Charles University in Prague

Faculty of Social Sciences

Institute of Political Studies

Department of Security Studies

MASTER THESIS

2024 Alexander J. Sherwood

Charles University in Prague

Faculty of Social Sciences

Institute of Political Studies

Department of Security Studies

A Framework to Weaponize Risk, Targeting an Opponent's Supply-Chain Vulnerabilities

Master's Thesis

Author: Alexander J. Sherwood

Study program: International Security Studies (MISS)

Supervisor: prof. PhDr. RNDr. Nikola Hynek, Ph.D., M.A.

Year of Defense: 2024

I dedicate this paper to my father, mother, sister, and those who were with me even when I was not with them.

Thank you.

1) I hereby declare that I have compiled this thesis using the listed literature and resources only.
2) I hereby declare that my thesis has not been used to gain any other academic title.
3) I fully agree to my work being used for study and scientific purposes.
4) During the preparation of this thesis, the author used ChaGPT to debug and generate R code related to plotting graphs, simplifying functions, and fetching data recursively from directories. Additionally, ChatGPT was used to retool the Parkinson's function for measuring rolling volatility. After using this tool/service, the author reviewed and edited the content as necessary and takes full responsibility for the content of the publication.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In Prague on 30/07/2024 Alexander J. Sherwood

Abstract

This paper used price volatility data sourced from the Institute for Rare Earths and Strategic Minerals as a proxy for aggregate risk to select magnesium from a list of critical raw mineral candidates with the intent of investigating its supply-chain characteristics during the COVID-19 pandemic. This was accomplished to then harmonize with a disaggregated risk framework, based on a retooling of a project finance risk framework by Farrell[1], to generate a series of potential attack vectors that a theoretical opponent could use to induce risk in magnesium-related supply-chains, reducing operational efficacy, as a method of attacking European critical infrastructure. The theoretical opponent was constructed, and their behavior was defined, using offensive realism as a framing for their motivation and actions. The disaggregated risk framework that was created identified four main classes of risk: political risk, market risk, operating risk, and technology risk. These classes of risk and their sub-classes were then utilized to identify five different attack vectors that a state actor could use to deliberately induce risk in magnesium and magnesium-adjacent supply-chains to increase specific or aggregate risk. These five attack vectors were the denial of physical assets in upstream, downstream, and midstream elements of the supply-chain; leveraging sovereign risk to either extract actors from contractual obligations or using contractual risk to force a counterparty to surrender sovereignty; cyberattacks, particularly against midstream infrastructure; the policy and structural dumping of magnesium supply on to the open market; and inducing political instability through covert action for strategic gain.

Contents

I. Abbreviations

BWE - Bullwhip Effect

CGS - Chinese Geological Survey

CRMs - Critical Raw Minerals

EC - European Commission

EI - Economic Importance

EU - European Union

HREE - Heavy Rare Earth Elements

LREE - Light Rare Earth Elements

REE - Rare Earth Elements

SC - Supply-Chain

SEP - Systems Engineering Processes

SR - Supply Risk

USGS - U.S. Geological Survey

OPFOR - Opposing Force

WIP - Work in Progress

II. Introduction

Ensuring the flow of critical commodities in supply-chains to end consumers underpins the access to and operation of essential assets vital to nations' economic prosperity and security[2, 3]. In international markets that experience supply, demand, and price volatility for critical commodities and manufactured products[4–9], small perturbations in supply-chain demand and supply can yield radical shifts in supply-chain behavior[10, 11].

Many papers have been published in Supply-Chain Management, Operations Research, Industrial Engineering, Security Studies, Strategic Studies, and other academic fields regarding the defense of infrastructure. What seems absent, however, is how an aggressive opponent may conceptualize supply-chains and what vectors they could exploit to induce some negative consequence in a target of their choice. Additionally, what specific literature does exist in Security and Strategic Studies, as well as International Relations, regarding the defense of supply-chains does not explicitly treat concepts of risk in the same systemic manner that the architects and operators of supply-chains use in their design, operation, and maintenance of those same systems.

In the pursuit of further securing critical commodities and raw minerals, numerous national bodies, including the European Commission (EC), have identified various commodities upon which different critical infrastructure sectors rely. These commodities vary in importance and susceptibility to disruption than others, so much so that legislation and risk-management frameworks have been adopted on a multilateral basis in certain instances.

The adoption of these measures by the European Commission, outlined in the Critical Raw Minerals Act (CRMA) *COM(2023) 160 - Proposal for a regulation of the European Parliament and of the Council establishing a framework for ensuring a secure and sustainable supply of critical raw materials*, specifically outline two variables as crucial components of analysis: Supply Risk (*SR*) and Economic Importance (*EI*)[12]. An initial investigation of these variables, which aggregate a variety of risks based on composite indices and inputs such as production and infrastructure sector reliance on a particular commodity[13], revealed that the aggregate risk to which a commodity and, more importantly, the supply-chain which provides that commodity to downstream consumers, was not captured at all in these measures; notably, cost performance was included in as a parameter, but not the underlying price of the commodity on the open market[13].

With the seeming absence of offensively orientated frameworks in the literature that prescribe how to attack, the nature of the *EI* and *SR* indices and a lack of risk in a systems context pose a novel opportunity to provide a theoretical framework that accomplishes, or at least begins an iterative attempt, to combine all three in the context of the EC's objectives to secure its access to CRMs.

Therefore, the objective of this paper is threefold. The first objective is to measure the aggregate risk of a CRM. Second, the paper seeks to examine the characteristics of the mineral's supply-chain during a period of high systemic stress under the axiomatic assumption that whatever risks the supply-chain was exposed to for that time period were magnified. In this instance, the COVID-19 pandemic was selected as this period of elevated supply-chain stress. The third and final objective is to create a framework that disaggregates risk into different risk classes, which could be applied by an offensive actor seeking to leverage these risks against their opponents. The deliberate induction of risk in a supply-chain by a state actor, or the organs of that state actor, is referred to as 'weaponized risk'.

This framework is contextualized through application to five potential attack vectors that an aggressive theoretical opponent could use to induce these risks in a supply-chain with the intent of damaging their target's ability materially to supply relevant CRMs necessary for the continual operation of critical infrastructure.

Hereafter, this paper initially provides a literature review in Section III, covering broad supply-chain phenomena, an exploration of the concept for risk, it's manifestations, and employment in different contexts; the broad concepts of realism, and especially offensive realism which as used to explain the behaviour of the constructed theoretical opponent which seeks to weaponize risk; how states weaponize different supply-chain elements as filtered through a realist lens; the different strategic logics which may be employed when weaponizing risk; and a breakdown of existing legislation regulating the definition of critical infrastructure.

