Proceedings of the International Conference on Industrial Engineering and Operations Management
Manila, Philippines, March 7-9, 2023

Modelling Resilient Healthcare Supply Chain: A Hybrid Vulnerability-Capability Model with TISM-MICMAC Approach

Vikrant Giri and Prof Jitender Madaan
Department of Management Studies
IIT Delhi, Hauz Khas, New Delhi, India, 110016
Vikrantgiri92@gmail.com; jmadaaniitd@gmail.com

Prof Nikhil Varma
Anisfield School of Business, Ramapo College of New Jersey NJ 07430, USA*
nvarma@ramapo.edu

Abstract

In today's global business context, high competition forces companies to operate in highly uncertain conditions. Whenever these uncertainties convert into risk, and the risk becomes reality the companies may face profitability loss. Moreover, if the company is dealing in the healthcare sector, a loss is not limited to profitability instead, it may lead to the loss of lives. Resilient Healthcare Supply Chain (RHSC) could be an answer to the uncertain disruption challenges. Although various studies have proposed a resilient supply chain, this research paper addresses the partially filled gap for RHSC. This research assumes that all medicinal products supply chain does not require the same level of resilience.

Moreover, it is challenging to achieve resilience free of cost. Hence, this research uses a vulnerability-capability framework to map the resilience requirements as a function of vulnerability and corresponding capability. Furthermore, it uses Total Interpretative Structural Modelling to establish a hierarchical relationship among various factors to better explain the relationships. In addition, this study uses MICMAC analyses which helps classify variables as drivers, linkages, and autonomous and dependent variables. This research concludes with interesting findings about the "what " and "how" of the theory and some future research directions with limitations of this research.

Keywords
Healthcare Supply Chain, Decision Science, TISM, MICMAC, Vulnerability-Capability framework.

1. Introduction

Pharmaceutical supply chains (PSCs) are amongst most critical supply chains. They can be considered critical due to their inherent function of supplying critical medicines to the patients. PSCs involves all activities from raw material acquisition management, to production, to packaging, to distribution (Warehousing and transportation), to last mile delivery. Since PSCs are accountable for ensuring accessibility, availability, affordability of quality medicine to the consumers, it becomes critical ensuring the efficient, effective, and smooth functioning of the PSCs in the highly complex and competitive business environment. However, maintaining the smooth functioning of PSCs has always been difficult for supply chain managers due to various risks and vulnerabilities that may get exposed during disruptive events(Creazza et al. 2022), (Pettit et al. 2010).

Supply chain vulnerability can be defined as a "function of certain supply chain characteristics and that the loss a firm incurs is a result of its supply chain vulnerability to a given supply chain disruption" (Wagner and Bode 2006a, p.304). Various vulnerabilities can be present with-in the supply chain. According to Pettit, Croxton and Fiksel (2013) "Forces of change create supply chain vulnerabilities". Peck (2005) concludes that there is no system, however well managed, invulnerable. Even capabilities can bring vulnerability together with them. For example, new IT infrastructures provides agility in information flows. And information sharing can be an enabler to resilient supply chains. However, this IT infrastructure comes with cyber threats that, if ignored, can disrupt the supply chains (Sazvar *et al.* 2021).

So, we can say vulnerabilities are the unknown or ignored threats or calculated risks that may get magnified in the presence of some disruption. For example, supplier dependence of a firm can make it vulnerable by reducing its flexibility to switching to the other suppliers in the presence of supplier disruption (Bourantas 1989). Here risk would be supply shortage and the vulnerability would be dependence.

Many researchers have researched on supply chain risk management from array of perspectives such as, risk modelling, risk identification, risk mitigation, risk measurement, risk assessment (Creazza et al. 2021 and 2022), (El Mokrini et al. 2016), (Madaan and Choudhary 2015), (Moktadir et al. 2018), (Nguyen et al. 2021). However focus on vulnerabilities in supply chain management has grabbed attention due to increased frequency of disruptive events (Pettit et al. 2013). This research is novel in its kind due to its capability to contribute in three major directions. Firstly, it uses one of its kind hybrid vulnerability-capability framework using TISM-MICMAC approach. Secondly, it discusses the less discussed operational and relational factors. Third, it is rare to find a vulnerability capability based hierarchal classification model specifically in pharmaceutical supply chain context.

1.1 Objectives

This research identifies, and model interrelationships among various vulnerabilities and capabilities that can be present in the pharmaceutical supply chain. In this way, this research has three objectives (1) what are main vulnerabilities that can be present in the PSC? (2) how are the identified vulnerabilities hierarchically related to each other? (3) what can be the vulnerabilities that should be focused first? By answering stated three questions, this research contributes to the existing literature in at least two manners. Firstly, this research enriches the PSC literature by methodologically finding, classifying and modelling the vulnerabilities that can be existed in the PSC. Secondly, this research could help in decision making related to disruption management scenarios.

2. Literature Review

2.1 Vulnerabilities in supply chain

Vulnerability and resilience are the two concepts inversely proportional to each other (Bogataj and Bogataj 2007). Vulnerabilities exist in every system; the system administrator should know the cost of risk associated with that vulnerability if exposed due to disruption. A supply chain system is vulnerable if it is designed to ignore threats. According to the dictionary definition (Vocabulary.com 2022), “Vulnerability is the quality of being easily hurt”. According to Wagner and Bode (2006), vulnerability is the exposure or susceptibility of the supply chain to the impact of disruption.

