A SECURITY ASSESSMENT OF SRI LANKA THROUGH INTELLIGENCE SHARING

Hirantha Sandalu Wijesinghe

Published on Sri Lanka Military Academy Journal in December 2021

ABSTRACT

Three decades of brutal terrorism and ethnic violence which crippled Sri Lanka's economy and social structure ended in the year 2009. However, a decade of peace was shattered withthe Easter Sunday attacks conducted by a religious extremist group in 2019. In the changing security context of Sri Lanka, we can foresee ethnic separatism and religious extremism being a significant security threat in the future.In order to counter these challenges and threats, a strong national security policy is deemed a prerequisite."Intelligence" is a crucial component in strengthening the national security of a nation and intelligence sharing is a very important component as it is the first step to prevent a terrorist attack. This encourages the military and law enforcement agencies to establish a system of intelligence sharing among the intelligence community and enhance public participation in countering terrorism measures.

This article outlines stages that will establish models which may be used as a template for statewide sharing of information and intelligence in Sri Lanka. It addresses two proposals: the development of a Terrorism Early Warning (TEW) Group and establishment of a statewide Intelligence Sharing Centre (ISC). The idea is that through effective intelligence sharing, law enforcement agencies in Sri Lanka will be able to better protect citizens' safety and, as a result, aid in terrorist prevention efforts. This study is based on qualitative data derived from secondary sources; reputed books, online journals, media reports, and existing literature. Moreover, this research which focuses on intelligence sharing includes both academic and policy implications.

Keywords –National Security, Countering Terrorism, Intelligence Sharing, Terrorist Early Warning

INTRODUCTION

According to Tzu (2002), terrorism has become a greater threat to world peace and some countries find it difficult to manage due to the destructive actions of these terrorist groups. In order to counter those challenges and threats, a strong National Security policy was deemed a prerequisite.For Sri Lanka to be secure, the policy should focus on all levels of the National Security Complex and sectors, giving special emphasis to ethnic group levels. Due to recent unresolved communal violence in Sri Lanka, some radical extremists and ultra nationalists have been encouraged to form groups resorting to violence by marginalizing moderates of the same religion or ethnicity. History has shown that the tensions are at that level due to fear of extinction and survival by ethnic groups in Sri Lanka which should be erased through a solid policy (Perera, 2020). This demands the government to establish a system of countering such threats by introducing several models to strengthen the nation security apparatus in Sri Lanka.

Information sharing is very important as it is the first step to prevent a terrorist attack (Travers, 2021). Shared information can improve the quality of investigations as there could be vital information or a missing piece. This encourages the military and law enforcement agencies to establish a system of intelligence sharing among the intelligence community and enhance public participation in countering terrorism measures. We live in a time when aggressive types of crime, organized and multinational crime, but also imported and domestic terrorism and insurrection, have a significant impact on the national security. Accurate intelligence and emergency management processes are more vital than ever in this context and national intelligence and response systems must adapt to new challenges.To combat terrorism effectively, the military must work closely with their communities and among themselves. They must develop new techniques and collaborate with new people. This necessitates a high level of comprehension: of the threat, of communities, of analytical methods, and intelligence.

The objective of this article is to outline stages that will establish models which may be used as a template for statewide sharing of information in Sri Lanka. And provide necessary recommendations on a comprehensive framework to counter possible terrorist attacks by establishing a data-sharing network among different levels of security in the country.The idea is that through effective intelligence sharing, military and the law enforcement agencies in Sri

Lanka will be able to better protect citizens' safety and, as a result, aid in terrorist prevention efforts. This article looks into a variety of options for assisting Sri Lanka in preventing possible terrorist attacks by establishing a data-sharing network among different levels of security in the country. It will also determine an appropriate way for developing a statewide information-sharing plan and outline the particular actions required to construct an Intelligence Sharing Center (ISC). Specific solutions based on research, case studies, and best practices from throughout the country will be found, putting Sri Lanka at the forefront of terrorism prevention through intelligence sharing.

