations, the national economies were no longer as relevant as they used to be, traditionally. In its turn, intelligence agencies today need to take a more transnational outlook and track the movement of goods, capital, and information across borders and where there might be chokepoints and weak links in global supply chains. Supply chain intelligence has become a major sub-discipline of economic intelligence which aims at giving businesses and governments the information necessary to cope with the risks of supply chain disruption.

Case Studies in Economic Espionage and Supply Chain Disruption

The economic intelligence theories can only be interpreted by considering the practical case studies. The history of international relations is full of cases when states utilize their intelligence services to achieve an economic advantage, both the industrial espionage of the 19 th century and the cyber enabled intellectual property theft of the 21 st century. These example studies are helpful to the emergent economies such as Tanzania in terms of securing their economic assets.

The intellectual property theft campaign against the United States and other advanced nations launched by the Peoples Republic of China is one of the best documented cases of modern day economic espionage. At least 200 cases of reported Chinese espionage against the United States have been identified in the report by the Center of Strategic and International Studies (CSIS), 2025, targeting a vast array of industries, aerospace and defense, biotechnology, and information technology [14]. The tactics are diverse in such cases, and they involve cyber-attacks and insider recruitment, the use of a front company, and joint venture to obtain sensitive technology. A very good example of the insider threat that every organization is exposed to is the case of Jiaqiang Xu, who was a Chinese citizen and was convicted of having stolen proprietary software belonging to his employer, a U.S.-based defense contractor [15].

It is hard to put an estimate on the effects of this systematic campaign of economic espionage, but it is certainly considerable. The theft of intellectual property does not only dilute the competitive edge of a company but it also kills innovation and investment incentives. In the case of a developing nation like Tanzania that is trying to establish its own knowledge based economy, the risk of economic espionage is especially high. The immature technology industry, the emerging manufacturing industry and the biodiversity in the country are all possible victimization of foreign intelligence agencies.

Another significant economic security challenge that has been somewhat thrust into the limelight over the past years is the disruption of global supply chains. The COVID-19 crisis revealed the weaknesses of JIT production and the risks of being overdependent on one supplier of essential products. The next conflict in Ukraine also demonstrated the power of weaponizing supply chains, with Russia trying to leverage its dominance over energy resources to blackmail European nations. Such incidents have caused fundamental reconsideration of supply chain management, where resilience and redundancy are considered the main focus.

In the case of Tanzania, the supply chain security is an important economic and national security concern. Imports make the country dependent on imports of all types of goods including machinery and equipment, pharmaceuticals, and consumer goods. These supply chains are important in that any disturbance in them would also affect the economy and health of the citizens of the country. The intelligence issue is to determine the most essential supply chains, determine the susceptibilities of the various supply chains, and create contingency plans to curb the probability of being affected. This involves a tight collaboration between the government and the private sector since businesses usually may represent the first to detect possible disasters of the supply chain.

In summary, the theoretical basis of economic intelligence and practical insights of real-world case studies looks like a good roadmap to Tanzania as it tries to safeguard its future economic situation. The later parts of this paper will expand this by formulating an effective and practical intelligence construct to the economic security of Tanzania. Human Intelligence (HUMINT) Aspect of Economic Security.

Although technical and open-source intelligence are crucial assets, one cannot overestimate the role of human intelligence (HUMINT) as a factor in economic security. HUMINT gives the finesse, background, and purposefulness that other intelligence fields are usually deprived of. As a part of the economic development of Tanzania, a strong HUMINT capability is needed to reveal the threats which cannot be easily detected in the open sources of information or the technical intercepts.

HUMINT has found one of its main uses in economic security within the field of counter-espionage. Human agents are frequently utilized by the foreign intelligence services to develop their sources in the government ministries, research organizations and even in private companies in order to get the access to sensitive information. These agents can be diplomats, business persons, academicians or even tourists. A highly-trained HUMINT can counter such threats through running counter-intelligence operations, screening the personnel of foreign posts in sensitive positions, and debriefing citizens of Tanzania who have been approached by foreign intelligence officers.

The human resources involved in the recruitment and management of foreign governments and corporations can also be an invaluable measure in understanding the strategy of the companies. As an example, an agency in a foreign ministry of trade may give prior notice of an imminent trade conflict or the introduction of non-tariff barriers. The multinational company may have a source that will give information about its investment intentions, its bargaining approach, and their evaluation of the business environment. Such intelligence could provide the Tanzanian policy makers with a great upper hand in their international negotiation processes as well as during the process of attracting and maintaining inwards foreign investments.

More so, HUMINT plays a critical role in comprehending the complicated and opaque world of shabby finance and natural resource smuggling. The networks of these activities are rather secretive and are usually based on personal relations and confidence. Human sources can be on most occasions the only way of obtaining the evidence required to break these networks. This involves a long-term and patient process of intelligence collection and keen knowledge of the local culture and social life.

In the case of TISS, training and tradecraft in the economic sector of HUMINT will necessitate a substantial expenditure. The officers will have to be trained on the art of recruitment, source handling and eliciting. They will as well be required to have a strong insight into the economics, finance, and international business. Officers who have work experience in these areas should be recruited. Moreover, TISS will have to have a definite legal and ethical system of the actions of the HUMINT operations, so that it could be implemented in the way, which is consistent with the law of Tanzania and the international standards.