To understand the difference between vulnerability and risk, let’s consider the following situation. Any working system is always surrounded by risks. But system gets disrupted only when the system is vulnerable to the specific risk. For example, during COVID-19 most of the supply chains got disrupted because of their global concentrated sourcing strategy. Although no system is without vulnerabilities. But it would be better if the associated losses are known beforehand. The present research identifies various vulnerabilities from the literature.

Table 1 presents only those vulnerabilities that have been considered after multiple discussions with the area experts.

2.2 Dependence: In supply chain networks dependence is inevitable. But the level of dependence can be one of the deciding factors that can affect the vulnerability of the supply chain. Dependencies in the supply chain can exist in any direction viz, supplier dependence and/ or customer dependence. Supplier dependence can be measured as the ratio of buying firm purchases from the supplier to the total supplies a firm buys (Bourantas 1989).

2.3 Accountability: Accountability refers to the responsibility of each member in the supply chain to fulfill their obligations, meet standards and regulations, and maintain high levels of performance. This involves being accountable for the quality of goods and services provided, adhering to ethical standards, and meeting deadlines and budgets. There are several instances where secondary distributers may act irresponsible due to absence of accountability mechanisms in the system. It could be so because secondary distributors often purchase medicine from other than manufacturers for higher profit margins and sell them to healthcare facilities (Marucheck *et al.* 2011).

By promoting accountability and addressing vulnerability, companies can improve their supply chain performance and reduce the risks associated with weak links in the chain. This can lead to increased efficiency, better risk

management, and improved overall business results. Additionally, fostering a culture of accountability and vulnerability can also improve collaboration and trust among supply chain partners, leading to more successful and sustainable partnerships.

2.4 Self-interest and Power dynamics: Self-interest refers to the pursuit of one's own goals and objectives, which may include maximizing profits, protecting one's reputation, or achieving competitive advantage. In a supply chain context, self-interest can drive individual or companies to prioritize their own interests over those of their partners, leading to behavior that can make supply chain vulnerable to mismatch and supply and demand. Self-interest and power dynamics can create disruption in PSC. As Yaroson et al. (2021) findings indicate that power dynamics can control the three major flows in PSC. These three flows are information, money, and material. Also, self-interest can drive the use of power (Tucker and Daskin 2022). Self-interest here means that the interest that causes hoarding the information about status of any of the three major flows.

Table 1. Literature review related to finalized vulnerabilities in supply chain

Source	**Vulnerability (Exposure/susceptibility to the impact of Disruption)**	**Sub factors**	**Risk**	**Logic/reasoning**
Wagner and Bode (2006b), Zhao et al. (2020), Svensson (2000, 2002, and 2004), Barnes and Oloruntoba (2005)	Dependence	Time dependence, functional dependence, relationship dependence, sales dependence Resource dependence	Supply Shortage risk or Sales drop risk	Depending on supplier/customer dependence risk will be supply shortage or sales drop.
Mark Stevenson and Jerry Busby (2015), Marucheck et al. (2011)	Accountability	Responsibility to fulfil obligations.	Contamination /Adulteration, counterfeiting. Substandard and falsified medicine	Patient safety and product recalls Viagra (Jackson 2009), Tylenol (Rogers 2009), Heparin (Blum 2008)
Nematollahi *et al.* (2018), Yaroson *et al.* (2021)	Self-interest and Power dynamics	Supply chain visibility, information asymmetry	May affect three basic flows in supply chain	This phenomenon is very normal whenever there is a shortage of product in the market, any supply chain actor who has power to control flow of product to reach to it's self-interest.
Zaprutko *et al.* (2020), WHO 2017)	Parallel trade	Cross border sales	Drug Shortage	Even after producing enough to cater to demands of one country parallel trade can cause shortage
Yaroson *et al.* (2021), Hou *et al.* (2018), Dubey *et al.* (2019)	Trust	Individual trust, network level trust		

Mehra and Verma (2020), Jia and Zhao (2017)	Publicized shortage	Self-interest and power	Drug shortage	Can act as catalyst to hoarding, counterfeiting, and falsification
Kamba *et al.* (2017), World Health Organization (2017), Vishwakarma, Garg and Barua (2019)	Weak reverse flow	---	Substandard or expired medicine back into the legitimate supply chain	Can affect penetration of expired medicine introduction into fair medicine supply chain
Gu et al. (2021), Creazza et al. (2021), Zijian Ao (2020)	IT infrastructure	Visibility, transparency, cyberthreats	connectivity	Can increase transparency as well as vulnerability to cyber threats

2.5 Parallel trade: "Varying prices for medicines create incentives to move products from one market to another to arbitrage the difference; this is known as parallel trade" (Liang 2006). In the US, Avastin, a brand that trade in cancer medicine, faced the penetration of falsified medicines in its supply chain due to parallel trade (WHO 2017). Parallel trade can also cause the shortage of medicine at some point in the supply chain which may further be an indirect cause of infiltration of counterfeit medicine (Reuters 2012).

2.6 Trust: Trust refers to the belief in the reliability, truthfulness, and integrity of a person, company, or system. In a supply chain context, trust is important for establishing strong relationships between partners and promoting collaboration and cooperation. When partners trust each other, they are more likely to share information, work together to address challenges, and support each other's goals and objectives.

2.7 Publicized shortage: Regulatory bodies publicize about the drug shortages that may provide opportunity for counterfeit/falsified medicine traders. For example, during COVID-19, a few phenomenon observed after the announcement related to the shortage of Remdesivir medicine. One was the hoarding of the medicine, and the other was falsified or counterfeit medicine together with high prices in case the medicine is available.

