Indian Public Policy Review 2023, 4(4): 70-83
https://doi.org/10.55763/ippr.2023.04.04.003

IPPR

Defining Strategic and Critical Vulnerabilities in Asymmetrical Trade Interdependence

Amit Kumar*

Abstract

As the world becomes more economically integrated, a complex web of asymmetric interdependences has emerged, allowing some states to wield disproportionate economic power. Consequently, recourse to economic coercion as a tool for compellence, deterrence, or co-optation has become much more frequent in current times. Debates around dependence-induced strategic and critical vulnerabilities have thus gained traction with an end objective to reduce or mitigate them. But a lack of conceptual framework underpinning the ideas of dependence, vulnerabilities, and strategic and critical vulnerabilities plagues the present decision-making apparatus, which runs the risk of treating subjects under each of these categories as synonymous. To prevent a one-size-fits-all approach emanating from the lack of conceptual differentiation, this paper presents a framework, in the form of a series of tests, to understand whether trade in a certain commodity between countries can be classified as a critical vulnerability.

Keywords: Dependence, Asymmetric-Interdependence, Strategic Vulnerability, Critical Vulnerability, Decoupling, De-risking, Trade, India-China

Publication Date: 09 August 2023

* Amit Kumar is a Research Analyst with the Indo-Pacific Studies Programme at the Takshashila Institution.

1. Introduction

In a world characterised by anarchy, states pursue goals based on their respective national interests. However, their relative capabilities (power) to meet those ends differ, thereby giving rise to a hierarchical structure to this anarchic global order. Military capabilities are a conventional tool of coercion, employed by states to pursue national interests in this global order. However, as the world has become deeply integrated, deploying the military option has become more challenging, owing to the increased cost associated with it.

Instead, in the world of complex but asymmetric interdependence, some states have acquired a dominating position owing to their differential capabilities in the international economic order. The differential capabilities of states to influence the dynamics of international trade have encouraged dominant trading countries to weaponise their advantages vis-à-vis dependent countries. The intensification of great power rivalry has further led to the deployment of coercive economic tools and the exploitation of economic dependencies to gain favourable political outcomes.

The anxiety and paranoia with respect to weaknesses arising from asymmetrical interdependence have been such that the term 'dependency' has become synonymous with 'vulnerability'. The conflation of the two terms runs the risk of viewing all forms of economic dependence as undesirable, with vulnerability seen as a definite (rather than potential) outcome thereof.

This leaves policymakers susceptible to approaching the issues of asymmetrical interdependence with a one-size-fits-all mindset. There exists a gap in our understanding of when interdependence becomes dependence, and when dependence gives way to vulnerability. Therefore, the need arises for a framework to distinguish and define the two terms conceptually.

This paper attempts to address this gap, defining strategic vulnerabilities arising out of asymmetrical interdependence or dependence in the context of international trade. The first section of the paper reviews some of the existing definitions of vulnerabilities detailed in supply chain management (SCM) literature. The second section proposes a framework to define strategic vulnerabilities, that can be uniformly applied by countries, to differentiate them from non-strategic vulnerabilities. It also provides a framework to distil a subset of strategic vulnerabilities - critical vulnerabilities. The paper concludes with a brief advisory note for readers and a discussion of the scope of future outputs.

2. Risk and Vulnerabilities through Supply Chain Management Literature

Before proposing a framework for our specific need, it would be pertinent to delve into some of the pre-existing definitions and frameworks underpinning risks and vulnerabilities, as viewed in supply chain management (SCM) literature.