LITERATURE REVIEW

According to Travers (2021), information sharing is crucial as it is the first step to preventing a terrorist attack and central coordination is one of the most important disciplines in intelligence. However, the most common problem that exists in today's intelligence community is the lack of intelligence sharing (Field, 2009). Richard (2011) states that many countries do not have such a system for sharing intelligence gathered by different agencies at the lower levels and the absence of intelligence sharing limits their ability to prevent terrorist attacks or to have an early warning. The culture of most intelligence agencies is that they operate systems of their own that are unable to exchange information among different agencies (Hamrah, 2013).

According to Zegart (2006), inability to exchange intelligence has resulted in many intelligence failures in preventing terrorism. If the intelligence or information cannot be shared in real-time, it makes it less likely to prevent terrorist activities. And Turner (2005), emphasized that a shared database for information collection and information sharing by a range of technologies is much needed in preventing terrorism in the current context. In the state security apparatus, different intelligence agencies gather valuable information and investigate different cases regularly (Federation of American Scientists, 1996). This information is only evaluated together at the higher levels of the government structure. The higher intelligence officials will have to focus on other nations or non-state actors, detect threats and stop them while maintaining firm intelligence efforts within the state and society at the same time. Most agencies around the world gather information in their silos and do not have any idea of what sort of information other agencies may have found on the same case, or a different person, or an incident that may have a link to the

same case (Zegart, 2006). Existence of a central hub to have access to such information is very important as such network can help the intelligence community to connect the dots in processing and analyzing information (Travers, 2021). The central issue is the absence of such information-sharing network that permits intelligence agencies and law enforcement to gain access to the information in the lower circles of the security structures.

As we know, terrorist financial networks have become a key component in the evolution of terrorist groups and terrorist activities. Without financing, they are unable to conduct their activities, and terrorists are involved in many illegal ways of raising funds for their cause (Warner, 2002). Such activities include drug trafficking, money laundering, theft, smuggling, human trafficking, etc. As we see here, mainly law enforcement agencies are involved in countering such activities. On the other hand, different agencies like the Navy, Coast Guard, customs, and border security agencies are involved. Many different agencies are involved in the process and there should be an information-sharing mechanism as these kinds of activities may have a direct link to terrorism funding. Some of these agencies do not have personnel dedicated to intelligence functions. Officers in these smaller, local agencies interact with the community daily, but they now lack the tools and resources required to generate, gather, access, receive, and share intelligence information.

It's a common belief among the intelligence agencies that the culture should change from "need to know" to "need to share"(Gordon, 2017). Different agencies have a lot of information, but only a limited amount of information is being shared. In recent history, we have seen tragic events that happened due to failures in exchanging information. And the 9/11 attacks can be taken as one of the best examples, as US agencies failed to connect the dots which may have helped them in preventing such incidents (Travers, 2021).

Collins (2019) states that in order to have a successful statewide intelligence-sharing network, members of these different agencies must work together collectively with law enforcement agencies as well as defence agencies on a shared vision. Key considerations are the creation, funding, comprehensive and detailed strategy, and tactical plan while tackling several technological and policy difficulties. A state must accommodate the different information systems already in place to successfully integrate all stakeholders, and solutions must address a

wide range of information privacy and system security concerns. Compliance with state intelligence act regulations and privacy laws, on the other hand, will be a significant challenge for information sharing (Gordon, 2017).

Since 09/11 in United States, federal, state, and local governments have implemented programs to increase information sharing in order to prevent terrorism. Bajll (2009) insist that many of these projects were launched by states and communities, and they were not always coordinated with other sharing initiatives, including those implemented by federal agencies. At the same time, the Department of Homeland Security (DHS) was working on programs to improve information sharing (Bajll, 2009). Lt. John Sullivan of the Los Angeles County Sheriff's Department is widely regarded as one of the country's foremost authorities on the sharing of information through the use of terrorist early warning centers (Davis et al. 2010). According to Sullivan, the efficient and timely transmission of indications and warnings to local emergency response agencies is a critical yet challenging component of the United States' terrorist management operations (Pherson & Sullivan, 2013). Fusion centers, which are joint efforts to integrate and analyze anti-terrorist information from diverse sources, have grown in popularity as part of homeland security and overarching counterterrorism tactics. Several states, including Arizona, Colorado, Illinois, Kansas, Maryland, Massachusetts, and New York, presently run so-called fusion centers, and several others, including Missouri, are contemplating doing so (Pherson & Sullivan, 2013). The statewide fusion center will function as a focal point for information collecting, fusion, and distribution.