2.8 Reverse flow: In Pharmaceutical supply chains, In developing countries there are many sustainability issues reported(Kamba et al., 2017). Although, there exist clear guidelines on how to return medicine (Narayana et al., 2014). Still, there exist improper disposal practices. For example, if a Distributer does not have a clear process for managing returns, it may struggle to efficiently handle the volume of goods that are being sent back to them, leading to supply chain disruptions and decreased efficiency. Similarly, a weak reverse flow can lead to increased waste and reduced sustainability, as goods that could be reused or recycled may instead be discarded.

2.9 Information Technology (IT) infrastructure: The relationship between Information Technology (IT) infrastructure and vulnerability in supply chains is complex and interdependent. On one hand, a strong and secure IT infrastructure can provide supply chains with benefits such as increased efficiency, transparency, and resilience(Gu et al. 2021). On the other hand, an IT infrastructure that is poorly designed, maintained, or protected can create vulnerabilities that can be exploited by malicious actors, resulting in supply chain disruptions, data breaches, and other security incidents (Creazza et al. 2021), (Zijian Ao 2020).

3. Methods

Research design of this this research consists of four phases. First phase explores academic and grey literature about vulnerabilities in supply chain. Second phase finalize and categorize vulnerabilities in supply chain after consulting with a number of experts. To check the consistency of the responses, this study adopts kappa statistics with in the second phase of the research. Kappa statistics is favored over other similar methodologies because of its ability to ensure inner consistency and its suitability to measure the agreement and disagreement among the decision. In third phase, study uses TISM based methodology (Madaan and Choudhary 2015), (Sushil 2012).This method is useful to

answer the basic question in research like “what” , “why” “how”. Fourth phase uses MICMAC analysis. Figure 1 represents four phase research methodology that has been used in this research.

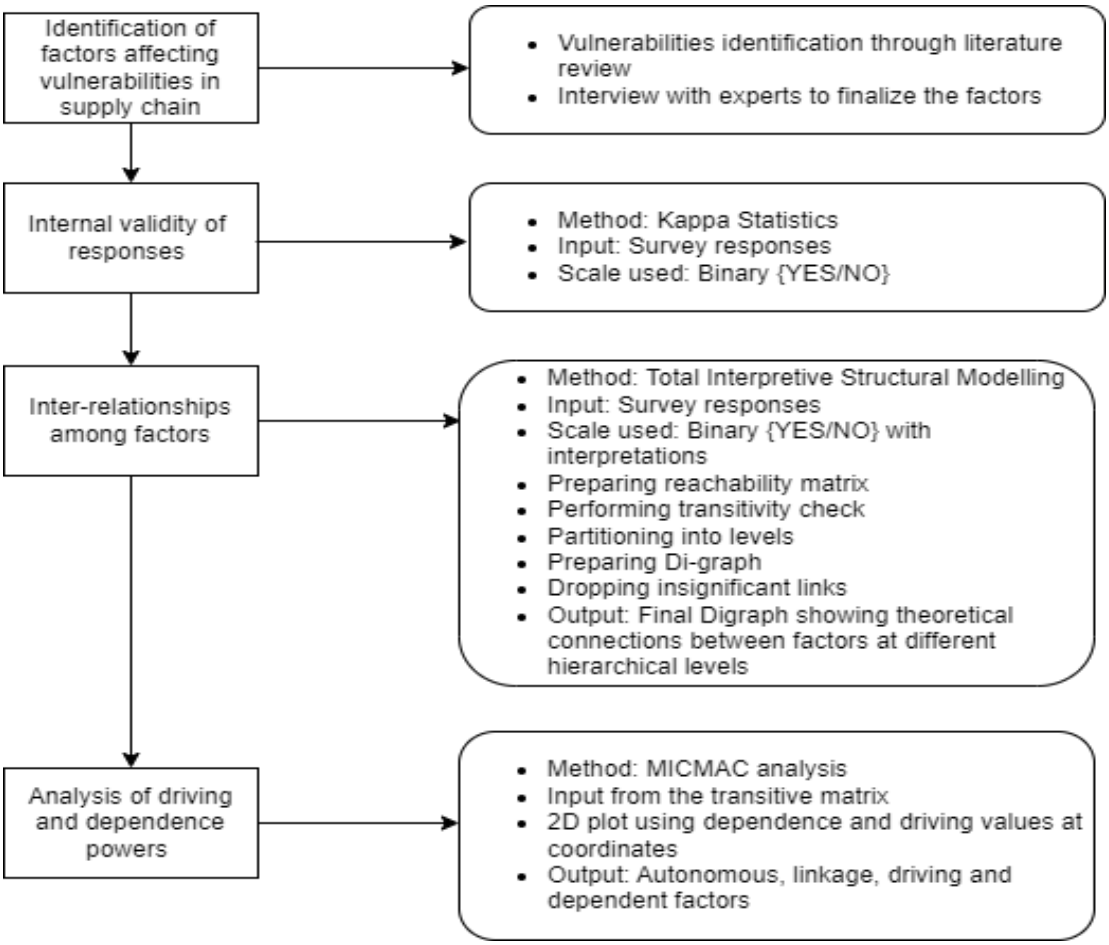

Figure 1. Research framework

4. Data Collection

Data for the research has been collected from various sources: news articles, WHO reports, OECD reports, including academic literature. This collected data has been coded into 15 factors. After that these factors have been reduced to 9 factors. For example, three variables transparency, trackability , traceability has been reduced to information technology infrastructure. The decision of finally chosen 9 factors relevant for the study is an outcome of multiple individual discussions with the 10 experts from Pharmaceutical industry working as supply chain managers. Decision panel suggested improvements in the factors at various stages of research. As represented in Figure 1, a four-phase analysis was followed to draw out various factors that can influence the vulnerability in supply chain.