Following this literature review, Section IV provides both the theoretical framework and methodology that underpins the approach taken to generate the end framework using Design Science Research (DSR), the research questions, how the systems thinking and the concept of risk align with the Security Studies and Strategic Studies fields, the alignment and necessitation of a post-positivist orientation when utilizing risk as an analytical concept, the conceptualization of weaponized risk and the theoretical opponent which seeks to actively induce risk along a supply-chain to target its adversaries, the scope of analysis, stages of analysis, the selection basis of the candidate material, the calculation of price volatility as a proxy of aggregate risk, and how risk is disaggregated.

Section V investigates the specific characteristics of the candidate mineral (magnesium) supply-chain by examining the material properties of the selected candidate material, its different derivative products, the current state of global production, the alignment of different critical end products with relevant infrastructure sectors, how the candidate material is produced,relevant transport considerations, and an analysis of the price history and price volatility of the material over the COVID-19 pandemic.

Section VI desegregates risk into different risk classes. This is performed for application of the framework to the investigated mineral supply-chain. Finally, five different attack vectors which employ different mixes of these risks are examined in Section VII

III. Literature Review

A. Supply-chains and Associated Phenomena

Supply-chains experience various different phenomena, arising from demand and supply activities. These supply-chains can be modeled as either linear or non-linear, where in the former raw materials are transformed into Work In Progress (WIP) inventory through manufacturing and/or processing, then to finished products, and are then distributed to end consumers through wholesale and retail flows[14]. Nonlinear supply-chains, by contrast, are characterized multiple actors each adding value, and or transporting material, during different stages of the supply-chain, and therefore exhibit mathematical chaos described by deterministic equations contingent on different initial conditions[15].

As described by Vonderembse et al., supply-chains can also be classified by the kind of product around which the supply-chain is orientated - *Standard*, which posses seldom evolving characteristics and has stable demand; *Innovative*, which encompass products that frequently change and are marked by variable, uncertain demand; and *Hybrid*, which exhibits characteristics of both[16][17].

Having now identified the different types and classifications of supply-chains, it is possible to investigate the different phenomena that affect them. Blanco et al. identify seven different phenomena associated with nonlinear supply-chains: waste, vulnerability, uncertainty, congestion, The Bullwhip Effect (BWE), diseconomies of scale, and self-interest[10]. These are defined the following table.

TABLE I: Blanco et al.'s seven nonlinear supply-chain phenomena[10]

Phenomena	Description
Waste	Use of resources without creating value
Uncertainty	Inability to predict the future due to incomplete knowledge or changing environment
Congestion	Excessive accumulation of products, processes, or information
Bullwhip	Upstream amplification of demand signals
Diseconomies of Scale	Increase of unit cost as output increases
Self-Interest	Reduction of system wide profits, due to individual profit focus

Of all of the seven phenomena described by Blanco et al., BWE, or 'demand information amplification[18] is of particular interest. This term refers to the empirical and theoretical phenomenon[18] where minute or small perturbations in downstream demand lead to increasing upstream demand variation and volatility[19][20][21].This amplified effect is a chief concern in operations research and supply-chain management given its associated costs[20].

Management of the Bullwhip effect demands supply-chain participants to forecast demand over different time-horizons, as well as production quantity, costs, and other variables[21]. The complexity of modeling such systems in magnified by poor information resolution and information time-delay[22], especially since forecasting over a long enough time-horizon may prove to be inaccurate.

The BWE stems from not only rational, operational concerns such as machine capacity and inventory, but also irrational human factors[20] such as actions influenced by cognitive limitations[23][24][20], information feedback[20], and others[20].

Shocks do not only propagate through demand, but also through supply[11, 25]. Disruptive risks, including those related to production, transportation, and the supply of outputs can propagate across a supply-chain are distinct from the BWE[26]. Supply disruptions manifest in the ripple effect which relate to ”structural disruptions” of upstream elements, not downstream changes in behavior[26].

B. Risk

Risk is an abstraction which is often employed across multiple fields in the evaluation of different threats and opportunities in many dimensions. No universal defition of risk exist, or what constitutes risk, especially in the practical application of risk in the field of security[27]. There exist different standards for how to apply risk, and are often employed across multi-disciplinary fields especially in regards to Supply Chain Management. What is concrete and absolute, however, is that failure to account for risk results in catastrophic outcomes[27][28], both to entire systems[29] and individual actors[30].

What risk is, how and why it is a pertinent concept for analyzing different vulnerabilities for exploitation, and why a unified framework for risk in the field of security studies is required, is the subject of this section.

1) The Nature of Risk

Risk as an analytical concept precedes its explicit codification in the 20^{th} century[31][32], which as a concept extends beyond the purely physical and mathematical into the metaphysical. This is not the concern of this paper and is outside of it’s scope. Risk, it context of this endeavor, is a concept related to the probability and/or uncertainty of events, induced or otherwise. The divergence of different institutions and academia in their understanding of risk, either within their own fields or across them, is indicative of the multidimensional nature of the concept[30]. Therefore, the definition of risk must be understood as inherently fuzzy in the general, unless applied to the specific operationalized domains to which it is applied.

In the literature, there exist numerous different generic definitions of risk, notably as articulated by in the field of economics, finance, and insurance, by authors such as Knight, Holden, Crow & Horn, Greene, Willet, Wood, and Athearn.

Most of these conceptualizations, as found by Athearn, correlate risk with uncertainty[33]. For example, Greene[33][34][35] summarizes risk as: ”uncertainty as to the occurrence of an economic loss,” while Willet[33][36] defines risk as ”...objectified uncertainty regarding the occurrence of an undesirable event,” and Wood[37] describes risk simply as the ”chance of loss.”

Perhaps one of the most influential codification of risk in the modern context was expressly posited by Frank Knight in his 1921 book *Risk, Profit, and Uncertainty*. Knight’s risk is defined as a knowable probability of an error in a judgement[38]. Under this framework, risk is distinguished from true uncertainty by virtue of the know-ability of probability associated with an error in judgement.

