Understanding the Intelligence Failure and Information Sharing in Handling Terrorism among Intelligence Community

Syariffah Nur Qasyfi Syed Mohamed, Mohammed Yaacob

Understanding the Intelligence Failure and Information Sharing in Handling Terrorism among Intelligence Community

Syariffah Nur Qasyfi Syed Mohamed, Mohammed Yaacob

Centre of Media Information and Warfare Studies, Universiti Teknologi MARA
40450 Shah Alam, Selangor, Malaysia.

Abstract
Information sharing in intelligence cycle has become a crucial subject in security field. The main objective of this paper is to understand the information sharing and intelligence failure in handling terrorism among the intelligence community. The role of intelligence community is to obtain information, analyses, and process the information for their clients. However, the terrorist attacks still occur resulting from intelligence cycle. Realizing information sharing in intelligence cycle requires efforts from the community.
Keywords: Information Sharing, Intelligence Cycle, Communication, Security, Management.

Introduction
Information sharing in intelligence cycle had been debated for being beneficial or damaging the intelligence cycle. Intelligence cycle is the process of intelligence involving five steps of cycle which is planning, collecting, processing, analyzing and dissemination. Intelligence community strained themselves from sharing information at any steps of the cycle as they still intact with the "need to know" practice. Literature has suggested that in the practice of intelligence cycle might be differ from each department but none to include the information sharing. Agencies tend to hide information and treat them as confidential and important to be kept only for their knowledge. The importance of information sharing has become crucial among law enforcement's departments especially in handling terrorism since the 9/11 Attack in 2001.
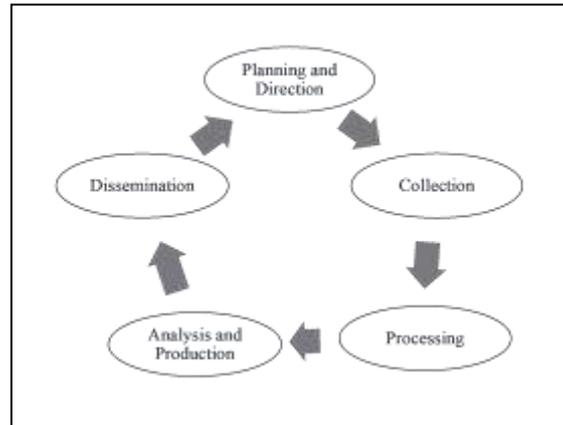
Figure 1. Intelligence Cycle

Intelligence Community

Intelligence community existed because of needs and demands, specifically from the government, organizations, and agencies such as policymakers, decision makers, and war fighters. Intelligence community act as another platform to gain and give whatever information that they receive and report it to the organizations that require the information. Literature suggests that intelligence community obtain data and follow the procedure exactly as how intelligent cycle functions. Intelligence community has been established quite sometimes ago, however the functions of this community has been enhanced when 9/11 attack happened in 2001 due to lack of information and miscommunication in U.S intelligence and operational team in countering terrorism (Lederman, 2004). The roles of community intelligence are to obtain information, analyses, and process the information for their clients such as National Security Agency (NSA), Defense Security Agency (DSA), Prime Minister Office and many more. The reason why intelligence community has been given the mandate to collect and analyses the data by government or agencies because it is to ensure the security of a particular country. As for example, in Canada, CSIS or Canadian Security Intelligence Service was formed in 1984 because the community is responsible to counter espionage and sabotage, foreign-influenced activities, terrorism, and subversion (Vitkauskas, 1997).