After that a questionnaire was designed for modelling a TISM based hierarchal relationship model. This include questions that can establish the contextual relationship among selected 9 factors. The contextual relationship was asked as “Does Information technology infrastructure (F9) influences dependence (F2) in the context of vulnerability in supply chain?”. The answers were get collected in “Yes” or “No” to answer “What” with a brief explanation to get the possible answers to “How”. Further, to get internal consistency KAPPA Statistics was used.

5. Results and Discussion

5.1 Numerical Results

Table 2 shows the initial matrix that is developed after analyzing the data from respondents.
The contextual relationship was asked as "Does Information technology infrastructure (F9) influences dependence (F2) in the context of vulnerability in supply chain?". The answers were get collected in "Yes" or "No" to answer "What" with a brief explanation to get the possible answers to "How". To delineate the relationship between factors, four standard symbols have been used (Warfield 1973). The four symbols are V,A.X, and O. one may confuse with the symbols as the same symbols are used for Interpretive structural modelling (ISM). TISM uses the same procedure and symbols as TISM is an extension to ISM in terms of total interpretations for every relationship and even some valid transient relations (Sushil 2012).

Where, V= F_i influences Fj; vice versa in not true; i=1,2,3…,9 represents row and j=1,2,3,…,9 represents column
A= F_j influences F_i; vice-versa is not true;
X= F_i influences F_j; vice-versa is true
O= None of the factors influences each other in the given context

Table 2. Systematic self-interaction matrix

	ITI(F9)	WRF(F8)	PBS(F7)	TRU(F6)	PRT(F5)	SIP(F4)	ACC(F3)	DEP(F2)	VUL (F1)
VUL (F1)	A	A	A	A	A	A	A	A	
DEP(F2)	A	V	V	O	O	V	O		
ACC(F3)	V	V	A	V	V	V			
SIP(F4)	A	V	X	O	O				
PRT(F5)	A	A	A	A					
TRU(F6)	A	A	V						
PBS(F7)	A	O							
WRF(F8)	A								
ITI(F9)									

contextual relationship
V= F1 influnces F2,vice versa is not true
A= F2 influnces F1,vice versa is not true
X =both factors influnces each other
O= none influence each other

*VUL(F1) means vulnerability as factor 1; DEP (dependence); ACC(accountability); SIP(self-interest and power dynamics); PRT (parallel trade); TRU(trust); PBS(publicized shortage); WRF(weak reverse flow); ITI(information technology infrastructure)

Table 3 is just another form of table 2. Table 2 is called reachability matrix (Madaan and Choudhary, 2015). Here. 1 represents an influence while 0 represents no influence in the given context.

Table 3. Reachability matrix

	VUL (F1)	DEP(F2)	ACC(F3)	SIP(F4)	PRT(F5)	TRU(F6)	PBS(F7)	WRF(F8)	ITI(F9)
VUL (F1)	1	0	0	0	0	0	0	0	0
DEP(F2)	1	1	0	1	0	0	1	1	0
ACC(F3)	1	1	1	1	1	1	0	1	1
SIP(F4)	1	0	0	1	0	0	1	1	0
PRT(F5)	1	0	0	0	1	0	0	0	0
TRU(F6)	1	0	0	0	0	1	1	0	1

PBS(F7)	1	0	0	1	0	0	1	0	0
WRF(F8)	1	0	0	0	0	0	0	1	0
ITI(F9)	1	1	0	1	1	1	0	1	1

Final reachability matrix (Table 4) is prepared after checking the transitive relations. A transitive relation is established from a common logic as if A=B and B=C; implies A=C. This exercise establishes those relations clearly that are not directly observable rather they are present die to transitivity and may be important to consider.

Table 4. Final reachability matrix after transitivity check

	VUL (F1)	DEP(F2)	ACC(F3)	SIP(F4)	PRT(F5)	TRU(F6)	PBS(F7)	WRF(F8)	ITI(F9)
VUL (F1)	1	0	0	0	0	0	0	0	0
DEP(F2)	1	1	0	1	0	0	1	1	0
ACC(F3)	1	1	1	1	1	1	1*	1	1
SIP(F4)	1	0	0	1	0	0	1	1	0
PRT(F5)	1	0	0	0	1	0	0	0	0
TRU(F6)	1	1*	0	1*	1*	1	1	1*	1
PBS(F7)	1	0	0	1	0	0	1	1*	0
WRF(F8)	1	0	0	0	0	0	0	1	0
ITI(F9)	1	1	0	1	1	1	1*	1	1

5.2 Graphical Results

Figure 2 represents a vulnerability-capability framework based TISM. This is basically a diagraph representing hierarchical inter-relations among various factors that can affect the vulnerability in supply chain. This model represents factors that may have positive or negative influence on the vulnerability in supply chain. This diagraph is obtained after level partitioning (Patil et al. 2021). In this diagraph thick arrows represents direct relations and dotted arrows represents transitive relations. A few transitive relations with weak justifications have been ignored. Also, as the factors affect vulnerability in supply chain in that sense eight thick arrows should have touch factor F1 at level 1. But to avoid over crowd of arrows they are ignored intentionally. Because in the present context it is understood that all selected factors are to influence vulnerability in supply chain directly.

Results MICMAC analysis are shown in figure 3. It is clear that ensuring accountability(F3) mechanisms can be the most crucial factor to consider while designing resilient supply chain. Furthermore, accountability can affect trust and IT infrastructure. To ensure accountability, IT infrastructure can be a good enabler. A strong and updated IT infrastructure can facilitate greater transparency, traceability, auditability, and visibility (Sunny et al. 2020). All these factors can lead to trust in the supply chain network (Lam et al. 2018).