As LeRoy and Singell explain, Knight’s criteria for know-ability was defined in three ways[38]:

1) ”a priori probabilities, which are derived deductively, as in rolling dice.
2) ”statistical probabilities, which are generated by empirical evaluation of relative frequencies.
3) ”estimates”

Of these three criteria, only the first two are classified as risk under Knight’s framework[39][38]. Estimates are, however, considered to be true uncertainty[39][38]. The issue with this definition arises from how Knight treats subjective probabilities, even as a concession to the reality that the objective probability of an event may not necessarily be obtained without some level of estimation[39][38]. Knights definition, therefore, significantly departs from common and colloquial understandings of risk[40]; and the utility of such a definition is significantly diminished.

Therefore, subsequent authors have offered alternative definitions of risk to rectify this issue for more effective operationalization. Holton, for example, posits that risk ought to be defined as the exposure of an individual[1] to uncertain events[40]. Under this definition, Holton provides the example of an individual who has flung himself out of an airplane without a parachute. Despite the fact that this individual is exposed to the risk of death, because that death is certain, that individual faces no risk[40]. This definition, Holton posits, is more in line with commonly understood conceptualizations of risk[40].

Risk also is frequently conceptualized as applicable to not only individuals, but also organizations[35]. In this conceptualization of risk, it is not only born by individual actors, but by collective groups, and even systems that exhibit emergent behavior. Risk is therefore a pervasive, totally encompassing, consideration in any human endeavor.

[1] Notably, the what constitutes an individual in Holton’s conceptualization of risk is narrowly constrained to a self-aware being, such as a human being or an animal[40]. Therefore, as Holton admits, organizations which operate legally and financially as separate entities, for example, states, corporations, communes, unions, churches, and other entities, cannot assume risk[40]. Holton’s, self-admittedly ”flawed”, conceptualization of risk assumes this position as, in the context of financial exchange, it is different individual stakeholders who assume risk[40].

2) Risk Contexts

Risk also arises from different risk sources in varying contexts, and any framework for managing risk depends on internal and external contexts applicable to a managed organization, including legal, financial, political, technological, regulatory, economical, or environmental factors[41]. These domain-specific risks also are effected by stakeholder considerations, market trends, network complexity, organizational culture, organizational structure, industry standards and guidelines, resources, capital, data, information and information flows, and contractual relationships[41].

Other domain-specific risks have been defined by the Securities and Exchange Commission (SEC) as volatility, inflationary, interest rate, and liquidity risk[42]. In project finance, they are commonly specified as legal, financial, technical, political, economic, completion, operational, and counterparty risk[43]; and in military-specific domains, for example, risks are designated as 'Hazards' by The U.S. Department of the Army, which are classified as mission, enemy, terrain and weather, troops and equipment, time, and civil[44].

In security and defense contexts, in particular, there appears to be no unified framework for risks among professional practitioners of risk management. Different organizations, public and private frequently utilize differing schema and risk analysis methodologies[45][27]. This lack of a unified risk management framework can be expected due to different operational contexts: the risk calculus required for the analysis of a military operation seeking to neutralize critical members of OPFOR (Opposing Force) is surely distinct from analyzing the maritime risk regarding the use of munitions by enemy proxies targeting trade. Therefore, especially in regards to different generic risk standards, many professionals perceive generalized frameworks to be of limited utility[27].

Nevertheless, semi-generic frameworks, especially in a security context, pose potential as versatile tools, especially when collaborating between different organizations with vastly different cultures, objectives, and operational procedures. Where there is a shared language and a need for interoperability and consistency in approach, authors such as Spring et al. have identified a need for something approximating a shared framework of risk[46][27].

With regards to *'security risk'* - a form of operational risk - Harris and Sadok identified three main ”themes” in their analysis of different risk frameworks as employed in the security field. These are a lack of[27]:

- consistent terminology
- ”a structured and consistent risk assessment approach”[27]
- internationally recognized risk standards adoption.

C. Risk Management and Standards

While risk is highly idiosyncratic to specific application domains, as indicated is Section III-B.2, it is absolutely vital to provide a systematized framework for risk analysis in any endeavor, lest a system designer be forced to fabricate one from first principles in every project. Such a proposition is, usually, untenable. This is especially true if the ownership and liability of a project shifts from one organization to another, or is shared my many actors.

To this end, there exist whole suites of domain-specific and generic risk management standards. The most notable of these are provided for by the International Standards Organization's *ISO 31000:2018 Risk management - guidelines*, and the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Enterprise Risk Management* framework. These generic frameworks provide standardized suites of tools for an organization or individual to apply to their unique application domain.

For example, ISO 31000:2018 and ISO 31010 prescribe a standard model of risk assessment[2] in the context of its contribution to risk management by identifying precisely defined iterative and chronological steps. These steps are establishing the context of the system, identification of salient risks, analysis of said risks, the evaluation of risk severity, and the treatment of risks[41].

These risk assessment steps are outlined by ISO 31000:2018 in pursuit of answering four fundamental questions[41]:

- ”what can happen and why (by risk identification)?
- ”what are the consequences?
- ”what is the probability of their future occurrence?
- ”are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?”

1) Risk Identification/Event Identification

As seen in Fig 1, ISO 31000:2018 classifies three processes as constituent elements of risk assessment: risk identification, risk analysis, and risk evaluation. In the three step iterative process of risk assessment, risk identification pertains to the,

> ”...process [which] includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact.”[41]

[2] See Figure 1

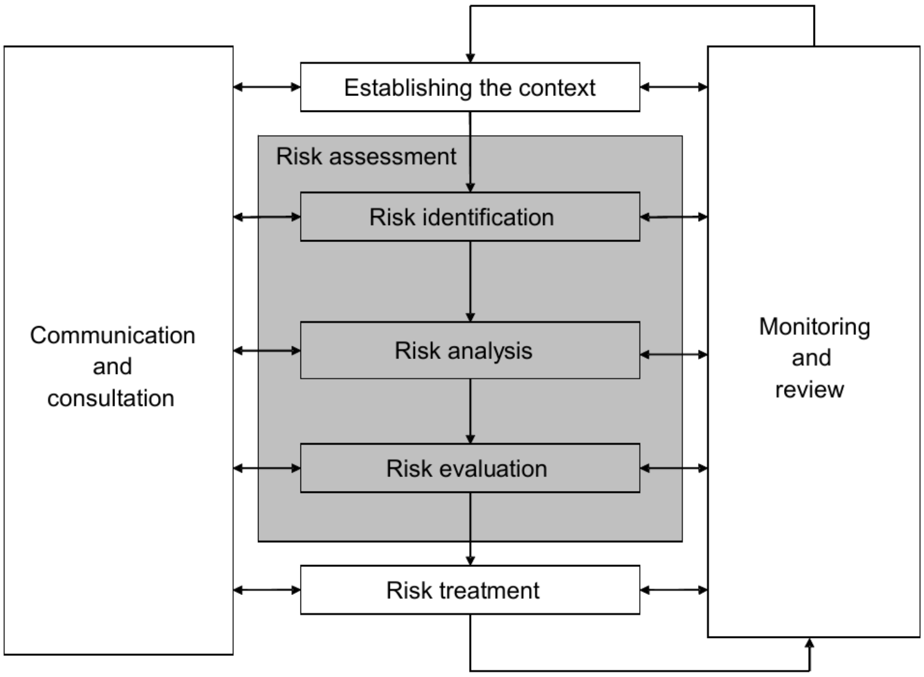

Fig. 1: ISO 31000 Contribution of risk assessment to the risk management process[41]

The process of risk identification is achieved through three broad classes of methods, some of which are suggested by the ISO standard. These three classes are either based on historical data, systematic approaches based on procedural querying of system variables, or inductive reasoning[41][47].