Practice of intelligence in Malaysia carried out by different agencies. Malaysian Special Branch, Defense Staff Intelligence Division, Royal Intelligence Corps (Kor Risik DiRaja), Military intelligence (MIO), Malaysian Armed Forces, Research Division of the Prime Minister's Department (Malaysian External Intelligence Organization) and Chief Government Security Office (CGSO). When talking about the intelligence in Malaysia, the first thing to pop-up in mind is the Special Branch (SB), Royal Malaysian Police (RMP). According to the Police Act, 1967 (Act 344) Section 3 (3), "the Force shall subject to this Act be employed in and throughout Malaysia (including the territorial waters thereof) for the maintenance of law and order, the preservation of the peace and security of Malaysia, the prevention and detection of crime, the apprehension and prosecution of offenders and the collection of security intelligence". While in the Armed Forces Act, 1972 (Act 77) Section 41 (3) described intelligence as "information which is or purports to be information as to any matter such that information about it would or might be directly or indirectly useful to the enemy, and in particular (but without prejudice to the generality of the foregoing provisions) as to any

matter falling within the following paragraphs, being a matter such that information as to it would or might be useful as aforesaid, that is to say;

i.   the number, description, armament, equipment, disposition, movement or condition of any of His Majesty's armed forces or of any forces co-operating therewith or any of His Majesty's ships or aircraft or of the ships or aircraft of any such co-operating force;

ii. any operations or projected operations of any of such forces, ships or aircraft as aforesaid;

iii. any code, cipher, call sign, password or countersign;

iv. any measures for the defense or fortification of any place on behalf of His Majesty;

v.   the number, description or location of any prisoners of war;

vi. munitions of war".

In earlier record of intelligence in Malaysia, Communist Party of Malaya (CPM) has been a threat since 1948 (by that time Malaysia is known as Malaya). On 22 January 1952, Sir Gerald Templar was appointed as the British High Commissioner in Malaya to face the issue of Malaysia Emergency or the communist attack. Sir Gerald Templar however use different initiatives from any commissioners before him. For the first time in history the intelligence force to gather the information on communist was establish. Sir Gerald Templar put on efforts in intelligence. His works come into success as the communist begin to draw back (Paidi, Hj, & Ghani, 1960). In 1960, Malaysia Security Forces defeated Communist Party Malaya (CPM) but they took their chance by reviving their struggle and urged the Second Malaysia Emergency in 1968. For almost 40 years Communist Party Malaya (CPM) widespread all over the country (Mohamad Yasid, 2016). The effective implementation of intelligence services by the Royal Malaysian Police Special Branch (SB) Division led to the setback of Communist Party Malaya (CPM) in 1989 (Mohamad Yasid, 2016). Malaysian Special Branch, Defence Staff Intelligence Division, Royal Intelligence Corps (Kor Risik DiRaja), Military intelligence, Malaysian Armed Forces carried the task of intelligence in Malaysian Law Enforcement Agencies. However, other agencies such as Research Division of the Prime Minister's Department (Malaysian External Intelligence Organization), National Security Council (NSC), National Civics Bureau (NCB) and Chief Government Security Office (CGSO) governed by the civil departments. National Security Council (NSC) also responsible in collecting intelligence information for the Prime Minister in sense of political interest. National Security Council (NSC) was established on 7 July 1971 as a result of the dis-solution of the National Movement Council (MAGERAN) in the same year. It was the responsibility of the National Movement Council (MAGERAN) to restore the peace of the country while facing the crisis. In this effort, National Movement Council (MAGERAN) responsible for strengthening public safety, national defense and maintaining public order, vital national supplies and services to the citizens. Later all the responsibilities transferred to the new agency, National Security Council (NSC).

The main function of National Security Council (NSC) is to (National Security Council, 2017);

a) Guarding the State Sovereignty and Strategic Interests - Guarding the integrity and sovereignty of maritime, space, cyber and strategic interests of the country by monitoring and controlling those area from threats.

b) Crisis and Disaster Management - National Security Council (NSC) serve as the focal point in handling crisis and disaster inside and outside of the country as it coordinates tasks and increase public awareness. The responsibilities comprising prevention and mitigation, preparedness, response and recovery and reconstruction.

c) Land, Maritime and Air Border Management - Enhance collaborations between neighbouring countries for better understanding through various programs between those countries.