Dependence (F2) has also come out as a strong factor that can affect vulnerability in supply chain. High levels of dependence on a single supplier or a small number of suppliers can create a sense of vulnerability for the dependent party, which can decrease trust in those suppliers. On the other hand, low levels of dependence can increase trust, as it reduces the risk of supply disruptions (Wells et al. 2017). However, it is important to note that trust and dependence are often intertwined and can influence each other in complex ways in the context of a supply chain.

There is only one autonomous variable that is parallel trade (F5). Autonomous variables do possess weak driving and dependence power. Hence, these variables or factors in the present case can be managed separately. Although, WHO (2010), reports that parallel trade has contributed to vulnerability in supply chain as it becomes the main reason of substandard Avastin, a highly investigated case in USA.

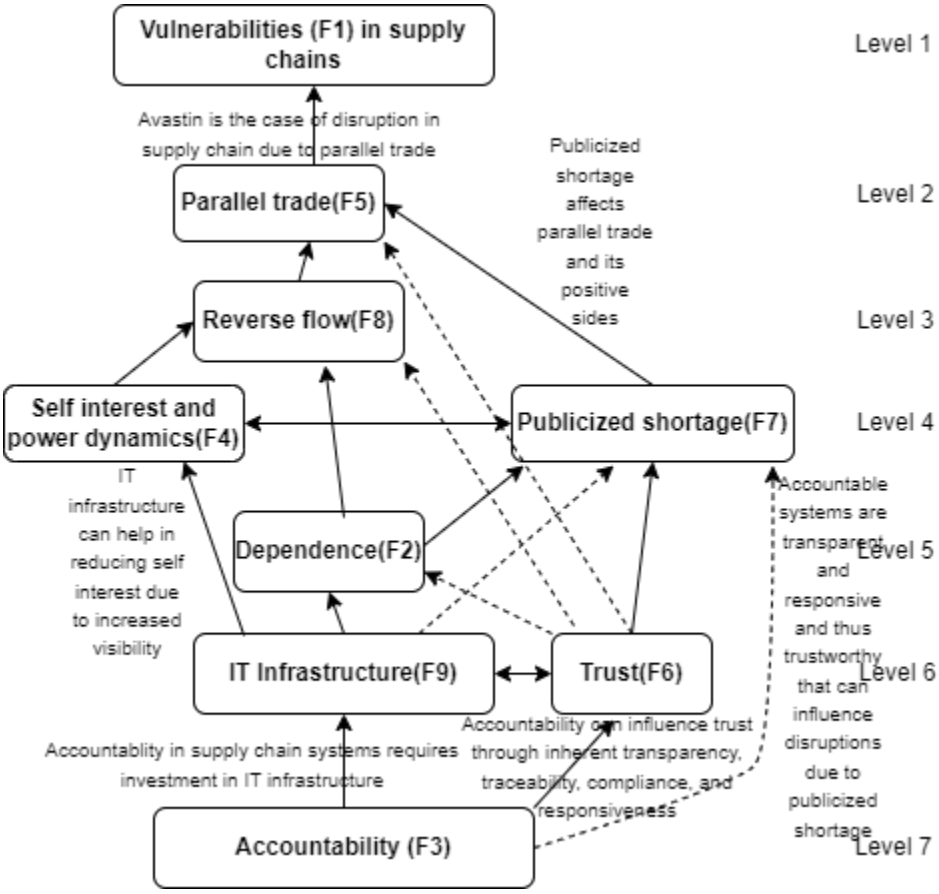

Figure 2. TISM based vulnerability-capability model for supply chain.

However, our analysis brings this to the autonomous category. It can be due to the reason that parallel trade is a legal business. The case of substandard medicine like the case of Avastin, can be mitigated if there exist strong accountability mechanism with the help of strong and updated IT infrastructure. Results of our study are significant in this context, as , for example, US government is planning to enforce Drug Supply Chain Security Act (DSCSA) (Brechtelsbauer et al. 2016).

MICMAC analysis results in zero linkage variables. Linkage variables possess both the driving and dependence powers and therefore becomes difficult to manage. Although, Self-interest and power dynamics (F4) is tending towards the linkage variable zone.

Finally, vulnerability (F1) is the clear dependent variable. These variables will get managed automatically if one focuses on the driving variables.

5.3 Validation

The proposed hybrid TISM-MICMAC based vulnerability-capability framework was shown to the experts and their feedbacks were considered. This was done to ensure the external validity of the model. Furthermore, for the external validity t-test can be applied to the model. For the internal validity kappa statistics have been used (Patil et al. 2021). Adding to this to check the consistency of the method employed, Sushil, (2018) has been followed.