A parallel process is found in COSO's enterprise risk management framework, termed *event identification*, which seeks to distinguish risks and opportunities to which operations are exposed[48]. Risk identification is therefore the process of utilizing these three classes of methods in the consideration of the following elements[41]:

- ”tangible and intangible sources of risk;
- ”causes and events;
- ”threats and opportunities;
- ”vulnerabilities and capabilities;
- ”changes in the external and internal context;
- ”indicators of emerging risks;
- ”the nature and value of assets and resources;
- ”consequences and their impact on objectives;
- ”limitations of knowledge and reliability of information;
- ”time-related factors;
- ”biases, assumptions and beliefs of those involved.”

2) Risk Analysis

After risk identification, each risk is analyzed to ascertain its characteristics, including the degree to which each relevant risk is present and its impact (i.e. it's weight) on the overall system. This analysis is therefore concerned with the effects of identified risks, the probabilities of their different manifestations, and potential future n^{th} order consequences[41]. It is essential to note that because risk 'events' can stem from multiple sources[41], n^{th} order considerations become of vital importance. Exposure to one class of risk stemming from multiple sources can radically affect multiple strategic objectives across multiple projects[41].

ISO 31010 specifically prescribes that in circumstances where one particular class or manifestation of risk stems from numerous sources or where a unique event is not identified, that focus of risk analysis ought to be on,

> " the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies."[47]

Risk analysis need not be strictly quantitative, as identifying probabilities related to risk events can be assigned qualitative or mixed semi-quantitative values[47]. Examples of qualitative probability assignments are provided by 31000 as 'high,' 'low,' or medium; these qualitative assessments are not rigidly enforced by these standards[47]. For semi-quantitative approaches, ISO 31010 describes different potential approaches to semi-quantitative probabilities as reliant on formulas and methods that generate either linear or logarithmic numerical scales representing different levels of risk[47].

3) Risk Evaluation

The final step in risk assessment is evaluation, which consists of the re-contextualization of risk severity and risk event probabilities by comparing relative rankings against predetermined criteria[47][41].

This risk assessment component also demands the creation of documentation, which is to aid in the ranking of relative risk event severity[47][41]. This documentation includes, but is not limited to, risk identification, analysis, and evaluation methodology; system scope; risk sensitivity and uncertainty analysis; different risk and system axioms; and data validity[47].

D. Risk Frameworks in Systems

This literature review has identified three key features that are frequently employed in a number of risk management frameworks: a generic systematic approach that is refined and attuned to domain-specific risks, the use of mixed qualitative-quantitative approaches, and a broadly defensive risk management orientation.

Without exception, most risk management frameworks operate on a systematic approach, first by approaching a 'system' from first principles, and then subsequently by attuning those first principles to the specific context. These risk management frameworks are often referred to as *Enterprise Risk Management* - holistic approaches to risk that take into account the entire enterprise or activity in it's context[49], as distinguished from *Traditional Risk Management* which is focused narrowly on particular components of the greater system[49][50].

This review identifies three general sets of principles from which risk management frameworks operate[3]. There categories of first principles are: systems engineering, existing risk standards, and supply-chain orientated risk management approaches.

Superficially, specific risk management frameworks identified in the literature search appear to, at least in broad generalities, follow the template of the iterative and chronological steps proposed by generic risk standards established by ISO, COSO, and others. Some of these frameworks are limited in scope to specific application domains, while others are focused on particular case studies within application domains, and yet others focus on more abstract, generic, applications of risk.

1) Supply-chain Risk Management and Resilience

There exists in the literature a split between studies focusing on qualitative understandings of the risks to which supply-chains are exposed[51], as opposed to mathematical/quantitative models[52][53][54] that seek to optimize the system characteristics underpinning supply-chains[55].

Few frameworks that analyze an entire supply-chain appear to exist[56]. Instead, impact analysis of different behaviors appears to be focused on either specific domains of application[56][4] or different techniques[56].

As applied to supply-chains, there appear to exist two different classifications of frameworks that appear to describe the same phenomena of management: supply-chain resilience and supply-chain risk management, especially as it relates to quantitative methods[66][67].

The former of these two, according to Hosseini et al., is a ”broader field” of study[67], while supply-chain resilience is orientated around the[5],

> ”SC (supply-chain) capability to utilize the absorptive capacity of SC entities to repulse and withstand the impacts of perturbations, to minimize the consequences of disruptions and their propagation by utilizing adaptive capacity and to recover performance level to normal operations in a cost-efficient manner using restorative capacity when absorptive and adaptive capacities are not sufficient.”[67]

In their review, Hosseini et al. conceptualize supply-chain resilience as predicated on three elements: absorptive capacity, adaptive capacity, and restorative capacity. These capacities are brought to bare

[3] These principles can and are mixed.

[4] For example in pharmaceuticals[57], motor transport[58], logistical networks[56][59], inventory[56][60], and manufacturing[61][62][63][60][64][65]

[5] Note that there are many definitions of supply-chain resilience[67].

against supply-chain disruptions in this order[67]. The first of these, absorptive capacity, refers to the ability of a supply-chain to absorb system shocks and reduce the deleterious outcomes of said shocks with as little energy as possible[67][68].

Adaptive capacity, meanwhile, is predicated on the capabilities of a supply-chain to overcome system failures or disruptions by organically adopting ”non-standard” or novel solutions on its own accord, without specific attention given to recovering normal functionality[67][68].

Finally, restorative capacity is simply defined as the ability of a system to return to normal working order in the event that adaptive or absorptive capacity prove insufficient to compensate for whatever shocks the supply-chain is subject to[67][68].