Other agencies also involved in keeping the country free from threats but do not received the credits on intelligence operation as the subject is not their core business. Their functions on intelligence are fewer highlighted and almost none in the literature. Malaysian Maritime Enforcement Agency (MMEA), Royal Malaysian Customs Department (RMCD), Immigration Department of Malaysia (IDM) and Police and Border Security Division (PBSD) among the agencies that involve in securing the country from threats. Malaysian Maritime Enforcement Agency (MMEA) was formally established with the enactment of the Malaysian Maritime Enforcement Agency Act 2004 to eliminate the overlapping functions and jurisdictions of too many agencies involved in the maritime enforcement in Malaysia. Royal Malaysian Customs Department (RMCD) involve in intelligence operations towards enhancing enforcement to disrupt smugglers and misappropriation. Immigration Department of Malaysia (IDM) ensure that foreigners to enter Malaysia obliged to the policies and regulations of the country. Immigration Department of Malaysia (IDM) also responsible for formulating immigration, passport and entry permit policies as well as matters pertaining to border or cross-border documentation. Police and Border Security Division (PBSD) ensure the national security and civil liberty by governing the Policing and Border Security of the country.

Terrorist Attack and Intelligence Failure
Intelligence is a critical subject in defense and security. The intelligence activities not always come to perfections and seldom faced the failures. The flaws in intelligence may come from various factors such as the agents, operations, procedures, lack of sources and equipment breakdown. Gookins (2013) in her article, "The Role of Intelligence in Policy Making" describes that it is the responsibility of the both policy makers and intelligence community in ensuring the right information is collected. In providing the right, precise, definite and authentic intelligence, the policy makers must provide intelligence community with accurate information and orders of what they required. Sometimes the information has been submitted as high value intelligence by the agents but rather valueless to the policy makers and vice versa. Officers or agents on the field collect information based on their experiences and judgements while the executives' branches require information based on the policy needs. The dissimilar situations give different direction for them in collecting and analyzing the information. Some degree of failure is expected from handling the intelligence as it is a risky operation dominates by the uncertainty and ambiguity in providing the useful information to the government (Johnson, 2006). The risk of handling clandestine and high value information is excessive. All agents must prepare and expect the blown of cover while delivering intelligence products. Intelligence operation usually comprises high profile

information and data that require proper attention and always involve with numerous pitfalls. The danger in delivering intelligence not only come from the agents himself or herself but rather the surroundings and enemies advancing the agents. The intelligence cycle itself may also give the effect on delivering intelligence product.

Johnston (2005) defines intelligence failures as imprecisions of facts in analysis because of missing or poor data. Intelligence failure is systemic organizational bombshell resulting from incorrect, missing, useless, or insufficient hypotheses Johnston (2005). Analytical failure is the main root causes to the critical intelligence failure (Folker, 2000). Folker (2000) claims that the most intelligence failure comes at analysis steps as the IC fails to predict the consequences and take actions against intelligence gathered. Folker (2000) in his journal article "Intelligence Analysis in Theatre Joint Intelligence Centres: An Experiment in Applying Structured Methods" described that intelligence failure critically occurs from the analytical errors. The failure of analysing raw data has washout to predict the North Korean invasion in 1950 (Finley, 1994). Finley (1994) conclude that the intelligence failure occurs from the result of;

i. No enough data to target an area.
ii. Too much data that caused misinformation or slow the information flow.
iii. Conflicting data such as reliability of sources, data priority and urgency and human attitude.
iv. The repetition of indicators leads to false alarm and tend to make evaluators to discount signs that appear common.
v. Withheld information from decision makers to protect certain parties.

When intelligence community did not manage to share information, therefore, intelligence failure happened. For example, the incident of a military personnel has brutally shot to death twice has caught the world's attention. This case was a bit different whereby the targeted victim has been chosen wisely and it has been organized properly. Besides, there is no civilians involved in and get hurt, but the attacker's aim is to kill the army. Parliament Hill Shooting is an event which happened in the 22th October 2014 at the National War of Unknown Soldiers Memorial in Parliament Hill, Ottawa, Ontario, Canada. Surprisingly, this incident has caused only two deaths; Michael Zehaf-Bibeau and Captain. Nathan Cirillo and no one was harmed by the sudden attack (Gatehouse & Smyth, 2015).