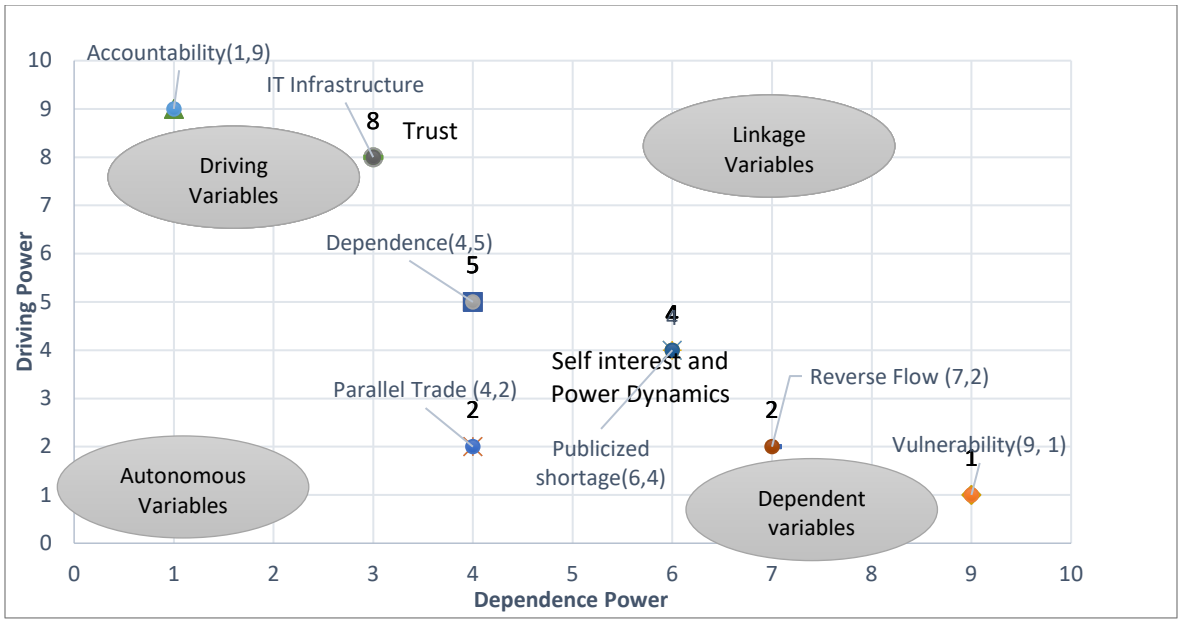

Figure 3. MICMAC analysis of the vulnerability-capability framework

5.4 Managerial implications and contributions

Managers may find it difficult to manage vulnerabilities in supply chain. This research proposes a very simple easy to understand hierarchical relationship between the factors that may affect a supply chain in a negative or positive manner. For example, this model proposes that accountability is the key requirement to manage to avoid exposure of the supply chain to disruptions. In this way, this research supports various research works (Kamba et al. 2017), (Lederman et al. 2005), (Mackey 2019), (Mackey et al. 2020), (Nunes-Vaz et al. (2019).

As it is clear from the TISM model and MICMAC analyses that accountability (F3), IT infrastructure(F9), trust (F6) and dependence (F2) are the important factors that has to be managed to avoid exposure of supply chains to the disruptions and hence making supply chains sustainable to the uncertain business environments.

According to proposed model, accountability can influence information technology (IT) infrastructure in the context of vulnerability in the supply chain. For example, when suppliers and transportation providers are held accountable for the security and reliability of their IT systems, they are more likely to invest in robust IT infrastructure and to implement effective cybersecurity measures. This can reduce the risk of cyber-attacks, data breaches, and other IT-related disruptions, and increase the visibility and communication in the supply chain, reducing its vulnerability (Chowdhury et al. 2022).

On the other hand, when suppliers and transportation providers are not held accountable for their IT systems, they may not invest in adequate IT infrastructure or implement effective cybersecurity measures, resulting in increased vulnerability in the supply chain. In such cases, the risk of IT-related disruptions increases, and the supply chain may suffer from lack of visibility and communication, making it difficult to identify and respond to potential risks and disruptions (Chowdhury et al. 2022). Therefore, accountability can play an important role in reducing vulnerability and increasing resilience in supply chain.

Trust(F6) has come out as an important factor that influence many relational and operational facets in supply chain (Sahay 2003). Sometimes, managers may find it difficult to decide whether to invest in IT infrastructure; what effect does it bring to the supply chain. Our research proposes a simple relation that IT infrastructure and trust go hand in hand. This result supports the previous works (Hua and Notland 2016), (Laeequddin et al. 2010), (Salam 2017).

Trust refers to the belief in the reliability, integrity, and good intentions of others in the supply chain (Capaldo and Giannoccaro 2015). Trust is built through consistent, reliable performance, transparency, and open communication (Fawcett et al. 2012).

6. Conclusions, limitations, and future directions

In present times, to maintain resilience of supply chains, it is important for supply chain mangers to understand the possible interplay between various factors that can affect the vulnerabilities in supply chain. To achieve this objective, this research proposes a vulnerability- capability framework that is based on TISM-MICMAC methodology. Data were collected from Academic literature and grey literature. Proposed factors were finalized with the help of inputs from the area experts (academic and practitioners). The results indicate that accountability (F3), Trust(F6), Dependence (F2), and IT infrastructure (F9) can play significantly important role in the resilient supply chains. These are relational (Trust, dependence), operational (accountability), and technological (IT Infrastructure) factors that forms the foundation for resilient supply chain.

Similar to all research, this research too has limitations, for example, sample size and selection. Also, in the external validation part t- test can be considered statistically more significant. Also, polarities of the effects of factors have not been considered which can be a future avenue for research. For this purpose, researchers can follow Sushil (2018b).

References

Barnes, P., and Oloruntoba, R., Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management, *Journal of International Management*, vol. 11, no. 4, pp. 519–540, 2005.

Bourantas, D., Avoiding dependence on suppliers and distributors, *Long Range Planning*, vol.22 no.3, pp. 140–149, 1989.

Brechtelsbauer, E. D., Pennell, B., Durham, M., Hertig, J. B., and Weber, R. J., Review of the 2015 drug supply chain security act. *Hospital Pharmacy*, vol. 51, no.6, pp. 493–500, 2016.