The Challenge of Illicit Financial Flows in the Mining Sector

Mining is one of the major industries in Tanzania, the foundation of its economy and the driver of further expansion, which is especially susceptible to illicit financial flows (IFFs). According to a report by Global Financial Integrity (2025), beneficial ownership in the Tanzanian mining industry is also quite risky [10]. The report revealed that the compound and in most cases opaque ownership arrangements of mining firms could be utilized to hide the real beneficiaries of mining incomes, evade tax, corrupt and even launder money.

This is a two-fold intelligence problem in fighting IFFs. First, it involves having the capacity to trace the money, which involves a complicated financial deal that cuts across several jurisdictions into the ultimate recipients. This demands a great level of financial intelligence (FININT) and close collaboration with financial intelligence units (FIUs) in other nations. TISS, together with the Financial Intelligence Unit of the Tanzanian (FIU-Tanzania) needs to establish the ability to process significant amounts of financial data and detect suspicious transactions and activity patterns.

Second, it must also have the capability of lifting the veil of incorporation and finding the real beneficial owners of mining companies. This can be addressed with the combination of open-source research, human intelligence, and forensic accounting. The intelligence analysts should be in a position to search the corporate records, legal documentation and media coverage to assemble the puzzle of corporate ownership. The real owners in most instances can be masked behind an array of shell companies and nominee directors and as such identification can be extremely hard.

Introduction of a beneficial ownership registry in a publicly accessible form as suggested by the Global Financial Integrity report would bring the mining industry to a lot more transparency. Nevertheless, a registry is not sufficient. The intelligence community should be equipped with the means and the knowledge of checking the data in the registry and exploring any anomalies or red flags. This needs a proactive and intelligence-based due diligence approach to be done to the new investors in the mining sector as well as current license holders.

The struggle against IFFs in the mining industry is not only an issue of safeguarding the government revenues; but it is also a question of national security. The networks that are used in smuggling money out of the country can also be applied in financing terrorism, organized crime, and other threats to national stability. Addressing IFFs, Tanzania is able not only to improve its economic growth but also national security.

The East African Community's Peace and Security Architecture: A Framework for Regional Economic Resilience

The East African Community (EAC) has been well aware of the fact that peace and security are preconditions of an economic integration and development. Article 124 of the Treaty to the Establishment of the East African Community gives a specific recognition to this connection giving a legal framework of a regional peace and security structure. This architecture has been developed over time to deal with various common security threats such as terrorism, piracy and transnational organized crime. In the case of Tanzania, this regional framework would be very effective in protecting its economic ambitions since any instability in any of the member states can easily be felt throughout the region.

The peace and security architecture of the EAC is a multi-layered and multi-dimensional structure, which involves a variety of institutions, policies, and functioning mechanisms. The top of this architecture is the Summit of Heads of State which offers general political direction and leadership. Policy making, implementation of the decisions reached during the Summit are handled by the Council of Ministers which consists of ministers of each partner state. This has been reinforced by the Sectoral Council on Interstate Security where ministers in the internal security field, the defense and the foreign affairs sphere convene regularly to discuss their actions, and devise a unified approach.

The Peace and Security Protocol is one of the most important elements of the peace and security system of the EAC and it was adopted in 2013. The protocol offers an elaborate basis of collaboration in a broad spectrum of security interests, including conflict prevention, management, and resolution; fighting against terrorism and piracy; and regulating the spread of small arms and light weapons. The protocol has also put in place several significant operational mechanisms including the EAC Early Warning Mechanism (EACWARN) which is a mechanism aimed at providing timely information on any potential conflict and crises and the EAC Standby Force (EASF); a regional peacekeeping force, which may be used to respond to security challenges in the region.

The EAC has been doing well in the field of intelligence cooperation in recent years. The intelligence and security heads of the partner states are in constant contact with each other sharing information and ensuring that all partners are on the same track. Such meetings offer a great opportunity to establish trust and create a shared vision of the threat situation within the region. In August 2025, the EAC defense and military intelligence chiefs again reiterated their dedication to a stronger relationship with regard to the security cooperation of the region with a specific emphasis on the joint training and capacity building as well as sharing of the best practices [16].

Nevertheless, even with these positive changes, peace and security architecture of the EAC continues to experience several challenges. The adoption of the Peace and Security Protocol has been sluggish and skewed and operationalization of critical systems including the EASF had been stifled due to a shortage of resources and political goodwill. A culture of secrecy and lack of trust among some of the partner states is also a limitation to the effectiveness of intelligence sharing. According to one study of the intelligence cooperation in the African region, although much is agreed regarding the necessity of the sharing of information, the specificities of what, when and how to share information tends to be a contention topic [17].

In the case of Tanzania, one of its priorities should include collaboration with its EAC partners to enhance the peace and security architecture in the region. This involves encouraging complete operationalization of the Peace and Security Protocol, financial and logistic assistance to the EASF and augmenting a culture of increased transparency and faith in the intelligence community. Tanzania would also be at the forefront in formulating regional measures to mitigate certain transnational challenges, including terrorism, cybercrime, and illegal financial transfer. Through investment in security in the region, Tanzania is able to contribute to establishing a more stable and predictable environment to economic growth and development, not just in itself but also in the entire East African region.