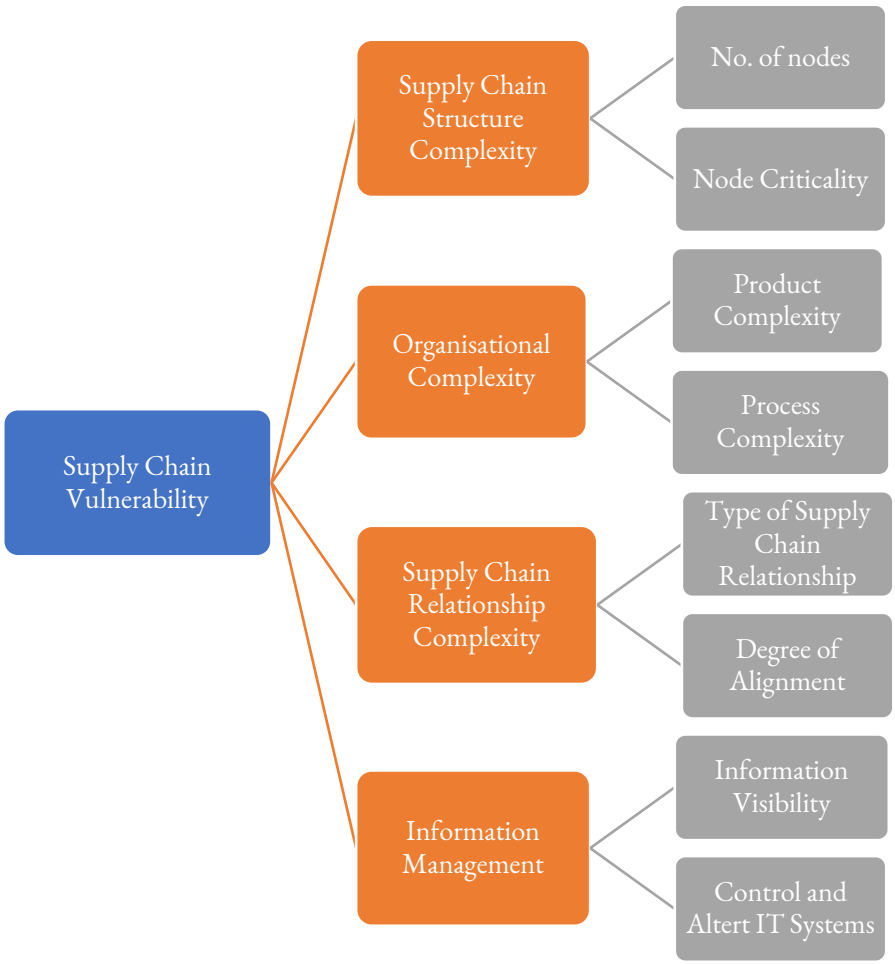
A preliminary review indicates that most of the existing SCM literature identifies factors such as natural disasters, operational difficulties, terrorist activities, volatility in demand and supply,

centralised distribution systems, outsourcing, and even globalisation as sources of supply chain vulnerability.

Sharma et al. (2021), in their paper titled *Supply Chain Vulnerability Assessment for Manufacturing Industry,* have carried out an extensive review of the SCM literature as well as interviews with experts in the manufacturing industry to identify 26 supply chain vulnerability (SCV) factors (Sharma, Srivastava and Kumar, 2023). The authors have simplified and streamlined these factors into four broad categories. This serves as a single-point source to understand how the idea of vulnerabilities and risks is viewed in the SCM literature.

At the outset, the paper differentiates supply chain risks from supply chain vulnerability. It defines vulnerability as "*design and process factors that may increase the exposure to different kinds of internal and external risks in the supply chain*" (Sharma, Srivastava and Kumar, 2023). In this sense, "vulnerability is used to measure the sensitivity of a supply chain to these disturbances". In other words, "risk is the *outcome* (always negative in case of supply chain disruptions) and vulnerability is a *driving force* that leads to risk in the supply chain." Lastly, "SCV is a precondition to supply chain risks" (Sharma, Srivastava and Kumar, 2023). [Emphasis added.]

Diagram 1: Illustrates the supply chain vulnerability driver model



As can be seen, the authors have outlined two metrics each to measure the four vulnerability drivers (Sharma, Srivastava and Kumar, 2023). The drivers and their respective metrics are further explained in detail below.