The Parliament Hills shooting has become an eye opener to the Canadians especially the government as not to look easy on their national security and the safety of the public as well as the government servants. Social media has changed the way to communicate and give a different meaning in communication. It instantaneous of receiving information has transformed the society. This new platform for communication can become advantages or can be a liability to an organization and in this case the government. It will be more hectic to manage during a crisis. The CBC news reported, during the shooting at Parliament Hills is happening, people start to use social media to share about what's happening how the events had affected them. At this point of time, people are aggressively sharing of what they want without any control as it is the social. This will lead to another perception towards the government on how they manage the event as well as how they can control the social media. So that it would not affect the image of the government. According to (Matters & Matters, 2015) one of the setbacks of social media is that, messages that being delivered can become

an alternate message and it will interfere with safety and response. This is because of the speculations, rumors or even misinformation can fill up the social media before the real truth or fact being laid out to public.

The attacked of Pearl Harbour in 1941 is one example of intelligence failure where the investigation suggested that there is no centralization on intelligence operation to propose a clear allocation of responsibility (Lucas, 1995). The Joint Congressional Committee concluded that the military services in in Washington failed to bring the intelligence on Japanese plans and intentions on the bombing. Military intelligence and political leaders had access to the information regarding the Japanese movements however was fragmented and treated with bureaucracy by different agencies and leave that vast information in puzzle (Wohlstetter, 1962). While analysing the incident of Pearl Harbour, Finley (1994) conclude that the intelligence was failed according to several factors;

- i.   Lack of actions taken against the information gathered by military intelligence.
- ii. Insufficient intelligence training and inappropriate staff attachment on operations and evaluation.
- iii. The safety of raw information at every stage was risked by no sufficient credence. The information from Washington to the field was inadequate and vice versa make it stopped or slowed for security precautions.
- iv. Fault in information analysis and dissemination. Rumours on attacking Pearl Harbour was widely spread in Japan but no one to realise that potential target was the US fleet.

There are many events that prove the disappointment in intelligence. The failure in intelligence services confirmed by indication to a few of the defining events of the last century (Johnson, 2007). The intelligence services failed to foresee the Soviet experiment of its first atomic bomb, the North Korean invasion of South Korea, the construction of the Berlin Wall, an apparent string of failures over Vietnam, the Soviet invasion of Czechoslovakia in 1968 and of Afghanistan in 1979, the Iranian revolution in 1979, the Polish crisis of 1980–81 and, more crucial, specified that its main attention for over forty years was the USSR, the end of the Cold War (Johnson, 2007). All these failures occurred during the major events in history and should not be overlooked. The causes of the failures must be examined and solutions for the problem should be work out. Intelligence failure is not only can collapse any operations but might cost lives of unnecessary citizens. In the other hand, Intelligence Sharing is not always a simple and smooth procedure but risky and dangerous endeavour in intelligence while to keep cover in secret. Yet some intelligence agencies tend to involve in duplication of collection and gathered intelligence that has been analysed by other agencies (O'Connell, 2006). IC in United States has built information sharing and collaboration systems that provide document libraries and document sharing (Department of Homeland Security, 2017) that can be access by intelligence analyst but in the form of raw data and not been synthesized (Wu, 2013). In United States, there are 17 intelligence agencies with thousands of employees, 16,000 of them work for a single agency named The Defence Intelligence Agency (DIA) (Best (Jnr), 2011). Intelligence collection is a high cost operation comprises surveillance, staffing and requirement of latest technology but intelligence officers experienced communication breakdown and happened to not speak to each other even though covering the same area (Johnson, 2006). Their attitude probably to put the clandestine information safe and secured

yet to discourage the information sharing. While some agencies have the tendency to limit the sharing and dissemination of intelligence to protect policy makers from being influenced (Best (Jnr), 2011).