In intelligence, several intelligence disciplines are used by the military to acquire information. These disciplines are broadly categorized into human intelligence (HUMINT), open-source intelligence (OSINT), and technical intelligence (TECINT). Lohman (1989) insists that out of the above human intelligence is the most important and the most valuable intelligence function. It is very accurate and timely. Human intelligence is received through interpersonal contracts built on trust. Most nations, and many private organizations, have HUMINT capabilities that they use to collect data on their adversaries and competitors. HUMINT plays an integral, if not an indispensable role within the intelligence and national security arenas. Whether it is against traditional nation-state adversaries or newer and more pronounced threats, such as terrorist or insurgency networks, or the more esoteric, like cybersecurity, the human factor remains a

dominant force (Thompson, 2016). Intelligence should come from the human being. To do that, the military needs to create an environment including the civilians. Therefore, before creating an information highway, trust must be built between the military and the civilians. This strategy is known as interdependency. According to Tzu (2002), developing local civil defense protocols, is critical to state survival. Shared information from the community or can improve the quality of investigations as there could be vital information or a missing piece. According to Pherson & Sullivan (2013), a single piece of information that comes from the community can play a bigger role since day-to-day activities that happen in society may have a connection to a terrorist network. Travers (2021) also states that, there had been many failures to happen due to the inability to connect these dots with different pieces of information gathered from the community. Dealing with currency, smuggling, money laundering, drug trafficking may have direct connections with terrorism as they may be funding sources for terrorist activities.

The Los Angeles TEW analyzes trends and identifies risks that might lead to terrorist acts in the country. Members of the TEW review media stories, information from various federal, state, and local authorities, and other open-source material to establish the reliability of the information (Pherson & Sullivan, 2013). The TEW identifies terrorist precursor events as part of its evaluation so that preventative and mitigation steps can be performed. Pherson & Sullivan (2013) also states that, in a crisis, the TEW's purpose is to offer intelligence and assistance to incident commanders, as well as provide suggestions that aid in decision making. The Los Angeles model also includes a Terrorism Liaison Officer (TLO) to help with information exchange. The TEW can interact effectively and efficiently thanks to its network of Terrorism Liaison Officers (Monahan&Palmer, 2009). In order to assist such an attempt, a TEW must interact with a fusion center at the state level. Fusion centers exemplify the idea of teamwork. Collaboration enables organizations to make the most of their existing resources and work together toward a common objective. Centers should prepare for future connections utilizing existing technology while adhering to specific requirements.

METHODOLOGY

This study is based on qualitative data derived from firsthand accounts and secondary sources from reputed books, online journals, media reports, existing literature, and academic research on

this wider topic. This paper empirically analyses the exiting intelligence-sharing mechanisms and how civilians are involved in the intelligence process. The objective of this article is to outline stages that will establish models which may be used as a template for statewide sharing of information in Sri Lanka. And provide necessary recommendations on a comprehensive framework to counter possible terrorist attacks by establishing a data-sharing network among different levels of security in the country.

DISCUSSION AND OUTCOMES

This article addresses two proposals: the development of a Terrorism Early Warning (TEW) Group and the establishment of a statewide Intelligence Sharing Centre (ISC). Sri Lanka would be able to work proactively and uniformly in the prevention and deterrence of terrorism if this capability was built. A TEW in an urban region will not entirely improve statewide information exchange capabilities. Only a statewide central hub like ISC could broadcast information across the entire state.