Capaldo, A., and Giannoccaro, I., How does trust affect performance in the supply chain? the moderating role of interdependence, *International Journal of Production Economics*, vol.166, no. xx, pp. 36–49, 2015.

Chowdhury, S., Rodriguez-Espindola, O., Dey, P., and Budhwar, P., Blockchain technology adoption for managing risks in operations and supply chain management: evidence from the UK, *Annals of Operations Research*, vol. xx, no. xx, pp. 1-36, 2022.

Creazza, A., Colicchia, C., Spiezia, S., and Dallari, F., Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era, *Supply Chain Management*, vol. 27, no. 01, pp. 30-53, 2022.

El Mokrini, A., Dafaoui, E., Berrado, A., and El Mhamedi, A., An approach to risk Assessment for Outsourcing Logistics: Case of Pharmaceutical Industry, *IFAC-PapersOnLine*, vol. 49, no. 12, pp. 1239–1244, 2016.

Fawcett, S. E., Jones, S. L., and Fawcett, A. M., Supply chain trust: The catalyst for collaborative innovation, *Business Horizons*, vol. 55, no. 2, pp. 163–178, 2012.

Gu, M., Yang, L., and Huo, B., The impact of information technology usage on supply chain resilience and performance: An ambidexterous view, *International Journal of Production Economics*, vol. 232, no. xx, pp. xx, 2021.

Kamba, P. F., Ireeta, M. E., Balikuna, S., and Kaggwa, B., Threats posed by stockpiles of expired pharmaceuticals in low- and middle-income countries: A Ugandan perspective. *Bulletin of the World Health Organization*, vol. 95, no. 8, pp. 594–598, 2017.

Laeequddin, M., Sahay, B. S., Sahay, V., and Waheed, K. A., Measuring trust in supply chain partners' relationships, *Measuring Business Excellence*, vol. 14, no. 3, pp. 53–69, 2010.

Lam, T., Heales, J., Hartley, N., and Hodkinson, C., Information transparency matters in relation to consumer trust in food safety, *ACIS 2018 - 29th Australasian Conference on Information*

Systems, pp. 1–12, Sydney, Australia, Feb 2-5, 2018.

Lederman, D., Loayza, N. V., and Soares, R. R., Accountability and corruption: Political institutions matter, *Economics and Politics*, vol. 17, no.1, pp. 1–35, 2005.

Mackey, T. K., Opening the policy window to mobilize action against corruption in the health sector: Comment on "We need to talk about corruption in health systems, *International Journal of Health Policy and Management*, vol.*8, no.* 11, pp. 668–671, 2019.

Mackey, T. K., Cuomo, R. E., and Mackey, T. K., An interdisciplinary review of digital technologies to facilitate anti-corruption , transparency and accountability in medicines procurement anti-corruption , transparency and accountability in medicines procurement, *Global Health Action*, vol.13, no. 1, pp. 1-13, 2020.

Madaan, J. K., and Choudhary, D., A Flexible Decision Model for Risk Analysis in Product Recovery Systems, *Global Journal of Flexible Systems Management*, vol. *16, no.*4, pp. 313–329, 2015.

Mark Stevenson and Jerry Busby, An exploratory analysis of counterfeiting strategies, *International Journal of Operations and Production Management*, vol. 35, no. 1, pp. 110–144, 2015.

Marucheck, A., Greis, N., Mena, C., and Cai, L., Product safety and security in the global supply chain: Issues, challenges and research opportunities, *Journal of Operations Management*, vol. *29, no.*7, pp. 707–720, 2011.

Moktadir, M. A., Ali, S. M., Mangla, S. K., Sharmy, T. A., Luthra, S., Mishra, N., and Garza-Reyes, J. A. (2018). Decision modeling of risks in pharmaceutical supply chains. *Industrial Management and Data Systems*, vol. 118, no.7, pp. 1388–1412, 2018.

Narayana, S. A., Elias, A. A., and Pati, R. K., Reverse logistics in the pharmaceuticals industry: A systemic analysis, *International Journal of Logistics Management*, vol. 25, no.2, pp. 379–398, 2014.

Nguyen, X. H., Le, T. A., Nguyen, A. T., Pham, T. T. H., and Tran, T. H., Supply chain risk, integration, risk resilience and firm performance in global supply chain: Evidence from vietnam pharmaceutical industry, *Uncertain Supply Chain Management*, vol. *9, no.* 4, pp. 779–796, 2021.

Nunes-Vaz, R., Arbon, P., and Steenkamp, M., Imperatives for health sector decision-support modelling, *International Journal of Disaster Risk Reduction*, vol. 38, no. xx, pp. xx, 2019.

Patil, A., Shardeo, V., and Madaan, J., Modelling performance measurement barriers of humanitarian supply chain, *International Journal of Productivity and Performance Management*, vol. 70, no. 8, pp. 1972–2000, 2021.

Peck, H., Drivers of supply chain vulnerability: an integrated framework. *International Journal of Physical Distribution and Logistics Management*, vol. 35, no. 4, pp. 210–232, 2005.

Pettit, T. J., Croxton, K. L., and Fiksel, J., Ensuring Supply Chain Resilience : Development and Implementation of an Assessment Tool, *Journal of Business Logistics*, vol. 34, no. 1, pp. 46–76, 2013.

Pettit, T. J., Fiksel, J., and Croxton, K. L., Ensuring supply chain resilience: development of a conceptual framework, *Journal of Business Logistics*, vol. 31, no. 1, pp . 1–21, 2010.

Sahay, B. S., Understanding trust in supply chain relationships, *Industrial Management and Data Systems*, vol. 103, no.8–9, pp. 553–563, 2003.