The most important event on intelligence breakdown in history was the 9/11 Attacks. This attacks stunned the policy makers at the country's vulnerability (O'Connell, 2006). William E. Odom (2004) claims that the attacks was a result from a massive breakdown in the intelligence system. Supporting by Best (Jnr) (2011), if the intelligence information was shared among the different agencies might have been served as clues in understanding the plot of the attacks to those agencies. The "need to know" has block and limited the information sharing between intelligence offices and law enforcement officials leads to the failure of detecting the plot at early stage. Contradict to the statement from President Office of United States(2007) claiming that the information sharing practiced among the IC of intelligence, law enforcement, defence, homeland security, and foreign affairs to intercept the ability of terrorist such as al-Qaida, interrupted terrorist plots, detained operatives, arrested or killed senior leaders, and strengthened the capacity of the Nation to counter and defeat the enemy. Another intelligence failure can be detected through the case of "underwear bomber". Umar Farouk Abdulmutallab plead guilty to eight charges in the endeavoured Christmas Day 2009 bombing of Northwest Airlines flight 253 and was sentenced to life in prison (Office of Public Affairs, 2012). Abdulmuttalab, a Nigerian man was attempt to detonate a bomb on a flight bound for Detroit from Amsterdam. The eight charges against him was attempted murder within the special aircraft jurisdiction of the United States; conspiracy to commit an act of terrorism transcending national boundaries; attempted use of a weapon of mass destruction; wilfully placing a destructive device on an aircraft, wilfully attempting to destroy and wreck a civil aircraft; which was likely to have endangered the safety of the aircraft; and three counts of possession of a destructive device in furtherance of a crime of violence (Office of Public Affairs, 2012). Best (Jnr) (2011) in his report "Intelligence Information: Need-to-Know vs. Need-to-Share" questioned the failure of sharing regarding the "underwear bomber" or in his writing known as "Detroit Bombing Attempt". According to the Senate Intelligence Committee Report later after the event found that there were various failures to sharing information. Abdulmuttalab's father had warned the officers in United States' Embassy in Nigeria about his son has been radicalized but no further action taken as no information of the warning been reported to other agencies. The "need to know" has limited the sharing of intelligence on Abdulmuttalab with other agencies such as Border and Security Department and Immigration to allow this man boarding the flight with a bomb in his underwear. He was travelling from Yemen to Africa and then to Amsterdam. From Amsterdam, he boarded Flight 253 to Detroit with intention to detonate the bomb during flight to cause the plane to crash and killing the 290 passengers and crew members on board (Office of Public Affairs, 2012). If the information of Abdulmuttalab's had been shared among intelligence and security agencies between Yemen, Africa, Netherlands and United States, Abdulmuttalab most probably was denied to fly out from Yemen at the first place.

12 died on November 5, 2009 as a result from information sharing failure. An Army Major, Nidal Hasan was accused of shooting some 45 service members at Ft. Hood, Texas (Best (Jnr), 2011). Hasan contacts with the terrorist was not shared among the intelligence agencies and they took for granted as Hasan was a military man and lived under a regimented system with strict officership and security standards. Moreover, Hasan communications is found to be not related to any FBI terrorism investigation (Best (Jnr), 2011). In the case of

Hasan, it is proven that intelligence analyst cannot easily access any information if it is not shared among them especially if they are from different department. The FBI and Department of Defence (DoD) failed to "connect the dot" or link the possible attacks by Hasan as they are not warned by each other of the potential threats. Intelligence failure can be witnessed through the incident of bombing of Brussel Airport in 2016, Belgium Jewish Museum shooting in 2006, Shooting and bombing in Paris attack in November 2015 and 9/11 attacks in 2001(Brunsden, Chassany, & Jones, 2016). The Islamic States was responsible in killing 130 in Paris and another 32 in Brussels (Brisard & Jackson, 2016).

The terror attack on Lahad Datu, Sabah by Sulu terrorist in 2013 also claimed by the media to as a consequence form the intelligence failure. The failure of sharing accurate and fast information about the Sulu terrorists to the security departments has resulted them acted only prior to the information which has been too late. The lack of sharing on intelligence create an overlapping works among the security agencies. Each of agencies works on the same tasks as no communication involved due to "need to know" basis. This overlapping and duplication of works causing the agencies to waste resources such as manpower, costs, time and information.

