Intelligence Information-Sharing

Name of the University

Name of the Writer

**Literature Review**

Nowadays, the world is a global community with interconnected parts that have a wholesome effect on the different nations residing within it. Within such an environment it is imperative that security of the state be maintained at all costs. This is where the different intelligence agencies come into play. These agencies play an integral part in collecting information regarding events that are about to occur and have occurred in the past. They use this information to assess the current and future conditions of the country. However, there has been some discomfort regarding the sharing of information between the different intelligence agencies operating within a country. But in recent years immense work has been done both in academics and in real life regarding information sharing between the different intelligence agencies operating within a country.

Research done by Skopik, et al, (2016), states that the threat landscape is changing immensely with each passing day. In terms of cyber-crime, a more organized approach to crime is being perpetrated. Attacks are taking place that are focused on circumventing traditional measures of security that are in place. Furthermore, networks have grown immensely in the past decade or so. They have become intertwined with other networks and the only way to safely secure the entire network is through combined efforts on part of all vested parties specifically intelligence agencies. With cyber-crime and cyber-attacks in order to fully grasp the entire situation regarding such crimes, information sharing is absolutely necessary. This is also important in order to thwart any future attacks related to the cyber world. Information sharing would prove to be useful in discovering malware and covert attacks, securing networks, early warning notice and the distribution of data on a more selective basis.

Furthermore, the work of Maras, (2017), entails the roadblocks that come in the way of sharing of intelligence between different agencies. This research dictates that the existing organizational framework is an important factor to consider when looking at the flow of information sharing between agencies. The organizational culture that is prevalent within agencies serving in the intelligence community has become a hindrance to the level of information that is being shared among them. Within these agencies secrecy and limited disclosures of any sort of information are prevalent and cultures associated with such characteristics are implemented within these agencies. Additionally, practicing the art of distribution of information and compartmentalization of information is impeding the exchange of information in the intelligence community. In order to further progress the information sharing, it is suggested that changes within the culture of the organization in the intelligence community is direly needed, as it is hampering the envisioning of information-sharing culture.

Furthermore, Weiser, et al, (2016) has also stressed immensely on the importance of digital forensic intelligence data and the development of a national repository for this data. This helps in information sharing between the different intelligence agencies. The modern world is heavily connected and this is leading to increasing connectivity for criminals as well. They can easily gain access to fiscal information such as credit card information that can put numerous people at risk. This is why it is important to form a national database for the collection of data in the discipline of digital forensics. This article illustrates how agencies around the world require the use of digital forensics in order to better protect the system in place. With a collection of information, they would not have to look far to gather up information regarding any certain impending crisis. Furthermore, all of this will help in increasing the understanding of any coming threat that could jeopardize the security of the homeland.

Further research has been done that shows how important the flow of information is between agencies is. As the more frequent the movement of information is the higher the chance that more awareness of threats related to homeland security is attained. The work of Jasper, (2016), illustrates how intelligence sharing has led to the increased awareness of threats of cyber nature and how they are potentially harmful to homeland security. With an increased in the frequency of information, activities of malicious actors in cyberspace that can have potentially detrimental effects for homeland security can be rooted out. This is really important as these groups have a plethora of resources towards dismantling any traditional form of defenses. These malicious actors can be either organized criminals or state-sponsored terrorist groups that mean to undermine the fabric of society. This research further states how increased intelligence sharing has benefitted homeland security in several instances. Such as the fact increased awareness regarding malicious groups in China that were targeting US-based companies

Work of Mohaisen, et al, (2017), focused on information sharing can be really helpful in accumulating actionable intelligence regarding a different threat to homeland security. They state that in the last decade the landscape of information threats and security has changed completely. This has made it very difficult for just one agency to work and defend the security of everyone. In this manner, the distribution of information needs to be facilitated between communities that are based on trust so that the defense could be facilitated to the maximum. Furthermore, the distribution of information threat indicators could be collected and could be used to scan information coming in alignment with them. This will also help in decreasing the time lag between information gathering and taking action on credible information. However, this piece of work illustrates some problems that might occur with collecting information for threat indicators. The report suggests that there should be models such as threat models that will help in collecting information on the basis of the risk understood from them, their measurement and scoring of each risk.