1. Supply Chain Structure Vulnerability drivers

   a) **Number of nodes:** It refers to the "number of alternative suppliers for a particular component." This metric suggests that chain complexity increases with an increase in the number of nodes, while also enhancing the resilience of the supply chain, and vice-versa.

   b) **Node Criticality:** It refers to the "number of linkages emerging out and merging in from a particular node. For a particular node, if the number of linkages coming in is more than the number of linkages going out, the node becomes vulnerable." It is so because any disruption in the demand from the customer will lead to substantial losses.

2. Organisational Complexity Vulnerability Drivers

   a) **Product complexity**: It refers to "the number of parts and components needed to produce a product." The underlying idea here is that supply chain vulnerability increases with the complexity of the product design.

   b) **Process complexity**: It takes into account both manufacturing and business process complexity. Factors like the number of bought-out components, product life cycle, variety of products, manufacturing lead time, and production process types increase manufacturing process complexity; long process lead time and high decision-making points increase business process complexity. The higher the complexity, the higher the vulnerability.

3. Supply Chain Relationship Vulnerability Drivers

   a) **Type of supply chain relationship**: This factor takes into account the existence of "active relationships and integration across different levels of the supply chain" to assess vulnerabilities. The lack of stronger and collaborative relationships among the supply chain stakeholders leads to increased vulnerability.

   b) **Performance measure alignment**: The metric seeks to measure the degree to which the performance (effectiveness) of an individual unit in a supply chain is aligned to other units within the supply chain. The underlying principle here is that a supply chain is as strong or vulnerable as the weakest link in the supply chain.

4. Information Management Vulnerability Driver

   a) **Information visibility:** This metric recognises that transparency and the free flow of information enhance the supply chain's resilience. Thus, a lack of access to key information (information asymmetry) increases the chances of its weaponisation by

actors that are privy to such information, leading to increased vulnerability in a supply chain.

b) **Detection and Control Mechanism:** It emphasises that the ability to detect and control supply chain vulnerabilities reduces the vulnerabilities and risks in a supply chain, and vice versa. Thus, the lack of statistical quality control techniques and inspection, forecasting tools, Enterprise Resource Planning (ERP), Material Requirements Planning (MRP), etc. contribute to increased supply chain vulnerability.

Another helpful framework to assess vulnerabilities in international trade is offered by Reiter and Stehrer (2021), which examines the following five components:

1. **Outdegree Centrality**: Seeks to detect the presence of a central player, i.e., a country that exports to many countries and has a high market share in the importing countries.
2. **Tendency to Cluster**: Takes into account the tendency among trading countries (exporting and importing) to form trade clusters. Formation of clusters is a severe vulnerability, as any disruption within the cluster could have devastating effects on individual countries within the cluster.
3. **International Substitutability**: Looks for substitutability of the trading product
4. **Hirschmman-Herfindahl Index**: Captures the situation when an importer country is dependent on just a few exporting countries, meaning that the market concentration among the exporting countries is high.
5. **Non-tariff measures**: Seeks to identify products most frequently subject to non-tariff barriers.

2.1 Limitations of the existing frameworks

While the reviewed literature provides comprehensive frameworks to assess vulnerabilities in a supply chain and international trading, it does not fully satisfy the objective set out in this paper, i.e., identifying strategic vulnerabilities arising out of asymmetrical interdependence between two trading countries. Furthermore, the above-discussed frameworks suffer from six key limitations as they fail to take into account the following:

Geopolitical motivations: The discussed frameworks do not take into account geopolitical motivations, i.e., the willingness of an actor to weaponise trade or economic dominance for political ends.

Country-wide perspective: The above-discussed frameworks view risks and vulnerabilities primarily from the perspective of firms. They fail to distinguish between business interests and national interests. In other words, they do not take into account that what might constitute a vulnerability for a few firms might not be a vulnerability for the country as a whole. For instance, a vulnerability for a firm that sources close to 50% of its supplies from a single source country may not

be a vulnerability for a country if that source accounts for less than 6% of the country's total imports of that particular product. Factors that might make a firm vulnerable might not lead to strategic vulnerabilities for a country.