Risk management, meanwhile, can be understood less as the properties of a supply-chain and more as an active approach. In their review, Emrouznejad et al. provide two different definitions of supply-chain risk management. These are:

1) “Risk management refers to strategies, methods, and supporting tools to identify and control risk to an acceptable level.” [69][70]
2) ”...a synchronized set of actions and approaches to direct an organization to minimize the risk for achieving the organizational goals.”[70]

Thus, it appears that the fundamental difference between supply-chain resilience and supply-chain risk management is that of perspective and ownership. Based on the definitions provided herein, supply-chain resilience is a property or characteristic of a supply-chain, or several embedded supply-chains. Risk management, meanwhile, is a series of actions that are performed on a supply-chain to reduce exposure to unnecessary risk.

Additionally, from the definitions provided for by Emrouznejad et al., it is clear that risk management in a supply-chain management context is fundamentally defensive as a concept. Risk is conceptualized as abstract and tangible burdens that different actors along a supply-chain must bare.

2) Risk Management Frameworks Derived from Standards

The subsection of the literature review herein covers different papers in the literature that derive some, or all of their risk frameworks from existing risk management standards. These papers are orientated primarily around the supply-chains of different industrial sectors, such as pharmaceuticals[57], motor transport[58],

Many authors apply existing risk standards as first principles when designing risk management frameworks. for example, Elamrani et al. adopt risk as first principles, and applying them to pharmaceutical supply-chains, thereby 18 different classes of risk, mapping probabilities of events occurring, and assessing the impact of different risks across different components of the supply-chain[57].

A similar approach can be observed in Semin et al.'s 2016 paper, *A process model of risk management in the system of management of strategic sustainability of cargo motor transport enterprises*, which broadly follows ISO 31000's risk assessment format[58]. Unlike Elamrani et al., however, Semin et al. do not provide an analysis of risk impact on a particular system, and are focused on more general application.

Yuntao et al. provide what they refer to as a *Framework of Comprehensive Risk Management system* for application in the defense and technology sector[71]. This paper adopts COSO's three dimensional *Enterprise Risk Management Integrated Framework*, as well as ISO3100, GB/T 24353, and AZ/NZS 4360 SET Risk Management Set to create a "Comprehensive risk management process" roughly analogous to ISO 31000[71]. Their paper additionally identifies six different broad categories of risk relevant to the sector of application[71].

3) Risk Management in Systems

Some authors either employ risk management frameworks in conjunction with traditional systems engineering principles or Systems of Systems (SOS). That is, they are directly attempting to identify the needs of the system stakeholders prior to implementing those requirements in the design of the system[72][73]. These systems may be embedded within larger macro-systems, where system boundaries are not defined, necessitating quantitative approaches such as Monte Carlo simulations and modelling using Bayesian Belief Networks, or in traditional engineering systems where risks can be qualitatively ranked[74].

A stakeholder-centric holistic approach is adopted due to the necessities imposed by the complexity of socio-technical systems[75][76]. Reductively focusing on singular elements of a system as it pertains to risk will result in unintentional n^{th} order consequences.

This is especially pertinent when dealing with embedded SOS. Citing Keating et al., Pinto et al. point out[32],

> "When engineering traditional systems, the tools and methodologies available are sufficient to provide a solution to a defined problem; the analysis conducted is dominated by technological components; and scoping and framing the problem is easy, since the boundaries are fixed. However, when dealing with SoS, the boundaries become fluid, there is no one right way of dealing with the problem at hand since it is emergent, and engineering these systems of systems becomes a satisficing issue, rather than optimising[77]."

Practically, this means that for critical infrastructure and supply-chain risk management it is necessary to account for risk across multiple intersecting domains[32] and stakeholders[32][78].

This holistic approach is mirrored in the application of risk management to Systems Engineering

Processes (SEP). Through the conceptualization and operation of risk to SEP[6], authors such as Ganguly et al.[73] provide frameworks to operationalize risk management throughout the entire life span of a product from conceptualization and design to prototyping and implementation.

4) Defensive Ambiguity and Orientation

Most papers collated for this review that provide a risk management framework are defensive in either of two conceptualizations. The first of these is the *de-facto* defensive orientation that most risk management frameworks adopt; these frameworks are concerned with mitigating risk that a system owner is subject to, as discussed in Section III-D.1. Under such a conceptualization, however, any system owner could define the leveraging assets in an offensive manner as defensive in any context. Thus, this conceptualization of nominally defensive risk frameworks must be cautioned such that a risk management system is not designed to be purposely misleading to an outside viewer.

How, then, is an analysis to distinguish between an offensive risk framework, which outright outlines methods of promoting failure in a system owned by another party and an ambiguously offensive/defensive mixed framework that provides tools nominally to be deployed in pursuit of risk management but could be used to attack (i.e., disrupt) an opponent's system? Other than implementation and intent of the user, both of which are subject to error in appraisal, domain application provides a useful barometer. Risk management in military and defense-sector contexts provides unique insight into strategically ambiguous risk management frameworks.

Many of these defense-sector and military frameworks borrow the same risk orientation as supply-chain risk management in their defensive posture towards to to protect designated strategic objectives, but *can* be employed to maximize risk for an opponent.

Here, this review finds authors such as Mandel who is expressly concerned with the definition and nature of risk, the utility of risk and its appeal to planners, as well as the (perhaps overly) broad nature of the concept[80]. A similar approach is taken by Preda, who aligns ISO 31000 methodology with the risk culture and requirements of defense in general[81]. These highly abstracted treatments of risk are contrasted to other frameworks in the defense field.

Roughly one level 'down' in abstraction, this review identifies authors such as Bernhardt[82], Liwång[83], Liwång et al.[84], Germann & Gregg[85], Vancactor[86], and Gaidowet al [87], deal with either specific elements of defense risk - for example, communication as with Liwång[83]; specific tools with Germann et al.[85]; or specific organizations as with Gaidow et al.[87] and Vanvactor[86].

[6] Defined as the, "...comprehensive, iterative and recursive problem solving process, applied sequentially top-down by integrated teams."[73][79]

5) Offensive and Defensive Risk Models Specific to Critical Raw Minerals

There appears to be a relative lack of offensively focused, systematized frameworks orientated around exploiting supply-chain vulnerabilities and seemingly none orientated specifically around critical raw minerals (CRMs).

Only three papers fulfill the criteria of prescriptively identifying vulnerabilities and attack vectors and subsequently providing a framework for future exploitation. In strategic studies, Layton's[88] systematized approach to supply-chain warfare is perhaps the most explicit. Orientated around economic warfare, Layton identifies the components of generic supply-chains and different leverage points that can be used in a military context to disrupt operation[88].