The Digital Frontier: Technology, Cybersecurity, and the Future of Economic Intelligence

Digital revolution has radically changed the economic intelligence landscape with both incredible opportunities and threats that have never existed before. In the case of Tanzania, a country that has adopted the digital revolution as an important element of its economic growth agenda, the capacity to negotiate this new horizon is a decisive factor in the future prosperity and safety of the country. The implementation process of these plans is guided by the Tanzania Digital Economy Strategic Framework and Government Cyber Security Strategy 2022-2027 which offer the roadmap to this journey, although their successful implementation is subject to a complex and progressive intelligence capability.

The possibilities of the digital revolution are huge. The massive and continually expanding sea of open-source information, through social media and news platforms to satellite images and financial market information, is a great and mostly unexploited source of economic intelligence. When artificial intelligence (AI) and machine learning (ML) are applied to this information, this data can be used by analysts to detect patterns, trends, and anomalies that would not be possible to notice using the traditional methods. As an example, AI-based tools have the potential to track global supply chains in real-time to give early notice of any possible disruptions. It is also possible to detect advanced financial offenses, like money laundering and terrorist funding, through the analysis of complex transaction networks.

Nonetheless, a new generation of threats has been created by the digital revolution as well. Those technologies which are propelling the economies can equally be turned into weapons by the opponents to take them down. Attacks on critical infrastructure, including power systems, financial systems, and telecommunication systems, may affect the economy in a disastrous manner. Cyber espionage leads to the theft of intellectual property and sensitive business information that poses a huge threat to innovation and competitiveness. And the disinformation and propaganda disseminated through the use of social media may break the social unity and confidence of the population.

In the case of TISS, the problem lies in the requirement to create the ability to perform in this new digital world. This will demand a heavy investment in technology and human capital. The agency must obtain the equipment and the skills to assemble, process and analyze vast amounts of digital information. It must also recruit and train a new generation of intelligence officers who will have competencies in cybersecurity, data science, and digital forensics. It must be the priority to create a special cyber intelligence (CYBINT) unit in TISS.

Additionally, TISS should collaborate with other government bodies, including the Tanzania Communications Regulatory Authority (TCRA) and the e-Government Agency (eGA) in order to come up with a coordinated and whole-of-government response to cybersecurity. This involves dissemination of information on the potential threats, coordination of response to large scale incidents, and the common standards and best practices on how to secure government networks.

The Tanzanian digital future is also dependent on the crucial role played by the private sector. Cyberattacks tend to attack businesses first, and businesses are better informed about the new threats and vulnerabilities. TISS ought to devise a formal information sharing and collaboration mechanism with the private sector in cybersecurity, the same manner that has been developed in the United States and Europe in terms of public-private partnership. The collaboration between the government and the business community will help develop a more robust and safe digital ecosystem among the entire population of Tanzania.

The TISS Act: A Legal Framework for Economic Intelligence?

The legal framework of the intelligence operations of the country is laid out by the Tanzania Intelligence and Security Service (TISS) Act of 1996 which was amended in 2023. This legislation requires a critical analysis to establish its appropriateness as an economic intelligence framework, as well as to establish any weaknesses and shortcomings that might have to be resolved.

The TISS Act gives the body a wide-range of mandate to access, match, and assess intelligence concerning security and also to provide advice to Ministers on security issues [8]. Although the Act does not specify that security is extended to economic security, the 2023 amendment, which introduces TISS as a national defense and security institution, creates the impression that the role of the agency is broadened. This enlarged mandate gives TISS a legal foundation to operate in economic intelligence like tracking that of threat to critical infrastructure, probing economic espionage, and judging the security consequences of foreign investment.

The Act also gives TISS various powers which are necessary in successful collection of intelligence. They are the authority to examine individuals and organisations that are likely to pose a harm to the security of the state, the ability to carry out security testing, and the ability to collaborate with foreign intelligence agencies [8]. These powers can be an effective instrument of defending the economic interest of Tanzania when properly exercised and in line with rule of law.

Nevertheless, there are also several limitations of the TISS Act that might impede its efficiency as the model of economic intelligence. The traditional security issues, espionage, sabotage, and terrorism, which the Act is concerned with, might not be adequate to counter the more complex and subtle issues of economic security. As an illustration, the protection of intellectual property, security of supply chains, and economic coercion threat are not clearly stated in the Act. Although these matters may well be seen as the wide scope of the problem of security, a more specific mandate would offer more clarity and focus to the operations of the agency.

The other possible constraint of the TISS Act is the absence of specific clauses regarding the public-private partnership. The coordination of the private sector as argued out earlier is the key to successful economic intelligence. The Act lacks an appropriate legal framework that such collaboration should be based on, and this may bring about uncertainties and unwillingness to provide sensitive information to the government by businesses. A formal system of information sharing among the public and the private should be one of the priorities and this should be under clear legal protection of both parties.

In addition, the provisions of the TISS Act regarding oversight and accountability will be essential to the prevention of the misuse of the increased mandate of the agency in the field of the economy. The Act creates some structure on how the minister and the parliament can carry out their supervision but the success of these structures will depend on political will to implement them. Since TISS will be increasingly involved in the economy of the country, it is necessary to make sure that its operations are under strict and independent control to secure the rights of the citizens and to avoid the attempts of the agency to serve as a political or commercial instrument.

To sum up, TISS Act is a good but deficient platform on which to build economic intelligence capacity in Tanzania. The high mandate and vast powers contained in the Act give TISS the legal authority it requires to confront many economic security threats. Nevertheless, in order to be effective, the Act will require further enhancement through the more explicit emphasis on economic security, a clear legal framework of the partnership between the state and businesses, and the effective oversight mechanisms. Through solving these shortcomings, Tanzania can be assured that its intelligence community is well placed to defend the economic future of the country.