1. The Terrorist Early Warning Group (TEW)

Gordon (2017) insists that the military must be able to gather, process, evaluate, and disseminate intelligence on potential causes of civil unrest and use that knowledge to change the operating environment. To do so, a new way of thinking about intelligence and early warning is required, one that relies on the best of law enforcement and military techniques while also drawing on the knowledge and insight of religious leaders, retired military officers, scientific communities, academia, and social workers. The concept of TEW Group is the main suggestion we would like to make for Sri Lankan defence and law enforcement authorities to get the community involved in achieving the National Security Strategy of Sri Lanka. The TEW group is a well-structured entity that operates in an organized manner with more authority. The TEW group should be created and strengthened to reposition the agenda for state intelligence. We suggest that every town and village must have a civilian intelligence unit to be coordinated by the intelligence agencies. This will provide reliable intelligence and early warnings against terrorist threats, if well-arranged and organized.

During the 30 years of the ethnic crisis in Sri Lanka, the Sri Lankan military received support from the local communities, and their contributions to the military's successes were remarkable. However, with the emergence of religious extremism, the strategy for forming the TEW groups has to be revamped and new strategies have to be put in place. The nature of modern terrorism has taken the fields of combat too close and its asymmetrical nature makes predictability difficult, if not impossible. Members of the TEW groups are able to provide reliable intelligence as representatives of the same area as the terrorists, providing information about particular individuals or groups, suspicious activities, changes in the religious ideologies, potential attacks, which makes it easier for the military to analyze from the root level to conduct proactive operations. Another advantage of initiating this is that these civil members are locals who know the culture of the area in which they live, and they are fully aware of the evolution of fundamentalism, radicalization, and extremism that lead to terrorism. This initiative brings intelligence to the local community from the high levels of governmental circles. Also, the state must strengthen this and expand their intelligence to the higher level and the bottom if early signs of terrorist threats can be detected and avoided. The higher intelligence officials will have to focus on other nations or non-state actors, detect threats and respond to them while maintaining firm intelligence efforts within the state and society at the same time.

Moreover, the value of information received from the local community in countering terrorism also serves as a call for thought as to why terrorists act in the way they do. Reflecting on such themes could lead to the discovery that we wouldn't be able to explain terrorism until one can completely empathize with the pain and the frustration that cause it (Stern, 2003). Gaining a better understanding of these facts could lead to appropriate actions towards fighting terrorism. The TEW group will have the capacity to provide the military with valuable information that will help them to prevent terrorism at the base level itself. Hence, this can become the human intelligence scheme applied to fighting terrorism, ensuring the security of the community as well as the state.

The TEW Group is responsible for gathering information related to any existing or perceived threats and acting as a civil intelligence unit, those who receive information from the local communities. This team may include religious leaders, retired military officers, intellectuals, and representatives from youth and social welfare organizations within the community. These groups

engage in social activities, and this enables the TEW group to identify the changes happening within society. It enables the military to obtain an early warning of any potential threat. The TEW group, which consists of different sectors of the community, can contribute in different ways to achieving the national security objectives. Their contribution may be to identify the evolution of religious ideology, provide leadership to the TEW group, coordination with the military, think tanks, knowledge of traditional and non-traditional security, creating awareness, etc. The information should be evaluated within this group before disseminating it to the authorities. Proper training and awareness programmes such as Terrorism Awareness and First Responder training should be provided to the TEW groups frequently by the military. Furthermore, in addition to terrorist threats, this group should be involved in finding other threats such as drugs and other criminal activities within their areas. Social and economic problems also need to be addressed, because these are factors that motivate vulnerable individuals to engage in terrorist activities. The TEW group should be able to identify the preconditions of terrorism in areas in which they live and monitor radical political, religious, and racial activities. The TEW group should have proper coordination and integration with the military. Collected and disseminated information should be properly stored in a secured database.

Recruitment of the members of the TEW group should be conducted under the direct supervision of the intelligence agencies with coordination of the area law enforcement agencies. Proper recruitment and selection need to take place in order to ensure the effectiveness of operations. Moreover, the loyalty of members of this group is very important as the security of the information has to be ensured and the information shared in real-time. However, it is the responsibility of the intelligence community to verify the information received by the TEW group. Processing and analyzing the information and the dissemination have to be done in an effective manner for maximum utilization of the information received from the TEW. Furthermore, it is the responsibility of the military to provide feedback to the TEW group which they receive from the security authorities from a higher level.