Another comparable framework this review found was van Niekerk & Ramluckan's economic information warfare model, which identified five scenarios in which an aggressive actor would employ different categorized methods to disrupt commodity chains[89].

Finally, Brown et al.'s *Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses* examines methods of increasing defensive capabilities by modelling terrorist offensive actors and state defenders wit h Stackelberg games[90]. These games are applied to numerous contexts, including attack on electrical grids, oil pipelines, metro transport systems, airport security, and supply-chains[90].

By contrast, this review identifies several defensive frameworks for mitigating supply-chain risk, especially regarding CRMs. Authors such as Bilsborough, Cui et al., and Funaiole et al. do establish different frameworks for the mitigation and exploitation of risk in different CRM supply chains, focusing on either the relationships between specific geopolitical actors in supply chains[91] or supply-chains for an individual CRMs[92] or groups of CRMs[93].

These defensively orientated frameworks are not systematized in the same manner as Layton, van Niekerk & Ramluckan, or Brown et al. - as they do not provide prescriptive models in the form of deliberately engineered systems for application in different domains. They are, however, specific to CRMs and the strategic contexts relevant to this proposed project. Therefore, the gap expressed herein presents an opportunity to marry the systematized approach of offensive frameworks to the strategic policy objectives of different security actors.

E. Realism

As a school of international relations, Realism is perhaps one of the oldest[7], most well established[94], yet unpopular schools of international relations and geopolitics[95].

[7] Some of its proponents even trace its genesis back to classical history[94].

Like all broad schools of international relations, political, and security thought the broad framework that it provides can be broken down into many sub-schools: classical, neo-realist, neoclassical, offensive, defensive, and many others.

The purpose of this section of the literature review is to provide a broad overview of realist thinking so as to provide contextualization of the methodology employed in this paper in generating the different actors which are used to explore aggregate and disaggregated risk. This section is by no means in depth - it is instead only used provide the reader with a understanding of the fundamental principles of the school so as to better grasp how and why this paper has taken upon itself to construct a theoretical opponent for an offensive framework.

Since the purpose of this paper is not to make inferences as to the behaviour of states, or the motivations of states, only in how state behavior could manifest, realism provides a convenient framework for contextualizing risk weaponization, nothing more.

Hereafter, this section of the literature review is broken down into four sub-sections: an overview of the fundamental concepts and axioms of realism as a broad school, offensive realism, and defensive realism.

1) Fundamental Concepts

Realism provides a structural framework for the interaction of state behavior that explains their seeking of power as reflective of a type of 'anarchy' that typifies the international order[96]. In this anarchic world posited by structural realism, all states seek their own security, less they be confined to the dustbin of history[96].

Realism makes no moral judgements[94]. It does not necessarily condone the actions of states, but seeks instead to describe their behaviors. On this basis, realism operates from positivist first principles or axioms, chief amongst which include the stipulation that all states are rational actors, that states are the resolution at which analysis should occur, the aforementioned anarchic world order, and the drive for power[94].

From these axioms, realists have determined that the least stable form of political status quo is multipolarity, that hegemony will seek to quash opponents that perceive as a threat to their power, and smaller states will join in arms or alliance to balance against an existing hegemonic state or a rising threat[96].

This bring attention to a number of vital concepts which have been articulated by realists: balance of power, balance of threat, and bandwagoning.

2) Balance of Power

With the caveat that the concept can bare different meanings and definitions to different practicitioners and scholars of realism[97], the balance of power generally refers to the relationship between different nations regarding the distribution of their capabilities to project power[97]. Balance of power can also refer to the equalibrium between different nations regarding their overall capabilities to survive[97, 98] that arises as a consequence of different nations each pursuing policies bounded by rational means and decision making[98–101].

3) Balance of Threat

First coined by Stephen M. Walt in his 1985 article titled *’Alliance Formation and the Balance of World Power’*, balance of threat postulates that state actors seeks to not only balance against larger powers and hegemons, but the additional spectre of ”perceived threats”[102]. This concept seeks to answer the question as to why many American allies did not align themselves with the Soviet Union despite the disproportional distribution of power between them and the United States of American. Walt proposed that the perceived threat, or in other terms, the perceived risk posed by the Soviet Union was sufficient to induce diplomatic alignment with the United States against the Soviet Union[102].

4) Offensive Realism

As a school of international relations and security, offensive realism holds that all states are fundamentally self-interested entities that seek to remediate the absence of security, brought on by the *’security’* dilemma incurred by an ”anarchic world order”, through the attempted maximization of their own power[103]. This, offensive realism’s primary proponent, John Mearsheimer argues, is the direct consequence of states attempting to prevent the rise of opponents, or the power of the existing hegemony, from dominating them and also seeking the maximization of their own power[103, 104]. Indeed, Mearsheimer argues that the ultimate state of security is that of absolute hegemon, as dictated by the requirements of the international political system[103, 104].

According to Johnson & Thayer, proponents of this school tend to argue that ruthless jostling in the ”international system” is the operative logic for such behavior[103–105].

As a framework for the ways in which states manifest in the international arena, Mearsheimer puts forth five axiomatic conditions which under pin this school of thought[103, 104]:

- The aforementioned anarchic world order.
- The military capabilities of great powers.
- The uncertainty of states as to the intentions of other actors in the geopolitical arena.
- States being concerned with continued survival as their primary objective.
- Rationality as given characteristic of states.

5) Defensive Realism

The systemic, structural neo-realist school of defensive realism, notably typified by the author Kenneth N. Waltz, emphasizes that while the interplay of systems on the international level are typified by anarchy, states are incentivized to maximize power only in so far that their needs are satisfied within the boundaries of existing conditions[95]. Thus, by happenstance and the patterns of interactions between states, it may be the case that many actors are not necessarily required to seek constant expansion[95].

The patterns of behaviour mapped by other schools of realism, for example offensive realism, which pertain to the need for constant expansion and pursuit of hegemony are then either the result of deliberate, necessary, policy or arise from a mistaken belief that,

> ”...aggression is the only way to make their states secure.”[95]

Thus, advocates of defensive realism argue that the superior maximum for more powerful states is to pursue policies of limited scope and restraint, preventing lapses into complete and total dedication to power maximization via military strength or other means[95, 106]. It is feasible then for states that are authoritarian to mutually agree to cessation of conflict or brinkmanship, absent even international institutions[95].

