Resilience and the threats to the supply chain

[Name of the Writer]

[Name of the Institution]

Resilience and the threats to the supply chain

**Abstract**

Supply chain forms one of the major department of homeland security, taking into account that resilience is greatly impacted by the intervention from both internal and external resources. In accordance with the research, it is asserted that the intervention from external resources have challenged resilience because technological advancement has blinded both national and international system of the negative impacts these strategies can have in the long run. After a long time, span of destruction, the government is trying to take initiatives that can help to address complications that are posed by external cyber intervention. It is doing more harm than good because these resources are challenging the strengths of supply chain and its resilience. These challenges are in the form of lack of security enactment, and vulnerabilities. Although different projects are serving at both national and international level, still these cyber interventions are becoming hard to eradicate because they have direct and more effective access to almost all related departments.

**Introduction**

Resilience is defined as the ability to be efficient enough to be prepared for any kind of unexpected risk event. The supply chain should be built on strong strategies that it can respond and recover from any kind of disruption and it can help to restore the efficiency of the supply chain. It is asserted that the supply chains are very complex and made on global perspectives so there are more chances of disruption *(U.S. Department of Homeland Security, 2019).* It is believed that the strength of the supply chain is parallel to the risks at its weakest link. With increased technology, there are a lot of threats that appear in different shapes and formats, hampering the overall framework of homeland security. These threats can be from hackers, any foreign advisory or the criminals themselves who are looking for an escape. As a result of such threats, the vulnerabilities are exploited and the underlying essence of supply chon is distorted. The cybersecurity and Infrastructure Agency is trying its best to work with those industry partners and governments that can ensure the safety of supply chain from any kind of threats, especially cybersecurity efforts(U.S. Department of Homeland Security, 2019). CISA has incorporated different strategies such as adhering to technological incorporation and a centralized approach to check and balance in order to ensure resilience and prevent threats to the supply chain. There are several assumptions and ideologies that are proposed to address, either getting external cyber support a positives strategy in the form of maximum protection or is it a disguise that seems to be a blessing apparently*(U.S. Department of Homeland Security, 2019).*

**Research Question**

External Cyber interventions a potential threat to homeland security causing disruption to the supply chain

**Hypothesis**

External Cyber Intervention are posing a serious threat to homeland security especially in terms of supply chain management

**Literature Review**

Cybersecurity is termed as one of the multidimensional challenges that require attention from different resources to keep check and balance because the threats of cybersecurity are equally threatful towards the national platforms of security. Homeland security and its supply chain is one of the features that is affected by the cyber intervention, disrupting and hampering the resilience of supply chains. As information technology is a diverse topic, different researchers have a different point of understanding towards it. According to Alderson, (2019), Supply chain is more like a product that comprises of different people, resources, information, and activities. With an increased approach to the use of technology and the use of technological media for prevention and security purposes, external cyber interventions are used considering their maximum potential. However, in the context of homeland security, the scenario is found to be different because external cyber intervention is in the form of hardware’s and software’s, that complicate and disrupts the security system automatically affecting the supply chain (Alderson, et al. 2019).

According to Fisher, (2019) using external cyber approaches and resources just because of their increased efficiency in native land has hampered USA’s security to a greater extent. He quoted the example of an incident that happens in 2017. The department of Homeland Security ordered to remove the Kaspersky security products from the networks because they were posing serious risks. It is also asserted that the so-called security system compromised the workability of confidential platforms because of some unauthorized access to some sensitive networks (Fisher, et al. 2017). However, Bjorck, (2015), is of the view that threats to homeland security are not confined to the use of cyber tools and extension at a departmental and governmental level, in fact, domestic use and the approach to innovative devices also plays a central role in hampering the homeland security. He asserted that domestic and local platforms are used to approach the supply chains and disrupt them (Björck, et al. 2015). Taking into account the significance of the initiatives that are taken by the government of the United States, Walker, (2018) quoted that it is evident that the threats to supply chain are evident, so, different governmental platforms are trying to resolve and mitigate the interruption in the supply chains. He mentioned different organization such as Departments of Homeland Security Science and Technology Directorate Centre of Excellence and the Food Protection and Defense Institute that are trying to incorporate new and unique ways that can help to understand the points where supply chains are more vulnerable to disruptions (Walker, et al. 2018).

In accordance with the idea that government is trying to take efforts that can help to overcome the threats by external cyber intervention, Farmer, (2019), proposes that the government is trying to create a cybersecurity model that can be used to protect the cyber assets of a nation. These protection strategies would appear in the form of Cyber Supply Chain Assurance Reference Model (Farmer, et al. 2019). However, the controversial point is, this model is not a universal approach that could address the issues and threats that are continuously opposing the success opportunities of the supply chain resilience. Moreover, the research by Flammini, (2019) infers that today, supply chain disruption is one of the most discussed topics because it caters to almost all dimensions of homeland security. A holistic evaluation highlights that external cyber intervention was one of the friendly approaches that were assumed to centralize security but it has distorted the resilience of supply chain by the intervention of hackers, data stealers, policymakers, unauthorized access initiatives and the centralization of data on platforms that are themselves not secure (Flammini, et al. 2019).