Prior to Easter Sunday attack, the traditional Muslim community was able to provide reasonable information regarding this extremist group and its development. Months before the bombings, Mohamed Razik Mohamed Taslim, a Muslim social worker from Mawanella, had been at the forefront of efforts to investigate the extremists. Taslim's story encapsulates both how the

country's Muslim community actively tried to stop the emergence of radical elements in their midst, and how the authorities failed to recognize repeated warning signs ahead of the Easter Sunday attacks (BBC, 2019). His information and coordination with the Criminal Investigation Department led to the raid in Wanathavilluwa, Puttalam, where a large number of explosives and chemicals were found. Moreover, a Muslim religious leader, Mufti Mohammed Rizwi, who testified before the select committee looking into the Easter Sunday attacks, said he had warned the defence authorities about the National ThawheedJama'ath in November 2012 (Daily Mirror, 2019). Therefore, the information from this community is very important to combat extremism by obtaining information about the threat from extremists within their community.

2. **The Intelligence Sharing Centre (ISC)**

The concept of an Intelligence Sharing Center can be established in Sri Lanka as the primary and major information and intelligence dissemination center of the State among emergency agencies. The Intelligence Sharing Center will be an interface for all key IT systems to ensure seamless flows of information across disciplines. These Intelligence Sharing Centers can be established in every district of the country and will also be interlinked with state-level intelligence agencies.

Countering terrorism and religious extremism play a significant task in the national interest of Sri Lanka. More than 20 million people live in the country, which spans over 65,000 square kilometers and is home to communities from different ethnic, religious, and cultural groups. Sri Lanka's response to multiple crises demonstrates the necessity for more comprehensive coordination and planning, as well as the development of a system for measuring the amount and type of response to an occurrence. Defence and law enforcement authorities and emergency services across the country needed to work together to monitor intelligence, identify trends, and mount a response. Simple collaboration agreements are insufficient to face these threats. Responding to every threat at maximal reaction levels had become prohibitively expensive. Even if such intelligence existed, there was no way to ensure that it reached all individuals on the response team.

As a local solution, this study suggest the formation of a district-level ISC to develop a district-wide group capable of a highly coordinated and concentrated response to terrorist attacks, based

on meticulous analysis of information and intelligence and detailed planning.. This information will be shared among different intelligence agencies as well as state-level intelligence authorities. ISC is an actual physical location with dedicated staff who will gather information, analyze, process it, and disseminate it to the relevant agencies. ISCs are staffed by intelligence officers from defence and law enforcement authorities. Members from different agencies will work in the same centre.

The ISC's mission is to analyze the strategic and operational intelligence needed to respond to and counter terrorism, as well as protect the communities of their territory. The ISC can keep track of trends and analyze threats in the respective areas that could lead to terrorist attacks. Members of the ISC assess media reports, information from the TEW groups, information from the state level intelligence agencies, municipal agencies, and other open-source data to determine the accuracy of the information. The ISC identifies terrorism precursor events as part of its assessment so that prevention and mitigation steps can be made.

The ISC also defines processes for identifying and distinguishing credible threats that necessitate a reaction, as well as determining the appropriate level of response. This also saves resources when responding because more comprehensive information is available for launching an appropriate degree of response rather than sending a full scale response. State-level intelligence authorities can collaborate with a wide range of partners to counter violent extremism, including these ISCs and the TEW groups. Through their everyday operations, which include receiving, analyzing, and sharing threat information, ISCs play an essential role in fighting violent extremism and protecting local communities. ISC's, as data analysis hubs, are important in helping frontline personnel know the local consequences of national intelligence by adapting national security threat information into a local context and assisting frontline personnel in understanding terrorist and criminal threats they may encounter in the field. ISC’s also report threats and difficulties they encounter in their areas to the state-level authorities, which allows the authorities to better support local initiatives.

Study recommends the following as the main mission focus of ISC:

- Establishing grassroot level intelligence and analytic capabilities in the local environment so that the local community can understand the importance of national intelligence by customizing national threat information into a local context.