Utility/Value of the product traded: The discussed frameworks do not make a distinction between vulnerabilities based on the utility/value of the product. For instance, what might constitute a vulnerability for a business engaged in the import of toys might not be a vulnerability of strategic significance for a country. Likewise, a disruption in the import of luxury furniture may not be a vulnerability for a country.

Consequence of disruption: The discussed frameworks also do not take into account the scale of impact that a disruption in the trade of a commodity/service would unleash while identifying vulnerabilities. Not all vulnerabilities might have an impact on a significant scale to render a country strategically vulnerable.

Latent Capability to Replace Supplies: While the above frameworks account for alternatives or substitutability, they do not take into account the potential or latent capabilities to fill in the demand-supply gap, even in cases where alternatives are unavailable. Consider, for example, the manufacturing of masks in India: When the pandemic hit, India did not produce enough masks for its population and was initially dependent on imports from China, but when supplies from China were disrupted, India quickly evolved into one of the largest mask-producing countries and even began exporting these to other countries. Here, while the alternative did not exist at the moment of the crisis, capabilities existed to quickly ramp up production and meet the burgeoning demand.

Dependency is not vulnerability: Lastly, existing frameworks view concentration as an outright vulnerability, which corresponds to the prevailing idea that dependence necessarily implies vulnerability. However, concentration and dependence as a consequence need not necessarily imply vulnerability when it comes to states.

Overall, the existing frameworks essentially approach supply chain vulnerabilities from an enterprise perspective, and do not deal with the issue of strategic vulnerabilities for states. While they do provide valuable insights, a state's framework for risks and vulnerabilities needs to be different from that of businesses. This is what we attempt to do in the following section.

3. A Framework to Assess Dependence, Vulnerability, Strategic Vulnerability and Critical Vulnerability

To begin with, it is worthwhile to briefly define the concept of dependence. In the context of international trade, dependency could be described as a situation wherein a country depends on a foreign entity to meet a substantial share of its supply needs. A dependency could arise out of broadly three factors: geography, economy, and technology.

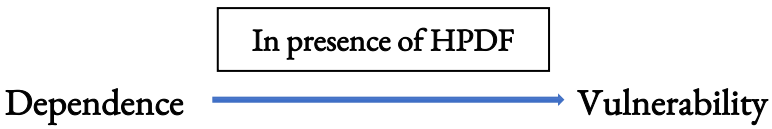
Geography/Resource Endowment: A case in point would be India's dependence on crude oil imports for its energy needs. Only a select few countries have petroleum reserves large enough to export them to the outside world and meet global demand.

Comparative Advantage: Dependency could also arise because of pure economics, i.e., when an entity has acquired a comparative advantage over other players. For instance, China's capabilities with respect to low-end manufacturing over the past few decades, or its current advantages with regard to assembling electronic equipment.

Technological Capabilities: Technology serves as the third source of dependency. It might be the case that only certain entities possess the technical competence to produce a sophisticated commodity, that competitors cannot match. Such capabilities take decades of capital investment, manpower training, industrial innovation and experience. The evolution of ASML and TSMC in the chip value chain or Airbus and Boeing in commercial airplane manufacturing are examples.

Besides, it is important to recognise that dependency could also be reciprocal or mutual. An exporting entity can be as dependent as an importing entity if the latter is a huge market for the former.

But dependence by itself should not be seen as a vulnerability. A case of dependence is of mutual interest to the two trading parties. However, if a case of dependence is accompanied by high-probability disruptive factors that make the relationship unreliable, it can be termed as a vulnerability. For instance, a case of dependence becomes a vulnerability if it is susceptible to frequent tariff or non-tariff barriers, supply shocks and disruptions, natural calamities, information asymmetry, and other factors that make dependence untenable. Thus, so long as a dependency is founded on relatively strong supply chain management basics, it need not be viewed as a vulnerability, because reducing dependency otherwise could lead to increased economic cost and reduced productivity. Thus, dependency-induced vulnerability can be imagined as:



Similarly, for a case of dependency to be termed as a strategic vulnerability, it needs to be tested against multiple parameters. To address this question, this paper proposes the following framework in the form of a four-stage test to determine whether a dependency amounts to strategic vulnerability.