Common criticisms of defensive realism can be classified in one of either two camps: that the assumptions of defensive realism are in and of themselves contradictory to realism as a broader school of thought, and is thus not realism at all[95, 107]; or that defensive realism, as articulated by provides insufficient incentives to explain the propensity of states to seek power and expand[95, 108, 109].

F. Existing Appraisal of Critical Raw Mineral Supply Risk

In recent years, there has been significant attention on the analysis of the aggregate and supply-risk of various (CRMs)[110]. These materials, essential for the functioning of modern economies and the development of advanced technologies, are the subject of extensive academic scrutiny and policy-making by national and international bodies[110]. Researchers have systematically examined the availability, demand, and geopolitical risks associated with CRMs, highlighting their critical importance and vulnerability in the global supply chain[8, 110–116]. The scholarly discourse often draws on the frameworks and findings provided by authoritative organizations, including the European Union (EU)[12, 13, 117], the U.S. Geological Survey (USGS)[118], U.S. Department of Energy[119], U.S. Department of Defense[120], Japan[121], the Chinese state[122], and others.

National and international policy-makers have underscored the imperative of managing the risks associated with CRMs to safeguard national and economic security[112]. Reports and strategic documents from entities such as the European Commission (EC) and the U.S. Department of Defense emphasize that disruptions in the supply of these materials could have severe repercussions for industrial competitiveness, technological innovation, and military readiness[3, 12, 120]. The EU, for instance, has highlighted that an over-reliance on imports for certain critical raw materials exposes member states to supply risks that could undermine economic stability and security[12].

Identifying which minerals are both vital and vulnerable is becoming an increasingly critical aspect of both foreign and domestic policy. Governments and international organizations are focusing on specific minerals deemed essential for strategic industries, including those related to green energy, defense, and digital technologies. The criticality assessments are often based on factors such as economic importance, supply risk, and environmental implications of extraction and processing. These evaluations guide policy decisions and strategic initiatives aimed at securing reliable and sustainable supplies of these materials[118].

A key policy response to the supply risks associated with CRMs is the enactment of legislative frameworks aimed at ensuring supply security. The EU's Critical Raw Materials Act (CRMA) is a notable example. This legislative initiative seeks to reduce dependency on third countries for CRMs by diversifying supply sources, promoting recycling, and investing in sustainable mining practices within the EU[12]. Similar measures are being adopted in other regions: the United States has implemented the National Defense Authorization Act, which includes provisions to secure supplies of critical minerals[3], and Japan has its Strategic Energy Plan that outlines measures for resource security[123].

The EU is particularly dependent on imports for a range of critical raw materials, including rare earth elements, cobalt, lithium, and platinum group metals, which are essential for industries such as renewable energy, electric vehicles, and digital technologies[12]. On this basis, and the focus of this paper, the EU framework provides significant illumination as to how, at least broadly 'Western', states conceptualize the management of supply risk.

A pivotal document supporting the CRMA is the "Study on the Critical Raw Materials for the EU 2023 – Final Report." This report provides a detailed assessment of the supply risks and strategic importance of various raw materials for the EU[117]. It screened 70 candidate critical raw materials for two variables: economic importance and supply risk[13, 117]. Through this selection process, the report identified 34 CRMs, and 36 strategic raw minerals[8][117].

By accounting for the cost and performance of different CRMs; production, criticality, and co-production; Global Supply concentration (HHIGS)and EU Sourcing concentration; country governance; import reliance; trade reliance; and supply-chain bottlenecks, the report provides a foundational outline[12] for how the EU conceptualizes supply risk, as based on global supply and prices. It should be noted, however, that much like the US GSG's framework (for example), the EU study does not account for aggregate risk. The Supply Risk index (SR) does not appear to account for market and financial risks such as currency risk, nor does it account for the price volatility of the different CRMs

[8] Or 'SRMs'. Note that Copper and Nickel under this EU framework do not meet the criteria of CRMs. Strategic minerals are distinct from CRMs in that they additionally are relevant to defense infrastructure, which falls outside the purview of critical infrastructure as defined by the EC[117].

on the international market[13] - a proxy for aggregate risk[124]. This report does not disaggregate risks, either; it does not explore the individual qualitative risks to which the supply-chains of each mineral are exposed[13].

1) Strategic v. Critical Minerals

Not all legislative frameworks conceptualize increased security through supply diversification and green policies. A particularly unusual, but illuminating, example of frameworks for ascertaining and planning to deal with the risks associated with critical minerals lies in the Chinese conception of mineral criticality, as outlined by the People's Republic of China Five Year Plans from 2016 onwards[122]. Under a specific, almost offensively realist conceptualization of foreign policy and strategy, different Chinese sources have constructed mineral criticality in a number of different ways, particularly in the delineation of 'strategic minerals'[122].

In 2002, three influential papers were published in Chinese-language discussions on "strategic minerals."[122] The first, authored by the former head of the China Geological Survey (CGS), defined strategic minerals as,

> "...minerals that are indispensable for the country's economy, social development and national defense, that cannot be guaranteed domestically, and that can influence the international market."

[122, 125]. Qi provided a similar definition, emphasizing three elements: pertinence to defense and economic activity, reliance on imports during wartime conditions, their necessity for national defense and economic development, and the degree of supply risk to which the domestic supply is exposed[122, 126]. Finally, Zhang[122, 127] defines strategic minerals as,

> "...minerals that are essential for national security, for which domestic supply cannot meet demand and the foreign supply situation is unreliable – to a point where there is a danger of urgent supply shortage."

Following these papers, subsequent discourse on strategic minerals progressed, with authors such as Wang defining these resources as crucial for a country's development, stability, and competitiveness, considering their abundance an indicator of national strength[122, 128]. Chen and Wang further expanded this definition by stipulating two criteria that resource must meet to be considered a strategic mineral: high reliance by China on foreign exports, or the vulnerability of "economic security and national defense" to supply and price volatility[122, 128].

This approach culminated in the 2016 establishment of an official catalogue of 24 strategic minerals, which includes rare earth elements, tungsten, and molybdenum, among others[122].

As seen above,'Strategic minerals' are a concept without a uniform definition[122]. Andersson et al.

identified six, frequently overlapping, criteria that must be met for a mineral to be considered strategic within a Chinese paradigm[122]. These are:

1) Importance for economic development/security
2) Importance for national defense
3) Supply risk
4) Substitutability
5) Minerals deemed important for developing China's Strategic Emerging Industries
6) Minerals that China has in abundance and for which it holds a competitive advantage relative to other countries.