Realisation on Information and Intelligence Sharing
Practicing information sharing within team members can help the team to achieve their mission as everyone is exposed to various kind of information and knowledge. Yet, this statement is also supported by (Mesmer-magnus & Dechurch, 2009) whereby the authors have inserted the findings made by Hackman noting that information sharing helps to improve the team members' task and socio-emotional functioning as it helps to benefit the team in decision making and strategy planning. (Sheptycki, 2013) has mentioned in his article stating that information sharing is to reduce knowledge gaps and to make sure what is unknown known within the whole department. One of the ways suggested by the author is to standardize the process of how to translate the information received to create a new strategy related to an issue. Hence, intelligence cycle is the fundamental for the department to process the information in order to develop new policy and to enhance the communication process, the author has suggested that the police department should adopt the information age gadgets or technologies as part of their working tools.

Information sharing requires each involved unit to be transparent with each other. Besides, whatever information received should only be used for the intended purposes as it involves with data policy matters (Bickers, Hopkins-burns, Bennett, & Namay, 2015). Basically, information sharing does not only can be done between units, but it might also involve the utilization of human intelligence (HUMINT) for precise information. Similarly goes to Lahad Datu cases whereby the authority should cooperate with the local residents in order to help them to locate the Sulu Army who are living among these local people. The evolvement of communication method is one of the factors on how information sharing among government agencies can be enhanced. Social media are becoming today's main tool in circulating information throughout the world. Hence, as for this study, there is no doubt to measure the effectiveness of social media in assisting the government body to gain more information, either from other government agencies or from the netizens. As for example, in Malaysia, we have Polis DiRaja Malaysia (PDRM) as the nation's main agency to handle criminal acts. Besides, we also have other non-governmental agencies who also act as crime watchdog to report any suspicious or crimes to the responsible department. Twitter is seen to become a

useful platform for the police department to be in touch with the netizens. As information sharing nowadays does not only occur within government, but it can also be assisted by involving the society

The use of Twitter has benefited the police department to share criminal acts and incident information. Furthermore, the use of Twitter is not only limited to crime updates, however, the information given are usually related to celebrations, meetings, events, agendas, and traffic updates. In addition, the statement is supported by Unsworth (2014) in which she also stated that information interaction between the enforcement body and the society is contentious, and it will benefit both parties in combating more crimes from happening. Thus, in this situation, the researcher has her own personal Twitter account, and it is relatable to confirm whether the social media is helpful for intelligence sharing between the government and the society. Most of the time, PDRM will update the latest information such as the now the society can download their newest application, known as Volunteer Smartphone Patrol (VSP) upon their absence for going back for Hari Raya Aidilfitri celebration. Furthermore, Unsworth (2014) also highlighted that information sharing between enforcement agency and the society can increase the cohesiveness of community policing. Besides, it also teaches the society to become aware of their surrounding by observing any suspicious acts and person. Although there is argument criticizing about community policing, nevertheless, many believe that the implementation of this policy can reduce terrorist attacks.

Despite of the benefits in implementing information sharing in between enforcement agency and the society, another scholar has disagreed by the idea of circulating and sharing information and intelligence either within the society or government agencies. Information technology (IT) and software used by each department has become the main concern for (Hollywood & Winkelman, 2010) as they mentioned on the differences of software used in each agency. This issue is argued because in the United States, the enforcement agencies are using different software as what has been mentioned that certain department utilize records management system (RMS) for case histories, whilst other might be using computer-aided dispatch (CAD) system. Other than that, information sharing requires agencies to ensure that they have reached their mutual understanding to give and receive information they possessed on a particular operation. There are few types of mutual understanding that must be practiced by agencies in order to practice information and intelligence sharing which are One-Off Sharing, and Systematic Sharing. Systematic Sharing allows agencies to circulate information they have to other departments. Besides, the process of sharing the information is arguable as the employees involved have to follow the step-by-step process before handing out the information they receive.