**Methodology**

In order to analyze the data that is collected from different research materials that are published, qualitative research methodology is used. It refers to the qualitative investigation of data, that would be accompanied by content analysis. Content analysis is a research tool that is used to decipher the existence of some specific themes concepts and words along with some qualitative justification that can help to analyze and decipher the relationship of different variables. It is one of the approaches that can be used to understand the underlying intentions and difference of a single idea or theme. Content analysis is one of the approaches that can help to elaborate or broaden the horizon of understanding of facts and figures by comparing and contrasting it with other existing ideologies and actives.

**Discussion**

From the research of Alderson, (2019) it is inferred that supply chain is not a simple phenomenon, in fact, it is a complex firework that invites attention and contribution from different departments and effective management automatically requires an approach that could address the issues at its peak. For the management of these complex platforms different options are used such as hardware’s and software’s but today they turn out to be the biggest threat. He is of the view that cybersecurity has brought massive mismanagement to the services and products. However, Fisher, (2017) represented a different point of view that is supported by some national decisions and incident such as the order to replace and stop using Kaspersky security because these software’s are an indirect approach to disrupt the national supply and chain. It ultimately affects the resilience and compromises the working and authenticity of the safety of information and resources. It is found that Björck, (2015) also accepts the ideologies presented above but the perspective is different because he uses locale understanding to incorporate an understanding of the facts and figures that are associated with the management and use of the cyber intervention. He proposed a common dilemma that public just focuses the personal benefit without knowing the future impact and it is the reason that national security is hampered by the lack of accountability.

The research by Walker, (2018) incorporated some constructive approach by introducing the national and governmental strategies that are used by the government to strengthen resilience and address the efficiency of the supply chain. In the same way, Farmer, (2019) enlighted with the opportunities that are proposed by the government to address the issues of cybersecurity that can cast a negative impact on the supply chain. The same ideology is promoted by Flammini, (2019) asserting that homeland security can only be maintained by some reflective and yielding approach to the mitigation of risks that are imposed by external resources.

**Findings**

From the exegetical analysis of the researches and content, it is found that there is greater stress on the negative impact of the cyber intervention in terms of homeland security. From the research material, it is gathered that cyber interventions have posed a serious threat to the supply and chain management because none of the actions and strategies are kept private, in fact, the country seems to be itself welcoming to the threats and risks (Schabacker, et al. 2019). Although government is taking serious action to understand and mitigate the impression of external cyber intervention still, it is one of the issues that is playing a central role in challenging the security paradigms. There are different historical and current scenarios of negative approach and threats are associated with the intervention of external cyber option where they are casting a negative impact on baseline making the supply chain weak and more vulnerable to different threats and warnings (Wallace, et al. 2019).

**Conclusion**

Homeland security is one of the most crucial platforms of success and security. The approach to technology and advancement has brought a great threat to the universal approaches that are used to empower both human’s resources and the management of those resources. In order to meet the increasing security concerns, significant steps are taken by the government agencies to take initiatives that can help to strengthen the resilience of the supply chain but it has inversed the expectations. Under the impact of external cyber interventions, cyber threat has increased in the form of different hackers, and foreign advisories who are trying to penetrate within the national homeland security system (Schabacker, et al. 2019). Catering to the sensitivity of the issue, the government is trying to take significant steps in the form of Intervention Planned and Cyber Management Models, but the threat is the same. Such interventions have distorted the underlying efficiency of strategies that are taken by the government to address resilience because supply and chain system is becoming weak and more vulnerable to different attacks and threats. However, the major section of threat is promoted by the 5 Generation that is taking technology for-granted and it has bought a great easiness for different external departments to intervene and destroy the resilience. It is asserted that there is a dire need of both practice steps and opportunities that can help to establish some overreaching framework that would be effective enough to address this issue (Schabacker, et al. 2019).

References

#### Agencies, A., Agencies, A., & Address: M. (2019). *U.S. Department of Homeland Security | USAGov*. *Usa.gov*. Retrieved 7 September 2019, from https://www.usa.gov/federal-agencies/u-s-department-of-homeland-security

Alderson, D. L. (2019). Overcoming barriers to the greater scientific understanding of critical infrastructure resilience. *Handbook on Resilience of Socio-Technical Systems*, 66.

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New contributions in information systems and technologies* (pp. 311-316). Springer, Cham.

Farmer, C. M., Whipkey, K., & Chamberlin, M. (2019). *Programs Addressing Psychological Health and Resilience in the US Department of Homeland Security*. RAND Corporation.

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of business continuity & emergency planning*, *11*(2), 163-173.

Flammini, F. (2019). *The resilience of cyber-physical systems*. Cham: Springer.

Gritzalis, D., Theocharidou, M., & Stergiopoulos, G. (2019). *Critical Infrastructure Security and Resilience*. Springer, Cham.

Schabacker, D. S., Levy, L. A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing Cybersecurity Vulnerabilities and Infrastructure Resilience. *Frontiers in bioengineering and biotechnology*, *7*.

Walker, J. J., & Cooper, M. K. (2018). Resilience. In *Companion to Environmental Studies* (Vol. 90, No. 94, pp. 90-94). ROUTLEDGE in association with GSE Research.

Wallace, R. (2019). Challenges to the US Security Doctrine of “Resilience”. In *Cognitive Dynamics on Clausewitz Landscapes* (pp. 77-90). Springer, Cham.