Practical Implementation of the Proposed Intelligence Framework: A Phased Approach

The proposed four-pillar intelligence framework can only be successfully implemented in a gradual and progressive manner. In this section, a road map is given on how TISS and the government of Tanzania can develop a world economic intelligence capability within the next ten years. The implementation is segmented into three phases that have their priorities and milestones.

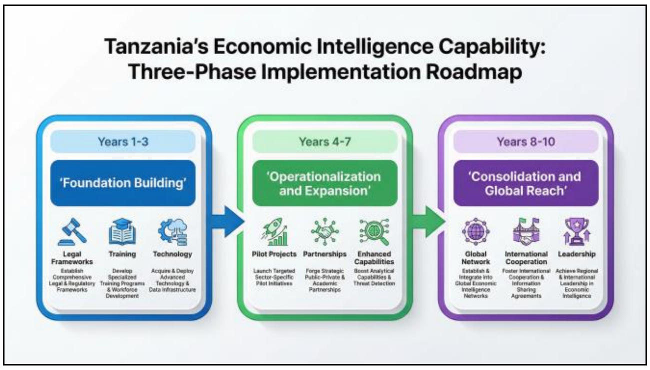

Fig 5: Tanzania's Economic Intelligence Capability - Three-Phase Implementation Roadmap

Phase 1: Foundation Building (Years 1-3)

The initial step to the implementation process should be the establishment of the economic intelligence underpinnings capabilities. It involves putting into place the legal and institutional infrastructure required, developing a fundamental numbers of trained staffs and obtaining the rudimentary technological foundation.

- **Legal and Institutional Reforms:** The initial move is to have an in-depth study of the TISS Act and other applicable legislation to establish and overcome any gaps or constraints. This will be followed by the formulation of a National Economic Intelligence Strategy, which would offer a clear mandate and a list of strategic priorities of the economic intelligence activities of a country. The strategic formulation must be formulated in a participative manner that will involve all the concerned government agencies and the stakeholders of the private sector.

- **Human Capital Development:** TISS must initiate an aggressive recruitment and training to develop a cadres of economic intelligence officers. It must also involve hiring people with economics, finance, business, and law backgrounds and also offer specialized courses in intelligence analysis, financial intelligence, and cybersecurity. One of the priorities should be the creation of a special Economic Intelligence Training Center in cooperation with a well-known foreign organization.

- **Technological Infrastructure:** TISS ought to invest in the fundamental technological infrastructure required to carry out economic intelligence, such as safe communications, data analytics applications, and a specific OSINT accumulation and examination framework. This phase must be concerned with the acquisition of proven and cost-effective technologies that can easily be fitted into the existing infrastructure of the agency.

Phase 2: Operationalization and Expansion (Years 4-7)

The second stage of implementation ought to be aimed at operationalizing the new economic intelligence capabilities and the further expansion of their scope and reach. This involves initiating a chain of pilot projects, implementing institutionalized structures of inter-agency and private partnership, and improving the technical collection of the agency.

Pilot Projects: TISS ought to initiate a cycle of pilot projects to experiment with its new economic intelligence instruments. The projects may target particular threats, e.g. illicit financial flows in the mining industry, or particular sectors, e.g. the telecommunications or financial services industry. These pilot projects should be informed by the lessons that they have provided in the further development of the capabilities of the agency.

- **Inter-Agency and Public-Private Cooperation:** TISS needs to implement procedures to cooperate with other government agencies and the business sector. This must also incorporate the formation of an inter-agency Economic Intelligence Task Force that involves all the relevant ministries and regulatory agencies and a number of industry-specific information sharing and analysis centers (ISAC) where the government and the private sector will be able to share information on any emerging threats and vulnerabilities.

- **Improved Technical Collection:** TISS must start investing in more sophisticated technical collection, i.e., signals intelligence (SIGINT) and cyber intelligence (CYBINT). This must be done in gradual and a step-by-step process with emphasis to be placed in the acquisition of capabilities that are specific to the threats that are posed to Tanzania.

Phase 3: Consolidation and Global Reach (Years 8-10)

The third and last implementation stage must be aimed at solidifying the success of the other two stages of implementation and extending the economic intelligence coverage of Tanzania to the world level. This will involve having the network of economic intelligence officers in strategic foreign offices, establishing an international OSINT surveillance capacity, and leading in regional and international intelligence collaboration.

Global Network: TISS needs to form a network of economic intelligence officers in key Tanzanian embassies and high commissions throughout the world. These would be officers who gather and analyze economic intelligence in their host countries as well as forging relations with their counterparts abroad.

- **Global OSINT Monitoring:** TISS must be able to create a global OSINT monitoring system, with the capacity to monitor the economic and political activities of the major countries and regions globally. This would enable the Tanzanian policy makers to have a better insight of the international economic environment and would be able to foresee and react to the threats and opportunities.

- **Regional and International Leadership:** Tanzania ought to aim at being at the forefront of regional and international intelligence in economic security matters. This may involve organizing local intelligence forums, exchanging of best practices with other African nations and attending international economic intelligence and security forums.