3.1 The Strategic Vulnerability Test

In this four-stage test, for any dependency to be termed as a strategic vulnerability, it must pass the first two tests (adversary and alternative) and at least one of the last two tests (incidence or cascading).

1. The Adversary Test

So long the strategic interest of a trading partner does not (or is not likely to) outweigh the mutual economic interest in an interdependence, dependence cannot be termed as a strategic vulnerability.

To account for this factor, the adversary test becomes imminent as strategic interests are most likely to triumph over mutual economic interest when the dependency is vis-a-vis an adversary. An adversary would harbour a geopolitical motive to weaponise trade or resort to economic coercion to extract favourable outcomes.

The existence of an adversary relationship can vary with time. It is up to governments to categorise each other as adversaries / non-adversaries. Also, while applying the adversary test, governments have to be mindful of accounting for 'extended adversaries' - trading partners that are most susceptible to one's adversary's pressure.

2. The Test of Alternatives

While examining a dependency vis-a-vis an adversary against the test of alternatives, if any of the three case scenarios emerge, it could amount to a strategic vulnerability.

Case 1: Dependency vis-a-vis an adversary is a result of an absence of alternatives (either source or product)

Case 2: Alternatives are available, but the scale is so large that it cannot be entirely met by others in the short run.

Case 3: Alternatives are available, but the 'switching cost' is too high

In each of the above cases, the disruption is likely to be so severe that supply cannot be revived even with increased expenditure. This sort of disruption will certainly bring about a halt in production activity or sales. Example: China's imposition of sanctions on solar panels and lithium batteries can hurt India's ambitions in the renewable energy or electric vehicle sectors.

The last two tests can be mutually exclusive depending on whether the product in question is an end product/finished good/service or intermediate good/service. In specific cases, both tests may apply. Thus, any case of dependency after having passed the first two tests, must clear at least one of the following two tests.

3. The Test of Incidence

This test seeks to measure the impact of disruption on the general population. Any dependency vis-a-vis an adversary that *clears* the 'alternative test' can yet not be classified as a strategic vulnerability unless its impact on the wider population is taken into account. Two parameters need to be satisfied in this regard:

1. Assessing the section of the population affected: If the consumption pattern of a significantly large population is impacted, a dependency vis-a-vis an adversary that has failed the alternative test is a potential strategic vulnerability. For instance, a 40% dependency on 'Made in China' electronics that cater to the needs of almost the entire consumer class is a strategic vulnerability for India. On the contrary, if the consumption pattern of only a minuscule percentage of the

population is impacted, a dependency on an adversary even to the tune of 100%, despite being an irritant, cannot be classified as a strategic vulnerability. For instance, an 80% dependency on a luxury item, catering to less than one percent of the consumer class.

2. Assessing the product's utility for the population: This parameter would take into account the utility of the product and the impact of any disruption on the lives of the people and the functioning of public utilities. Thus, by this standard, any form of dependency on an adversary relating to the import of products such as soft toys, idols, and decoratives cannot be classified as a potential strategic vulnerability. On the other hand, dependency on an adversary vis-a-vis drugs (vaccines), oilseeds, laptops, and smartphones would amount to a strategic vulnerability.

For instance, India's dependence on Chinese imports for electronics and medical equipment and devices satisfies both parameters and thus, amounts to potential strategic vulnerability given it clears the first two tests as well.

4. The Test of Cascading Effect

This test seeks to assess the cascading effect of the weaponisation of a dependency by an adversary on other domestic sectors, within the supply chain or beyond. This is not a compulsory test, but an additional one to determine the severity and degree of a strategic vulnerability. A plausible example could be India's dependency on China for Active Pharmaceutical Ingredients (APIs). The fact that India sources more than 60% of its API supplies from China means that any disruption or weaponisation in this segment would severely restrict India's capability on two fronts. One, it would severely curtail India's generic medicine manufacturing, and two, it would dent its status as the pharmacy of the world, thereby also jeopardising the medical tourism industry.