Salam, M. A., The mediating role of supply chain collaboration on the relationship between technology, trust and operational performance: An empirical investigation, *Benchmarking*, vol. 24, no. 2, pp. 298–317, 2017.

Sunny, J., Undralla, N., and Madhusudanan Pillai, V., Supply chain transparency through blockchain-based traceability: An overview with demonstration, *Computers and Industrial Engineering*, vol. 150, no. xx, pp. 1- 13, 2020.

Sushil, Interpreting the interpretive structural model, *Global Journal of Flexible Systems Management*, vol. *13, no.* 2, pp. 87–106, 2012.

Sushil, Modified ISM/TISM process with simultaneous transitivity checks for reducing direct pair comparisons, *Global Journal of Flexible Systems Management*, vol. 18, no. 4, pp. 331–351, 2017.

Sushil, How to check correctness of total interpretive structural models? *Annals of Operations Research*, vol. 270, no. 1–2, pp. 473–487, 2018a.

Sushil, Incorporating polarity of relationships in ISM and TISM for theory building in information and organization management, *International Journal of Information Management*, vol. 43, no. xx, pp. 38–51, 2018b.

Svensson, G., A conceptual framework for the analysis of vulnerability in supply chains, *International Journal of Physical Distribution and Logistics Management*, vol.30, no. 9, pp. 731–750, 2000.

Svensson, G., A typology of vulnerability scenarios towards suppliers and customers in supply chains based upon perceived time and relationship dependencies, *International Journal of Physical Distribution and Logistics Management*, vol. 32, no. 3, pp.168–187, 2002.

Svensson, G., Key areas, causes and contingency planning of corporate vulnerability in supply chains: A qualitative approach, *International Journal of Physical Distribution and Logistics Management*, vol. 34, no. 9, pp. 728–748, 2004.

Wagner, S. M., and Bode, C., An empirical investigation into supply chain vulnerability, *Journal of Purchasing and Supply Management*, vol. 12, no. 6, pp. 301–312, 2006.

Warfield, J. N., Intent Structures, *IEEE Transactions on Systems, Man and Cybernetics*, vol.*3, no.* 2, pp. 133–140, 1973.

Wells, C. V, Kipnis, D., and Wells, C. V., *journal of business and psychology trust , dependency , and control in the contemporary organization,* vol.*15, no.* 4, pp. 593–603, 2017.

WHO, *Working document WHO/ACM/ draft preliminary draft survey on national legislation on counterfeit medicines, 1 4 May , 2010.*

Zhao, G., Liu, S., Lopez, C., Chen, H., Lu, H., Mangla, S. K., and Elgueta, S., Risk analysis of the agri-food supply chain: A multi-method approach, *International Journal of Production Research*, vol. *58, no.* 16, pp. 4851–4876, 2020.

Zijian, Z., and Ao, L., Network vulnerability and the coordination mechanism of cyber supply chain security resilience investment, *Journal of Industrial Engineering and Engineering Management*, vol. *34, no.* 5, pp. 130–136, 2020.

Biography

Vikrant Giri is presently a Research Scholar in the Department of Management Studies, Indian Institute of Technology Delhi, New Delhi. He is a Gold Medalist and has presented his previous works at various National and international conferences. His area of interest includes resilient and sustainable supply chain; health care supply chain, and blockchain operations. He has been awarded for best paper for the most outstanding paper in International Conference on Recent Innovations in Science, Technology, Management and Environment held at Indian Federation of United Nations Associations, New Delhi, India. He has recently started reviewing for journals of repute.

Prof Jitender Madaan received his B.Tech Degree in Production and Industrial Engineering from M.B.M Govt. Engg College, Jodhpur (JNV University), India, and obtained his M. Tech in Manufacturing System Engg. from Department of Mechanical Engg. MREC (Now MNIT), Jaipur and PhD in Mechanical Engineering from the Indian

Institute of Technology (IIT) Delhi, India. Prior joining IIT Delhi, Dr. Madaan has many years of working experience in other universities including IIT Roorkee; GGSIP University Delhi. His current research interests are Reverse Logistics and Supply Chain Management, Sustainable Operations Management, Production Management, information and governance effectiveness, Systems Modelling and Simulation, etc. To date, Dr. Madaan has published over 4 book chapters, over 25 refereed international journal papers and 48 peer reviewed international conference papers. He is a reviewer of several international journal of repute.

Prof Nikhil Varma is an Associate Professor at Ramapo College of New Jersey. He has a Bachelor of Computer Engineering from Birla Institute of Technology, Mesra, India and a master's in computer engineering from Concordia University, Montreal, Canada. He also has an MBA from HEC Montreal and completed his PhD in Management from the same university. Nikhil is also a guest professor in IIT, Delhi and Molde University, Norway where he teaches Supply Chain Analytics and Blockchain related courses.Nikhil is currently working as a Web 3.0 subject matter expert (cannonball) at AlgoBharat, a partner to Algorand Foundation. One of the objectives of AlgoBharat is to help in the diffusion of Blockchain in India leveraging the India stack.
Prior To academics, Nikhil Varma spent time in the industry as a developer, analyst, management consultant and a project manager. He was also an Entrepreneur and started two companies. He was in the board of a public company that acquired his startup.Nikhil is passionate about optimizing operations and using machine learning to develop efficient delivery platforms. He teaches Blockchain to Managers and has given lectures at several institutions and conferences on institutionalization Blockchain. He has co-founded a community based EdTech company that uses to power of community to rapidly develop content and disrupt the education market.