- Delivering timely, comprehensive, and reliable threat analyses to state and local partners, including:

    - Identified weaknesses in the area, as well as trends or patterns in criminal and terrorist operations.
    - Terrorism, signs of violence and early warning
    - How to report suspicious activity to the appropriate law enforcement officials.
    - Other danger mitigation efforts, such as preventive measures or preventive acts, are also recommended.

- Sharing information with state level decision-makers to aid in resource prioritization in the face of identified threats.

- Providing intelligence with the TEW groups and local partners to assist frontline staff in their community engagement initiatives, such as raising awareness of potential dangers in their neighborhoods.

- Conducting programs to facilitate information flow between the ISC and the TEW groups as a strategy for forming partnerships between both entities.

Intelligence sharing between different intelligence agencies and the TEW groups is enabled through the ISC. This type of network allows law enforcement intelligence units to share information with the military intelligence community while allowing the latter to share information with local law enforcement, and vice versa. As a result of ISC, different intelligence agencies who work at different levels can share information. If further developed, ISC can be awell-prepared entity that will detect potential sources of attacks, offer courses of action, and provide ongoing intelligence support and technical assistance to the military because of its expertise with this large store of information.

Furthermore, there are several technical requirements when establishing an intelligence-sharing network. State-wide IT systems need to be developed, and such systems should have the ability to query and retrieve information from relevant information systems of other relevant intelligence and government agencies. ISC should have the capacity to electronically pass on the information and digital records from one agency's information systems to another agency's information systems. Also, networking is very important and members of ISC should get notifications on critical events, actions, and transactions on a case, person, or event. When investigations are being conducted, ISC members should have the ability to discover agencies that have information concerning a specified individual; to ascertain or confirm the identity of an individual and link identity to documents, decisions, and other official actions and the current legal status of an individual.

Moreover, Artificial Intelligence (AI) is expected to be particularly useful in intelligence due to the large data sets available for analysis. In this capacity, AI is intended to automate the work of human analysts who currently spend hours sifting through drone footage for actionable information, potentially freeing analysts to make more efficient and timely decisions based on the data (Gonzales et al., 2014). According to Morgan et al. (2020), the Central Intelligence Agency alone has around 140 projects in development that leverage AI in some capacity to accomplish tasks such as image recognition and predictive analytics.

Sharing information can disrupt, deter, or lessen an act of terrorism or a simple criminal activity, which is the most basic measure the government can do to safeguard its citizens. A state must make every effort to assist law enforcement officers with more detailed information about prospective suspects or incidents. Providing statewide access to the multiple criminal justice databases with hundreds of thousands of accused aliases and case information is a crucial step towards protecting the public from potential threats of terrorism.

CONCLUSION

No doubt that the information obtained from civil society or human intelligence is more essential than it was necessary to introduce policies to deal with the most important part of countering terrorism. The main role of intelligence is to assist the leadership of the state in statecraft and

human intelligence plays a vital role in it. However, controlling the quality of the intelligence received by the community is a very challenging task and trickier than the other means of collecting information. So, the military must be cautious when processing human information into intelligence as outcomes are not determined with mathematical precision. According to Tzu, "just as water, which carries a boat from bank to bank, can also be the means of sinking it, so reliance on human intelligence, while producing great results, is frequently the cause of utter disaster."

The intelligence community needs to improve its capabilities for domestic intelligence. It is recommended that the information be supported in a real-time manner by local and state agencies. The weakness in terrorist prevention is a failure of present operating systems to correctly gather, evaluate and disseminate information and access to databases. Using current technology and statewide intelligence-sharing networks, information exchange may significantly lower the risk of terrorism. Implementing an information-sharing enterprise could potentially assist defence and law enforcement authorities to avert a terrorist attack by compiling information from many sources and delivering that intelligence to the appropriate public safety personnel. This guideline or model could be utilized as a template for national information sharing by existing policies and strategy options.