3.2 The Critical Vulnerability Test

Having devised a framework to distinguish strategic vulnerabilities from the concept of risk, vulnerabilities, and dependence in general, it is also important to underline that not all strategic vulnerabilities are similar. Some strategic vulnerabilities may be of a more severe or critical nature than others. Depending upon the severity of the challenge they pose, a different approach might be needed to deal with them.

For this reason, this paper further seeks to delineate critical vulnerabilities from the pool of strategic vulnerabilities. In this sense, critical vulnerabilities are a subset of strategic vulnerabilities.

Two additional tests could be applied to a strategic vulnerability to determine whether it qualifies as a critical vulnerability. These tests would supplement and follow the four-stage test mentioned above.

1. National Security Threat

Case of strategic vulnerabilities that pose a direct threat to national security and can offer adversaries disproportionate leverage. For example, dependence on the adversary's investments or technology in electricity grids, communications, and satellites, banking & finance, digital infrastructure, and all Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR) related sectors can be termed critical vulnerabilities, as these sectors are then highly susceptible to cyber-attacks. Any exploitation of such vulnerabilities even through a short-term disruption can significantly undermine national security and thereby influence decisions that affect the national interest.

Here it is necessary to point out that India's dependence on Russia for spares and serviceability of the Russian-origin inventory of weapons amounts to a critical vulnerability owing to the deepening China-Russia relationship. The case of India's dependency meets the adversary test given the growing strategic alignment between China and Russia. The case also fails the alternative test because India currently operates a large inventory of Russian-origin weapon systems, which makes it dependent upon Moscow for spares and serviceability requirements. In light of the absence of any alternatives, this case of dependency on Russia for spares becomes a critical vulnerability, as it could have implications for national security during a conflict with China.