This gradual and step-by-step process will enable Tanzania to develop a world-standard economic intelligence capacity that will prove an invaluable resource on its way to a trillion-dollar economy. This will safeguard the economic resources of the country, as well as, strengthen the strategic status of the country as a regional and global economic force.

Conclusion

The desire by Tanzania to become a USD 1 trillion economy by 2050 is an ambitious and bold target that can easily change the country and the lives of its citizens. Yet this road is not the one without its dangers. The 21 st -century international security environment is an intricate and disputed space, in which economic power is simultaneously both an instrument of statecraft and a subject of attack. The medieval sense of separation between economic policy and national security is no longer applicable in this space. In the case of Tanzania, national survival, rather than prosperity is pegged on the protection of its economic assets, its critical infrastructure, and its strategic industries.

This paper has contended that Tanzania should adopt a proactive and intelligence-driven strategy in the protection of its economic future. Based on the practice of the United States and Europe, and the case of Tanzania and the East African region, this paper has suggested an elaborate economic security intelligence framework. This framework is anchored on four fundamental pillars namely proactive threat identification and integrated intelligence collection, collaborative analysis and assessment and intelligence-led policy and action. To achieve success in this framework implementation, a massive investment on the human capital, technology, and institutional reform will be required. It will also involve a new mindset whereby economic security is a collective responsibility between the government and the private sector where regional cooperation is not an option but a necessity.

Tanzania Intelligence and Security Service (TISS) is the service that is vital in this endeavor. The legal foundation of the involvement of the agency in economic intelligence is the TISS Act of 1996 in its updated form of 2023. Nevertheless, in order to be effective indeed, TISS will have to come up with certain specialized knowledge in such fields as economic analysis, financial intelligence, and cybersecurity. It should also create the culture of cooperation and information exchange, both with the governmental and the private sector. And it should be acting in a set of high supervision and accountability so that its authorities should not be misused.

The road to the trillion-dollar economy will be a long and difficult road, but it is a road that Tanzania can and will have to move on. Through a proactive and intelligence-driven response to economic security, Tanzania will be able not only to safeguard itself against the 21 st century threats but also to take advantage of the opportunities of a global economy. Defensive is not only strategy use of intelligence; it is an essential facilitator of the economic transformation of the Tanzania state as this way it is made sure that the dream of the wealthy and safe country turns into reality of all its inhabitants.

The Unseen Shield: The Role of Counterintelligence in Economic Security

Economic intelligence is devoted to collecting and using information to assist an economy in making decision whereas counterintelligence is the invisible barrier against the intrusion of the foreign enemies in taking a peep or causing havoc in the economic resources of the nation. With the ambitious economic agenda of the Republic of Tanzania, not to mention that counterintelligence is a luxury and an absolute need. The inability to secure sensitive economic data, sensitive technologies and deliberations on strategic policies can have disastrous results that will affect competitiveness, damage investor trust and ultimately jeopardize the national developmental process.

Economic counterintelligence has the primary role of detecting, disabling, and controlling the operations of the other intelligence services that are working against the economic interests of a country. It is a complicated and manifold problem, which needs profound understanding of the motives, means, and goals of the adversary. Foreign intelligence services employ very diverse methods of obtaining economic intelligence, including the employment of old time methods of human intelligence (HUMINT), including the recruitment of spies into high-level government and industry positions, and highly technical cyber espionage missions, which are capable of stealing huge amounts of data within seconds.

In the case of TISS, the building of a global economic counterintelligence strength will be achieved by a significant change of attitude and a big cost on new skills and technologies. The agency should not be in the defensive positions, where it aims at ensuring the information is never lost, but more proactive and aggressive, in that it attempts to disrupt and deceive the opponent. This needs intensive knowledge on the concept of denial and deception and also capability to operate advanced counter-espionage missions.

The identification of insider threats is one of the most critical issues of economic counterintelligence. The intelligence services of the foreign countries usually target to get people in the ministries of the government, the state owned corporations, as well as the companies that are privately owned with access to classified information. The reasons that influence these people can be different such as money, ideology or personal resentment. These insider threats need to be identified and neutralized using a multi-layered strategy, which involves conducting comprehensive background checks, frequent security awareness trainings, and application of complex monitoring systems to identify anomalous behavior.

Another priority of the economic counterintelligence is the protection of critical technologies. As Tanzania aims to ascend to the next level in the value chain and build its own local technological assets, it will also become an even more popular target of technology theft. TISS needs to collaborate closely with the business sector and the research community in order to determine the most vital technologies in the country and create a holistic approach to their safeguarding. This is to be comprised of physical security, cybersecurity, and a proactive counterintelligence program to prevent and intercept any attempts of technology theft.

In addition, critical economic counterintelligence would play a vital role in ensuring that the integrity of policymaking process is intact. The foreign intelligence service might want to sway the decision of the government through disinformation, raising their influence agents or using other covert methods. TISS needs to be in a position to detect and counter such covert influence activities so that the government policy is developed in the best interest of the people of Tanzania.

Finally, effective economic counterintelligence is also a vital element of an overall economic security policy. In the case of Tanzania, cultivation of such capability will be a long and a strenuous undertaking, though it is a challenge that the country must face in case it can meet the ambitious economic targets. With a constructed invisible barrier of counterintelligence, the Tanzania government can safeguard its economic resources, secure its technological future and have its path to the trillion-dollar economy not stampeded by the hidden hand of its foreign enemies.