Conclusion
There are many arguments on intelligence cycle for being outdated and the missing element of collaboration and information sharing (Aydin & Ozleblebici, 2015). Information sharing is different to the intelligence dissemination but frequently been confused especially in law enforcement circles (Duarte, 2007). Numerous observers criticized intelligence community in anticipating actions of terrorist syndicates for their shortage of vision or a failure to "connect the dots" as well as predicting actions of megalomaniacal, someone who is obsession with power and kleptocracies leaders, someone who is corrupt (Wirtz, 2006; Hurtado (2016); Ahmed, Khalid, Ammar, & Shah, 2017; Ahmed, Majid, & Zin, (2016), in his study proposed that

intelligence cycle should consist the element of communications and cyber security to face the 21st century's intelligence challenge. However, his study focus on the arising use of internet and social media. George (1979) has suggested that intelligence failure can occur at any point in the intelligence cycle. His study concerned on exploring the intelligence cycle itself which are setting intelligence requirements, collecting data, analyzing data, and disseminating finished intelligence (Wirtz, 2006).

Realizing the information sharing in intelligence cycle requires great effort and trust between agents and agencies. Human limitations can become a major motivation either restriction to apply information sharing in the intelligence cycle. Agents should be provided with training and education on proper information sharing while practicing the intelligence cycling.

Corresponding Author
Mohammed Yaacob
Centre of Media Information and Warfare Studies
Universiti Teknologi MARA
40450 Shah Alam, Selangor, Malaysia.
Email: mbyzur@yahoo.com

References
Ahmed, U., Khalid, N., Ammar, A., & Shah, M. H. (2017). Assessing moderation of employee engagement on the relationship between work discretion, job clarity and business performance in the banking sector of Pakistan. Asian Economic and Financial Review, 7(12), 1197-121. https://doi.org/10.18488/journal.aefr.2017.712.1197.1210

Ahmed, U., Majid, A. H. A., & Zin, M. M. (2016). Moderation of meaningful work on the relationship of supervisor support and coworker support with work engagement. *The Journal of Business, Economics, and Environmental Studies (JBEES)*, *6*(3), 15-20.

Aydin, B., & Ozleblebici, Z. (2015). Is Intelligence Cycle Still Viable ? In *International Conference on Military and Security Studies-2015* (pp. 1–6). Istanbul.

Best (Jnr), R. A. J. (2011). Intelligence Information: Need-to-Know vs. Need-to-Share. *Congressional Research Service*. Retrieved from https://www.fas.org/sgp/crs/intel/R41848.pdf

Bickers, P., Hopkins-burns, V., Bennett, A., & Namay, R. (2015). Information sharing by government agencies : The effect on the integrity of the tax system, *13*(1), 183–201.

Brisard, J.-C., & Jackson, K. (2016). The Islamic State's External Operations and the French-Belgian Nexus. *CTC Sentinel*, (Nov/Dec), 1–8.

Brunsden, J., Chassany, A. S., & Jones, S. (2016, April 4). Europe's failure to share intelligence hampers terror fight. *Financial Times*. Retrieved from https://www.ft.com/content/f9baf7e8-f975-11e5-b3f6-11d5706b613b

Department of Homeland Security. (2017). Homeland Security Information Network (HSIN). Retrieved August 17, 2017, from http://hsin.dhs.gov

Duarte, N. (2007). Unleashing our untapped domestic collection is key to prevention. *Naval Postgraduate School.*

Finley, J. P. (1994). Nobody likes to be surprised: Intelligence failures. *Military Intelligence Professional Bulletin*, *20*(1), 7–15. Retrieved from

http://web.b.ebscohost.com.ezaccess.library.uitm.edu.my/ehost/detail/detail?vid=4&sid=c2c44c49-4525-4339-a9e2-5c876bba233c%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=aph&AN=9706170978

Folker, R. D. (2000). Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods. *Intelligence*, (January), 45.

George, A. (1979). International violence : terrorism , surprise , and control. (Y. Evron, Ed.). *Jerusalem: Leonard Davis Institute for International Relations*, Hebrew University of Jerusalem.

Gookins, A. J. (2008). The Role of Intelligence in Policy Making, *28*(1), 65–73. https://doi.org/10.1353/sais.2008.0025

Hollywood, J. S., & Winkelman, Z. (2010). Improving Information-Sharing Across Law Enforcement: Why Can't We Know? *Police Executve Research Forum*.

Hurtado, L. A. V. (2016). *Colombia and the intelligence cycle in the 21st century , the digital age*. University of Tartu.