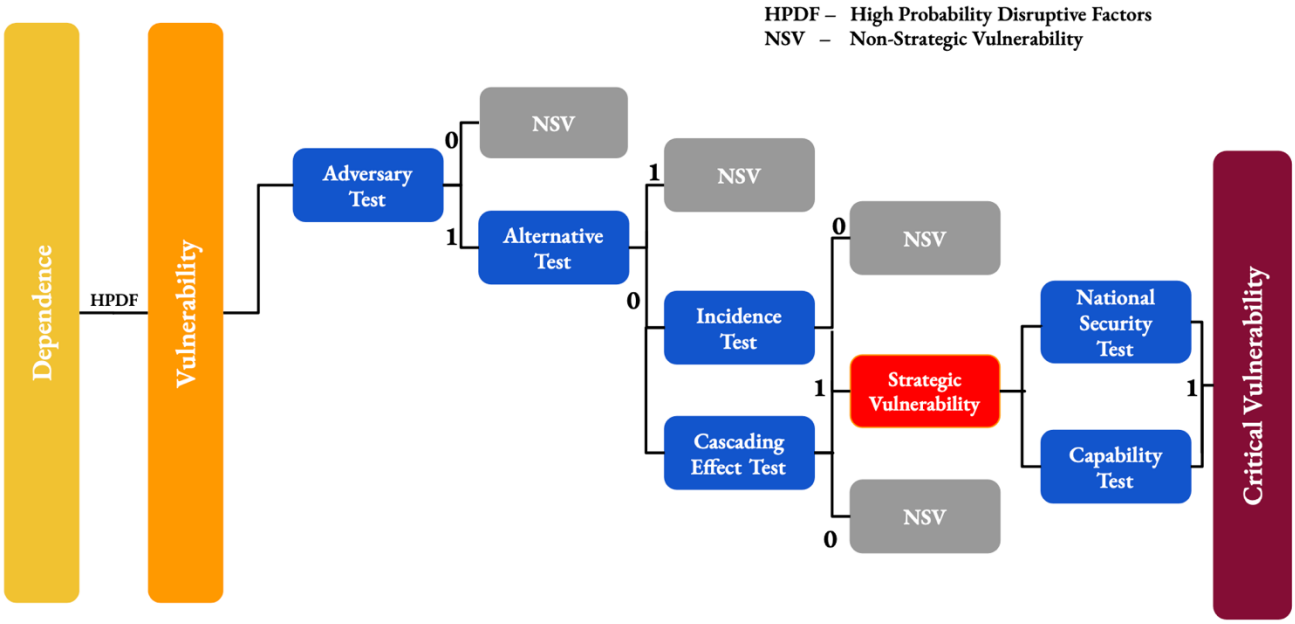
2. Capability Gap

Vulnerability vis-a-vis an adversary relating to a product of sophisticated and specialised technology that cannot be replicated in the short to medium term (rather would take decadal efforts). Examples: advanced chips, precision weaponry, space technology, missiles, ships, & aircraft. On the other hand, if the adversary's specialisation can be replicated and expanded in a relatively shorter period ~6 months to 2-3 years, it is a strategic and not a critical vulnerability. Example: assembly of electrical equipment; production of medical equipment, etc.

3.3 Framework through Flowchart

The following framework presents a four-stage test to determine strategic vulnerabilities arising out of trade dependency or asymmetric interdependence in trade.

'0' and '1' denote the result after putting the case of dependence through various tests. If a case passes the test, the number '1' is assigned and if fails the test, the number '0' is assigned.



4. Conclusion

The ideas discussed in this framework are not exhaustive, but serve the purpose of incorporating the most significant factors that determine whether a case of dependence constitutes vulnerability, and of what kind. The caveat this framework may encounter is that it does not apply to any and all cases of global trade interdependence; more specifically, it applies best to bilateral cases.

This paper forms the first of a series of outputs on dependency-induced vulnerability in the context of international trade, and shall serve as the backdrop for future outputs in this series. The framework discussed in this paper will henceforth be applied to various case studies globally, with the central study of interest being the India-China trade relationship.

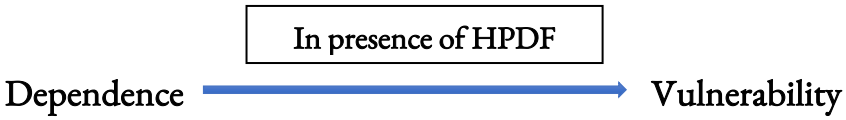
Glossary

Several terms or concepts discussed in this paper tend to be defined and understood very differently in popular discourse or specific contexts. For the purposes of conceptual clarity during this analysis, we adopt the following definitions:

Risk: Risk in a supply chain is defined as "the likelihood of an adverse and unexpected event that can occur, and either directly or indirectly result in a supply chain disruption" (Garvey, Carnovale and Yeniyurt, 2015).

Dependence: Dependence refers to a situation where Party A is reliant on Party B to carry out business operations - broadly sales and purchases. In this context, dependency can be buyer-based (downstream) or seller-based (upstream). The degree or severity of dependence can create conditions of vulnerability.

Vulnerability: Vulnerability (arising out of trade dependence) is a case of dependence tied to other disruptive factors that can render the dependence relationship untenable, fickle, or unreliable. In other words, it is a case of dependence that is susceptible to distress due to the presence of high probability disruptive factors (HPDF). Thus, dependency-induced vulnerability can be visualised as