Furthermore, with the rise of information sharing, homeland security policing is also on the rise. This was highlighted by the work of Sedgwick and Hawdon, (2019), who illustrated the fact the homeland security policing has been on the rise. This is further leading to all police organizations coming together and cooperating with each other by sharing intelligence regarding any threats. Their work has listed that more light is shined on the increased cooperation between the federal and local policing agencies. Very little focus is kept on the cooperation between agencies who have a contiguous jurisdiction. Moreover, there is a humongous amount of research that details how information is shared between agencies but there is limited research present that actually details how any other cooperation than information sharing is done between different agencies. This piece of work suggests that other than information-sharing agencies have seen to be in cohesion in some form or the other. This includes joint activities and agrees on sharing the benefits that emerge from working together.

Vogel and Dennis, (2018), illustrated how important it is to share information between different agencies in order to increase awareness and thwart any threat that might threaten homeland security. They used the example of September 11 and the Iraq War of 2003 in order to further emphasize their point. These two instances saw the failure of intelligence agencies who were unable to prevent immense loss of life. Lessons were learned from such circumstances and the United States of America has recognized the importance of information sharing not only domestically but also internationally in order to work around any breakdowns in intelligence in the future. This paper further focuses on how this is the perfect situation for using Science and Technology scholars. It is exciting to consider the opportunities and the level of difficulties that will arise from such a relationship. Furthermore, the level of information that would be generated from the engagement between this type of scholar and the secret intelligence units would be something than what was ever done before.

Varga, et al, (2018), relates information sharing regarding the nation's cyber situation with increasing the awareness regarding the threats to it. These threats have potentially detrimental consequences for homeland security as well. According to their work, as more and more dependency is increased on the IT services with increasing modernity has the potential chance of cyber-attacks and service management mistakes that could have dire consequence for the security of the country. In order to mitigate this and increase awareness regarding such incidences, it is important to develop cyber situational awareness. However, this can only be done through increased information sharing that will lead to the formation of threat indicators. The paper aimed at the basic components of information that have to be collected in order to form a well-developed picture of increasing awareness regarding the situations related to cybersecurity. This is because cybersecurity has become the new war front for countries and can literally implode a country if not managed with a fine-tooth.

Further work done by Simola (2019), shows focus on cybersecurity threats as well and the need to increase awareness on these threats in order to impede their effect on national security. In recent times there has been a rise in threats related to the cybersecurity of the nation. Challenges related to cybersecurity are on the rise and agencies and different organizations need to step up in order to face these challenges. The only way forward is cooperation and cooperation in the sense of information sharing between the relevant authorities is immensely needed. Not only that information sharing between governmental and non-governmental entities has also been shown as an important step to be taken in mitigating risks related to cybersecurity and the threat that it poses to homeland security. However, in order to promote information sharing between different entities, this report highlights the importance of forming information sharing models that could help in an effective manner of transfer of information. So, in the formation of such a model, this article works on locating the different factors that affect the formation of such models and how they can be mitigated.

Lastly, Paula and Zhuang, (2019), have worked on researching the level of information sharing related to threats to cybersecurity that could have consequences for homeland security. In their research, they looked upon various entities such as government, adversaries, and citizens in order to analyze the level of information sharing that occurs between these different organizations. They see that a mixture of approaches has been done in literature in order to analyze this relationship such as quantitative and qualitative. Quantitative literature has defined the limitations and the benefits that have occurred in information sharing between several stakeholders. It further proposes measures that enable a faster, effective and secure means of relaying information between these different groups. Lastly, this review construes around eighty-two papers that have identified different approaches to information sharing and how it has affected the security of the nation.

References

Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53-65.

Maras, M. H. (2017). Overcoming the intelligence-sharing paradox: Improving information sharing through a change in organizational culture. *Comparative Strategy*, *36*(3), 187-197.

Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for actionable threat intelligence. *arXiv preprint arXiv:1702.00548*.

Pala, A., & Zhuang, J. (2019). Information Sharing in Cybersecurity: A Review. *Decision Analysis*, *16*(3), 172-196.

Sedgwick, D., & Hawdon, J. (2019). Interagency Cooperation in the Era of Homeland Policing: Are Agencies Answering the Call?. *American Journal of Criminal Justice*, *44*(2), 167-190.

Simola, J. (2019). Comparative Research of Cybersecurity Information Sharing Models. *Information & Security*, *43*(1), 175-195.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Varga, S., Brynielsson, J., & Franke, U. (2018, August). Information requirements for national-level cyber situational awareness. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 774-781). IEEE

Vogel, K. M., & Dennis, M. A. (2018). Tacit Knowledge, Secrecy, and Intelligence Assessments: STS Interventions by Two Participant Observers. *Science, Technology, & Human Values*, *43*(5), 834-863

Weiser, M., Biros, D. P., & Mosier, G. (2016). Development of a national repository of digital forensic intelligence.