The Blue Economy and Maritime Security: A New Frontier for Economic Intelligence

The long coastline of the Indian Ocean in Tanzania is the major economic factor which is not fully exploited. It has been noted that one of the major catalysts of future development in the Tanzania Development Vision 2050 is the concept of the blue economy, which includes a broad spectrum of economic activities created on the ocean, including fisheries and aquaculture, maritime transport and tourism. Nevertheless, the concept of the blue economy is closely connected with the problem of maritime security. The Indian Ocean is a disputed and intricate maritime area, the threats confronting it are numerous, among them piracy, unlawful, unreported and unregulated (IUU) fishing, smuggling and maritime terrorism. The security of the maritime zone in Tanzania is thus a major condition that determines the future sustainability of the blue economy.

A successful maritime security plan should be intelligence driven. The magnitude of the maritime space renders the policing process unattainable unless there is a clear insight into the type of threats and their probable locations. This necessitates a multi-dimensional intelligence endeavor that incorporates satellite imagery, aerial surveillance, coastal radar and a human intelligence capability to make up a complete picture of the maritime environment. To facilitate this, TISS in conjunction with the Tanzanian Navy, which is the maritime police and other interested agencies should design a specific maritime intelligence capacity to aid this.

IUU fishing is one of the greatest threats to the blue economy of Tanzania. It is believed that IUU fishing costs the world economy tens of billions of dollars every year, and the Western Indian Ocean is one of the hotspots of the practice. The IUU fishing does not only strip the marine environment of its fish stocks and destroys the ocean ecosystem, but it also leaves the coastal populations without a source of livelihood and the government without essential revenues. Hunting down IUU fishing will have to be an intricate intelligence campaign to determine the vessels, their owners, and their activity. This could be done by integrating vessel monitoring systems (VMS), satellite imagery analysis and sharing of information with the regional and international partners.

Another significant menace to the Indian Ocean maritime security is piracy. Although the cases of piracy have decreased in recent years, through the concerted efforts of the international naval forces, the threat has not been removed. The original causes of piracy such as poverty, political instability, and economic opportunities of communities in the coastal areas have not been solved. A new wave of piracy would be catastrophic to the maritime business, increasing the cost of insurance and compelling ships to use longer and more expensive routes. The intelligence problem is to track the operations of the pirate groups, to determine their safe haven, and to give early warning of their possible attacks.

Directive smuggling of prohibited good including narcotics, weapons and fake goods is another significant issue to maritime security in the area. Criminal networks utilize the same routes that are legitimately used to transport legitimate trade in moving their illegal cargo. Such interdiction of these smuggling activities must be of high level of intelligence collaboration, not only regionally but also among the international partners. TISS needs to liaise closely with other countries that have their counterparts to exchange information about the route, methods and networks used in smuggling.

Last but not least is the possibility of maritime terrorism. The terrorist groups can want to attack the ports, offshore oil and gas platforms or commercial vessels to disorient economic activity and create an atmosphere of fear. The figure above is a graphic reminder of this menace by an attack on the French oil tanker Limburg in 2002 off the coast of Yemen. Security in the maritime infrastructure is related to the proactive and intelligence-based strategy in securing the infrastructure, with the emphasis laid on the need to find and neutralize the terrorist threats prior to their realization.

Finally, blues economics would be significant in the future development of the Tanzanian economy, but a significant security problem. The defense of the maritime domain of the country needs an intelligence-driven and comprehensive security strategy, with an emphasis being put on the creation of a dedicated capability of marine intelligence, enhancing the collaboration with other countries, and resolving the factors that contribute to the maritime insecurity. A proactive and future-oriented approach to maritime security can help Tanzania to make sure that its blue economy would remain successful as well as safe.

Strategic Communication and Public Diplomacy: The Soft Power of Economic Intelligence

The geopolitical situation of the 21 st century does not view the strength of the nation as the size of its military and its economic production, but also in its capacity to create the narrative and transform the way other people think. This is soft power and it is the crucial, but frequently neglected aspect of economic security. In the case of Tanzania, a country with the aim of attracting foreign investment, marketing its exports and improving its regional and international position, a good communication of its economic stories is an extremely important strategic tool. Economic intelligence will play a significant role in this undertaking not only in the provision of the raw material of the strategic communication but also in the assistance of shaping the message and addressing the audience.

In economic security, strategic communication refers to the systematic and coordinated application of information in the promotion of the economics of a country. This can be done in numerous ways such as public diplomacy about tourism and investment, to specific messages to refute negative perceptions and misinformation. This is aimed at generating an optimistic and attractive story about the economy of the country, business environment and its prospects. The background of this story is economic intelligence, which includes the real and current data about the condition of the economy and power and weakness of various industries and the prospects of foreign investors.

Strategic communication involves public diplomacy. It entails meeting the foreign audiences such as the media, civil society and business community to establish relations and encourage better appreciation of the policies and values of the nation. In the case of Tanzania, foreign investment can be greatly attracted by the use of public diplomacy. Through demonstrating the political stability of the country, its dedication to economic restructure and also its pleasant investment environment, Tanzania can stand out among the rest of its competition and secure the long time high quality investment that it requires to reach its development objectives.

In this regard, economic intelligence could be very significant in combating the effects of disinformation and propaganda which could be employed by the enemies to disrupt the economic stability of a country. In the era of fake news and social media, one of the most important national security capabilities is to recognize and refute false stories. When it comes to the TISS, along with other governmental structures, it needs to come up with the ability to track the information landscape, predetermine possible threats, and work promptly and efficiently to address them. This involves a mix of conventional intelligence analysis, data science and strategic communication skills.