Johnson, L. K. (2006). A Framework for Strengthening U.S. Intelligence. *Yale Journal of International Affairs*, *1*(2), 116–131.

Johnson, L. K. (2007). Strategic Intelligence. In A. S. Hulnick (Ed.), *Strategic Intelligence* (Vol. 1–5). Westport: Praeger Security International.

Johnston, R. (2005). Analytic Culture in the US Intelligence Community: An Ethnographic Study. *The Center for the Study of Intelligence* (Vol. 160). Retrieved from http://scholar.google.com/scholar?q=related:LPH9g5ubT4YJ:scholar.google.com/&hl=en&num=30&as_sdt=1,5%5Cnpapers2://publication/uuid/A603D066-21F1-480D-8EB7-2E9052410D01

Lederman, G. N. (2004). Restructuring the Intelligence Community.

Lucas, J. W. (1995). *Organizing the Precidency: the Role of the Director of Central Intelligence, 1947-1977*. Gearge Mason University.

Mesmer-magnus, J. R., & Dechurch, L. A. (2009). Information Sharing and Team Performance : A Meta-Analysis, *94*(2), 535–546. https://doi.org/10.1037/a0013773

Yasid, M. A. F. (2016). Peranan Pasukan Cawangan Khas Polis. *Sejarah*, *25*(2), 23–39.

National Security Council. (2017). *National Security Council*. Retrieved July 26, 2017, from https://www.mkn.gov.my

O'Connell, A. J. (2006). The architecture of smart intelligence: Structuring and overseeing agencies in the post-9/11 world. *California Law Review*, *94*(6), 1655–1744. https://doi.org/10.2307/20439079

Odom, W. E. (2004). Fixing Intelligence for a more secure America. *Journal of the American Intelligence Professional*, *48*(2), 230. https://doi.org/10.2307/20202357

Office of Public Affairs. (2012, February 16). Umar Farouk Abdulmutallab Sentenced to Life in Prison for Attempted Bombing of Flight 253 on Christmas Day 2009. *Department of Justice Website*. Retrieved from http://www.justice.gov/opa/pr/2012/February/12-ag-227.html

Paidi, Z., Hj, R., & Ghani, A. (1960). Darurat di Tanah Melayu : Peristiwa dan Pengajaran Untuk Generasi Masakini Dalam Konteks Ketahanan Nasional, 13–33.

President Office of United States. (2007). *National Strategy for Informatioan Sharing: Success and Challenges in Improving Terrorism-Related*. Washington DC. Retrieved from http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf

Sheptycki, B. J. (2013). Information flows in the police organization ; what is going on inside the machine ?, (435), 1–18.

The Commissioner of Law Revision. Armed Forces Act 1972, Percetakan Nasional Malaysia Bhd § (2006). Kuala Lumpur: Laws of Malaysia.

The Commissioner of Law Revision. Police Act 1967, Percetakan Nasional Malaysia Bhd § (2006). Kuala Lumpur: Laws of Malaysia.

Unsworth, K. (2014). Questioning trust in the era of big (and small) data. *Bulletin of the Association for Information Science and Technology*, *41*(1), 12–14. https://doi.org/10.1002/bult.2014.1720410108

Vitkauskas, D. (1997). North Atlantic Treaty Organisation: The Role of a security Intelligence Service in a Democracy.

Wirtz, J. J. (2006). The American approach to intelligence studies. In L. K. Johnson (Ed.), *Handbook of Intelligence Studies*. New York: Routledge. https://doi.org/10.4324/9780203089323.ch2

Wohlstetter, R. (1962). *Pearl Harbor: Warning and Decision by Roberta Wohlstetter*. Standford University Press.

Wu, Y. (2013). Strengthening Intelligence Education with Information-Processing and Knowledge- Organization Competencies Strengthening Intelligence Education with Information-Processing and Knowledge-Organization Competencies. *Journal of Strategic Security*, *6*(3), 10–24. Retrieved from http://scholarcommons.usf.edu/jss%5Cnhttp://scholarcommons.usf.edu/jss/vol6/iss3/2