Defence and law enforcement agencies should continue to encourage the implementation of these systems while developing an information exchange plan, which will improve functionality and serve even more responsibilities. In order to meet the needs and requests of the intelligence community and other stakeholders, the policy recommendation expands the network for information exchange. The statewide Intelligence Sharing Center will function in the background to support all intelligence and information exchange in the state, with a major emphasis on national defence challenges. When necessary, intelligence will be shared across disciplines through the systems of the Intelligence Sharing Center. Moreover, there must be a consistent and systematic set of measures in place to assess the success and/or failure of ISCsFuture studies should examine the existing military intelligence paradigm and present notion of information sharingin Sri Lanka, as well as whether or not the country's existing systems of public participation in sharing of intelligence have been successful. Further research on logistical and technological arrangements for an effective intelligence sharing mechanism has to be conducted.

Hirantha Sandalu Wijesinghe serves as an Intern (Research) at the Institute of National Security Studies (INSS), the premier think tank on National Security established under the Ministry of Defence. The opinion expressed is his own and not necessarily reflective of the institute.

REFERENCES

Bajll, M. A. (2009). Homeland Security Intelligence: Regional Fusion Centers. American Intelligence Journal, 27(1), 61–66.

Ballast, J. (2017). (Rep.). NATO Defense College.

Collins, A., (2007). Contemporary security studies. Oxford: Oxford University Press.

Davis, L. M., Pollard, M., Ward, K., Wilson, J. M., Varda, D. M., Hansell, L., & Steinberg, P. (2010). The Evolution of Fusion Centers and Information-Sharing. In Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security (pp. 39–58).

Federation of American Scientist (1996). The Evolution of the U.S. Intelligence Community-An Historical Overview.

Field, A. (2009). Tracking terrorist networks: Problems of intelligence sharing within the UK intelligence community. Review of International Studies (4), 997-1009.

Gonzales, D., Harting, S., Mastbaum, J. and Wong, C. (2014). Improving Interagency Information Sharing Using Technology Demonstrations: The Legal Basis for Using New Sensor Technologies for Counterdrug Operations Along the U.S. Border.

Gordon, J. (2017). Intelligence sharing in NATO. AtlantischPerspectief, (6), 15-19.

Hamrah, S. (2013). The Role of Culture in Intelligence Reform. Journal of Strategic Security, 6(3Suppl), 160–171.

Lohman, D. (1989). Human Intelligence: An Introduction to Advances in Theory and Research. Review of Educational Research, 59(4), 333-373. doi:10.2307/1170203

Monahan, T., &palmer, N. A. (2009). The Emerging Politics of DHS Fusion Centers. *Security Dialogue*, *40*(6), 617–636. http://www.jstor.org/stable/26299838

Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020, April 28). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World.

Perera, M. G., 2020. Futuristic National Security Policy for Sri Lanka to Attain Vistas of Prosperity and Splender. Diplomacy & World Affairs, 2(2), p. 20.

Pherson, K. H., & Sullivan, R. A. (2013). Improving the Quality of Analysis in Fusion Centers: Making the Most of the Nation's Investment. Journal of Strategic Security, 6(3), 309–319.

Richard. B. A. (2011). Intelligence Information: Need-to-Know vs. Need-to-Share. Congressional Research Service.

Stern, J.(2003).Terror in the Name of God.Ecco New York

Thompson, L. D. (2016, July 28). Intelligence Collection and Information Sharing within the United States. Brookings. https://www.brookings.edu/testimonies/intelligence-collection-and-information-sharing-within-the-united-states/

Travers, R., (2021). Information Sharing, Dot Connecting, and Intelligence Failures: Revisiting Conventional Wisdom. [online] Homeland Security Digital Library.

Turner, M. (2005). Why secret intelligence fails. Washington D.C.: Potomac.

Tzu, S. translated by Minford, J. (2002). The art of war. New York: Viking

Warner, M, (2002) Wanted a definition of intelligence studies, in (ed) Intelligence", 46, Retrived May 6 2010 from http// www. homeland security. org/journal/articles/Marrin html

Zegart, A. (2006). An Empirical Analysis of Failed Intelligence Reforms before September 11.Political Science Quarterly,(1), 33-60.