Moreover, economic intelligence may be applied in facilitating trade and investment promotion in a country. The usefulness of the intelligence community in enabling businesses to discover new opportunities and competing more efficiently in the global market can be achieved by giving the business detailed information about the foreign markets, such as market trends and regulatory requirements, as well as potential partners. It is a successful model that has been applied by several countries including South Korea and Japan whereby the intelligence service collaborates with the private sector in facilitating their international growth.

In the case of Tanzania, a strong economic intelligence capacity supported by the strategic development of a communication and public diplomacy should be one of the priorities. This will involve a different thinking about intelligence and in this, intelligence is not only understood as a means of identifying a threat but also as a means of generating opportunities. It will also need some new skills such as the skills in PR, marketing, and cross-cultural communication. Through the concept of soft power, which is economic intelligence, Tanzania will be not only able to safeguard its economic future, but also to increase its influence and the position in the world.

Ethical Considerations and the Social License to Operate: A Foundation of Trust

Tanzania has to deal with a complicated ethical issue as it builds its economic intelligence capabilities as well. The gathering, processing and application of intelligence, especially the economic field, pose an array of moral concerns that have to be resolved so that such new capabilities are not misused and applied in a way that would not go against the values of the nation and rule of law. Any inability to deal with such issues of ethics can prove devastating, as it will damage the trust of the population, the integrity of the intelligence services and in the end, the economic development, which they are meant to safeguard.

The possible conflict between the interest of the state to safeguard the national security and the interest of the commercial confidentiality of the private sector is one of the most important ethical issues in economic intelligence. The list of economic intelligence frequently needs to gain access to secret data about business, which may include business secrets, financial data, and plans. Although the provided information can be critical in identifying and alleviating economic security threats, its gathering and utilization should be handled with a lot of care not to impair the competitiveness of the private sector. TISS should come up with clear instructions and processes on how sensitive business information should be collected and managed with stringent restrictions on how it is spread and utilized. They are supposed to be in collaboration with the private sector when formulating these guidelines so that they are effective and just.

The other significant ethical issue is the possibility of economic intelligence application to gain political or personal interest. The intelligence services might collect information that can be a potent tool and there is always a danger that the information will be used to attack political opponents, personal scores and give an unfair edge to preferred businesses. In order to curb this risk, it is necessary to establish powerful and autonomous oversight mechanisms. This must incorporate external as well as internal checks and balances, on the one hand by the legislature and the judiciary. The oversight agencies should be granted the power and the means to probe any claims of misconduct and to make the intelligence agencies answer their deeds.

There are also several ethical concerns related to the employment of covert approaches in economic intelligence. Although covert action might be required in certain instances in order to deal with serious threats to national security, it should be administered sparingly and with a lot of care. Deception, manipulation and other underhand means may cause a poisonous impact on the credibility of the population and may tarnish the reputation of the country in the global arena. TISS needs to develop a strong and strict procedure of approval and control of covert operations, and the use of covert operations should be of high level. It is a procedure that must be used to make sure that all the covert operations are reviewed through a rigorous legal and ethical filtering process before approval.

Lastly, building a powerful economic intelligence environment should be followed by the promise of transparency and accountability to the people. The fact that intelligence work needs secrecy to some extent does not mean that it can be used as an excuse to perpetrate evil or to escape the focused attention of people. TISS ought to be as open as it can be concerning its operations, but this must not interfere with its sources and methods. This must involve constant issue of unclassified reports on economic security threats, and constant briefing of parliamentary committees and the media. Being transparent will help TISS gain the social acceptance and trust it has in its operations as well as can assure that it can enjoy the social license it requires to operate effectively.

To sum up, ethical aspect of economic intelligence cannot be seen as a minor point of all successful economic security strategies; it is a keyword of any successful economic intelligence strategy. Through direct confrontation of the ethical issues, creating a unified set of principles and effective control systems, and by means of its transparency and openness of the government, Tanzania can make its economic intelligence capabilities become the instrument of good, secure the economic future of the country without compromising its democratic principles.

A Proposed Structure for the Economic Security Intelligence Directorate (ESID)

A well-coordinated and focused organizational government body within the Tanzania Intelligence and Security Service (TISS) is needed in order to have the proposed intelligence framework successfully implemented. This article suggests a creation of Economic Security Intelligence Directorate (ESID), where there is a certain hierarchy of responsibilities, and the structure is established clearly. The suggested structure will make sure that there are distinct authority, accountability and operational efficiency lines.