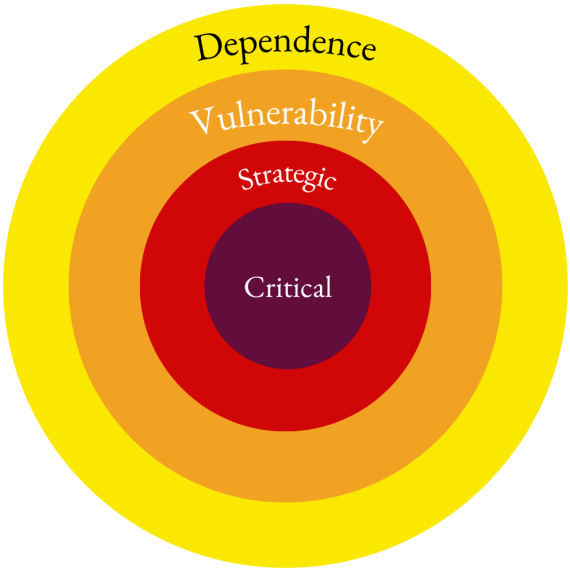
A case of dependence that is susceptible to frequent tariff or non-tariff barriers, supply shocks and disruptions, natural calamities, information asymmetry, and other factors that make dependence untenable. Dependence in isolation shall not be viewed as a vulnerability.

Strategic Vulnerability: This paper defines strategic vulnerability as a subset of vulnerability that can be primarily attributed to strategic motivations (economic coercion) by an adversarial state and can likely have geostrategic/geoeconomic implications on the state exposed to the vulnerability. Any vulnerability that is not strategic can be defined as a **non-strategic vulnerability (NSV).**

> **Strategic**: In the context of international relations, it is an approach to maximise national interests, i.e., pursue power and security, through tools of compellence, deterrence, and co-optation. A strategic approach could be applied to varying fields - domestic politics, international politics, business, or any other field characterised by competition among rivals.
>
> **Geostrategic**: Geostrategic is the strategic approach specific to the field of international relations. In this sense, the terms strategic and geo-strategic are often used interchangeably. It is the interplay of geography (loosely translated to nations or states) and strategy. Geopolitics and Geoeconomics are two constituents of geostrategic approach.

Geopolitics: Geopolitics is the use of political tools to further geostrategic/national power or interests. Geopolitical interests are connected with the direct or indirect control of territories (which contain resources) (Kurecic, 2015).

Geoeconomic: Geoeconomics can be defined as "the geostrategic use of economic power (Wigell, 2016). Alternatively, geoeconomics is using economic strength to pursue geostrategic interests. Geoeconomic interests are connected with resource management (exploitation and exports) and the inclusion of resources into national economies (Kurecic, 2015).



Critical Vulnerability: It is a strategic vulnerability of a severe nature that meets either of the two conditions: if the vulnerability can have a profound impact on a country's national security, or if such a vulnerability is a consequence of an enormous capability gap vis-a-vis an adversary that cannot be matched in the foreseeable future and would instead take decadal effort.

References

Garvey, M. D., Carnovale, S., & Yeniyurt, S. (2015). *An analytical framework for supply network risk propagation: A Bayesian network approach*. European Journal of Operational Research 243, 618–27 (2015).

Kurecic, P. (2015). *Geoeconomic and Geopolitical Conflicts: Outcomes of the Geopolitical Economy in a Contemporary World*. World Review of Political Economy 6 (4), 522-43 (2015). Retrieved from https://doi.org/10.13169/worlrevipoliecon.6.4.0522

Reiter, O. & and Stehrer, S. (2021). *Learning from Tumultuous Times: An Analysis of Vulnerable Sectors in International Trade in the Context of the Corona Health Crisis*. The Vienna Institute for International Economic Studies. Retrieved from https://wiiw.ac.at/learning-from-tumultuous-times-an-analysis-of-vulnerable-sectors-in-international-trade-in-the-context-of-the-corona-health-crisis-dlp-5882.pdf

Sharma, S.K., Srivastava, P.R., & Kumar, A. (2023). *Supply chain vulnerability assessment for manufacturing industry*. Ann Oper Res 326, 653–683 (2023). Retrieved from https://doi.org/10.1007/s10479-021-04155-4

Wigell, M. (2016). *Conceptualizing regional powers' geo-economic strategies: neo-imperialism, neo-mercantilism, hegemony, and liberal institutionalism*. Asia Europe Journal (2016). Retrieved from http://link.springer.com/