Organizational Hierarchy

ESID would be based in the operation branch of TISS and report to the Deputy Director General (Operations). This would make the economic intelligence completely integrated into the wider national security apparatus and there would be a proper chain of command on how economic intelligence activities can be conducted. The suggested hierarchy will be presented in the following organizational chart:

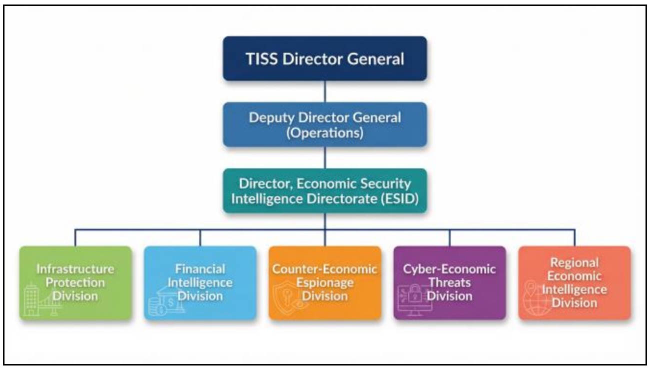

Fig 6: Organizational Structure of the Economic Security Intelligence Directorate (ESID)

Divisional Responsibilities

It would be divided into five expert divisions, each with its mandate and field of specialization:

1. **Infrastructure Protection Division:** This division would handle the evaluation and mitigation of the threat to the critical economic infrastructure in Tanzania, such as Standard Gauge Railway, port facilities, energy infrastructure, and special economic zones. It would carry out routine security checks, liaise with the operators of infrastructure and give early notification of any possible threat.

2. **Financial Intelligence Division:** This department would collaborate with the Financial Intelligence Unit (FIU) based at the bank of Tanzania with the aim of detecting and investigating money laundering, illicit financial flows, and other financial offenses that may be a threat to the economic safety of the country. It would as well support the Prevention and Combating Corruption Bureau (PCCB) in its anti-corruption campaigns.

3. **Counter-Economic Espionage Division:** This department would ensure that there is protection of the strategic sectors in the country against foreign economic spies and industrial espies. It would perform counter-intelligence activities, screen foreign technical staffs, keep up on suspicious technology shipments and secure research institutions and intellectual property.

4. **Cyber-Economic Threats Division:** This department would work on ensuring that the cyber-attacks of infrastructure and financial systems in Tanzania are mitigated. It would build cyber threat intelligence, track key systems in real-time, and coordinate cybersecurity-related issues with the private sector.

5. **Regional Economic Intelligence Division:** This division would be tasked with the responsibility of tracking economic threats in and out of the East African region and the rest of the world such as transnational organized crime, regional economic wars, and transnational illicit activities. It would also liaise with local intelligence services and global partners.

Such a proposed structure would give TISS the field-specific abilities and the organizational focus necessary to respond effectively to the dynamic and changing issues of economic security. The distinct separation of work between the five divisions would guarantee that all the critical threats are addressed, whereas the hierarchical design would ensure the efficient command and control. Introduction of ESID will take a major step towards development of a world economic intelligence capacity in Tanzania and such an introduction would send a strong message to the world that the country is keen about safeguarding its future in terms of the economy.

References

1. The White House. National Security Strategy. Washington (DC): The White House, 2025.
2. Office of the Director of National Intelligence,2023 National Intelligence Strategy. Washington (DC): Office of the Director of National Intelligence, 2023.
3. Muzinich JG, Raimondo GM, Taiclet JD. U.S. Economic Security: Winning the Race for Tomorrow's Technologies. Independent Task Force Report No. 83. New York: Council on Foreign Relations, 2025.
4. European Commission. Joint Communication on a European Economic Security Strategy. JOIN(2025) 20 final. Brussels, 2025.
5. Shagina M. Supply-chain resilience: the foundation of economic security. International Institute for Strategic Studies (IISS) [Internet], 2025. [cited 2026 Jan 8]. Available from: https://www.iiss.org/online-analysis/online-analysis/2025/12/supply-chain-resilience-the-foundation-of-economic-security/
6. Central Intelligence Agency. A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Washington (DC): Central Intelligence Agency, 2009.
7. The United Republic of Tanzania. The Tanzania Development Vision 2050. Dodoma: Planning Commission, 2025.
8. The Parliament of Tanzania. The Tanzania Intelligence and Security Service Act, 1996. Act No. 15 of 1996.
9. The Parliament of Tanzania. The Tanzania Intelligence and Security Service (Amendment) Act, 2023. Act No,2 of 2023.
10. Global Financial Integrity. Illicit Financial Flows Risks Related to Beneficial Ownership in the Mining Sector in Tanzania. Washington (DC): Global Financial Integrity, 2025.
11. The United Republic of Tanzania. Tanzanian Government Cyber Security Strategy 2022–2027. Dodoma: Ministry of Information, Communication and Information Technology, 2022.
12. Jamestown Foundation. Tanzania faces looming threats from East African jihadist turmoil. Terrorism Monitor [Internet], 2023, 21(15). [cited 2026 Jan 8]. Available from: https://jamestown.org/tanzania-faces-looming-threats-from-east-african-jihadist-turmoil/
13. East African Community. Peace & security [Internet]. [cited 2026 Jan 8]. Available from: https://www.eac.int/security
14. Center for Strategic and International Studies. Survey of Chinese espionage in the United States since, 2000. [Internet]. [cited 2026 Jan 8]. Available from: https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000
15. Center for Development of Security Excellence. Jiaqiang Xu – economic espionage [Internet]. [cited 2026 Jan 8]. Available from: https://www.cdse.edu/Portals/124/Documents/casestudies/jiaqiang-xu-economic-espionage.pdf
16. UPDF. EAC defence intelligence chiefs pledge stronger regional security cooperation [Internet]. [cited 2026 Jan 8]. Available from: https://www.updf.go.ug/regional-security/eac-defence-intelligence-chiefs-pledge-stronger-regional-security-cooperation/
17. Cline LE. African regional intelligence cooperation: problems and prospects. Int J Intelligence CounterIntelligence,2016:29(2):225–244.