This strategic orientation, referred to by Brady as an ”realist theoretical mindset,” views competition for resources as a key driver of global politics[122, 129]. Such an orientation of Chinese strategy cannot be observed in the differing analysis of supply risk for pertinent minerals between domestic and foreign authors. Direct evidence of this is sparse, as there is a lack of available literature by domestic authors regarding risk frameworks[122]. What can be observed, however, are the strategic policy actions of the Chinese Communist party.

The Chinese state is widely perceived as taking a strategic approach to mineral resources[122]. This perception is partly rooted in China's history as a centrally planned economy, where state planning of mineral resource exploration and exploitation has been a key characteristic[122, 130]. According to Economy and Levi[122, 131],

> ”...the state continues to play a dominant role in guiding resource investment and pricing. And concern over resource security remains a central focus of Chinese decision makers.”

This strategic approach extends to China's overseas pursuit of resources, with Chinese firms securing supplies of strategically important raw materials worldwide through state-directed investment and state-backed capital[132].

Perceptions of China's strategic approach to raw materials are reinforced by its application of protectionist policies, particularly regarding REEs[111, 122, 131]. These measures include extensive use of quotas and taxes, restrictions on foreign firms' involvement in the REE supply chain, and concentration of production and export among a few large companies[111, 122, 133]. China's dominance in the REE market, as of 2023, is pronounced: Chinese entities held financial interests globally in 63% of REE production, 11% of cobalt and copper production, 13% of lithium production, and 6% of nickel production[111]. Therefore, when combined with aggressive foreign investment in supply-chains via the B&RI and accusations[134, 135], some of which are well founded in the analysis of contractual clauses[136], of deliberately aggressive foreign policy via economic means[9], it is clear that at least based on appearance, there is a distinct demarcation between policies and frameworks which take a purely ’defensive’ approach and those that do not.

G. Realism, Minerals, Supply-chains, and Weaponization

As this paper adopts a offensive realist approach, it behooves it to examine existing literature in the field of Security Studies and International Relations on the topic of CRMs and supply-chains. There is one problem with this: namely that there are very few articles that directly discuss the supply-chains of CRAs in a strategic contemporary context.Additionally, this review did not find any literature examining this question from a systems perspective and a realist lens. Nor is there seemingly any apparent applied framework for induced risk between geopolitical actors appears to exist, except those models identified in Section III-D.5, never mind one orientated around CRMs in particular.

Under a strictly realist framework, and in direct opposition to conventional liberal and neo-liberal thought, economic interdependence is a direct prelude to warfare[140]. Within a realist framework, therefore, does the practice of weaponizing risk operate under the same logic as warfare by operating as an extension of it?

Inferences can be made regarding the nature of system risk, economic interdependence, and state behavior; however, this paper is not particularly concerned with answering the question articulated in the previous paragraph, only in providing a framework as to how to do so. If a state wished to implement weaponized risk under the same logic as warfare, that is its prerogative.

What is certain is that states do weaponize of different critical assets and supply-chains. One of the most important articles identified in this review is Glencross’ *’The geopolitics of supply chains: EU efforts to ensure security of supply’*, where he discusses not only the reliance of the EU on Chinese supply of CRMs, and the genesis of the EU CRMA as a direct response to shifting EU attitudes towards open markets, but also the deeper existential security concerns of the EU regarding China’s dominance in the CRM supply-chain[141][10].

Glencross provides a vital insight in his exploration of Farrell & Newman’s weaponization of ’economic interdependence’[141, 142], citing examples such as Chinese economic retaliation to Japan regarding the Senkaku Islands in 2010 by temporarily freezing the export of CRMs[141, 143]; and the export restriction of Gallium, Germanium, and Graphite to the EU arising from US-China tensions[141, 144, 145]. These actions are indicative of a wider pattern of behavior, as exemplified by an increase in Chinese export restrictions by a factor of nine between 2009 and 2020[141, 146].

[9] This is by no means a uniform consensus[137–139].

[10] See sub-section III-F.1 for the discussion of China’s positioning in the CRM supply-chain

It is clear that asymmetrical system networks carry with them the potential for weaponization[140], whether in the form of weaponizing currency risk[140] or reducing the supply of state-of-the-art computer chips[141].

When supply-chain disruptions are mapped to deliberate hostile activities, be they during explicit times of war or during nominal peace, actions by state actors essentially constitute a concerted effort to induce risk in the systems upon which an opponent is reliant.

1) Logics

How then does the literature describe different strategies to leverage such risk. There are prominant examples in the field of security studies that discuss the implementation of assets in different strategic contexts. One of these examples can be found in Ding & Dafoe's article *The Logic of Strategic Assets: From Oil to AI*[147], where they provide a simply linear framework for determining the *'strategic level of an asset'* (*SLA* as

$$SLA = Importance \cdot Externality \cdot Nationalization \tag{1}$$

Where in the above[147], *'Importance'* refers to an assets' military or economic utility; *'Externality'*, is the "the economic and/or security externalities associated with an asset, such that uncoordinated firms and individual military organizations will not optimally attend to the asset;" and *'Nationalization'* is "...the degree to which these externalities are rivalrous between nations."

According to Ding & Dafoe, cumulative-strategic logic encompasses strategic assets and dependent industries characterized by significant entry impediments, including "...first-mover dynamics, incumbency advantages, economies of scale, or other cumulative dynamics," and include complicated technology reliant upon cumulative investment that often leads to insufficient investment by the market in these assets. The assets characterized by this logic include aircraft engines, computer infrastructure such as servers, and military equipment that requires high budgetary expenditure due to complexity[147].

By contrast, assets dictated by infrastructure-strategic logic that the market does not readily supply and under-invests in, such a railroad infrastructure[147]. These "foundational" assets generate, "positive spillovers across the national economy or military system, in which subnational actors (for example, firms or military branches) underinvest because they do not appropriate all the associated gains."

Finally, Dependency-strategic logic governs assets such as CRMSs - where the supply-chains the provide said assets are subject to disruption by an opponent due to, "...the physical, organizational, or national concentration" along the supply-chain[147].

These logics are not mutually exclusive, indeed Ding & Dafoe propose a set graph as a representation of this intersecting conceptual model, see Fig. 2.

Not only are these logics subject to false positives and negatives[147], but it is unclear where one logic ought to be employed over another due to the dependent nature of technology on input minerals. As Ding & Dafoe stipulate, for example, computer chips occupy the intersection of all three logics while raw minerals occupy the dependency-strategic logic portion of the framework[147].

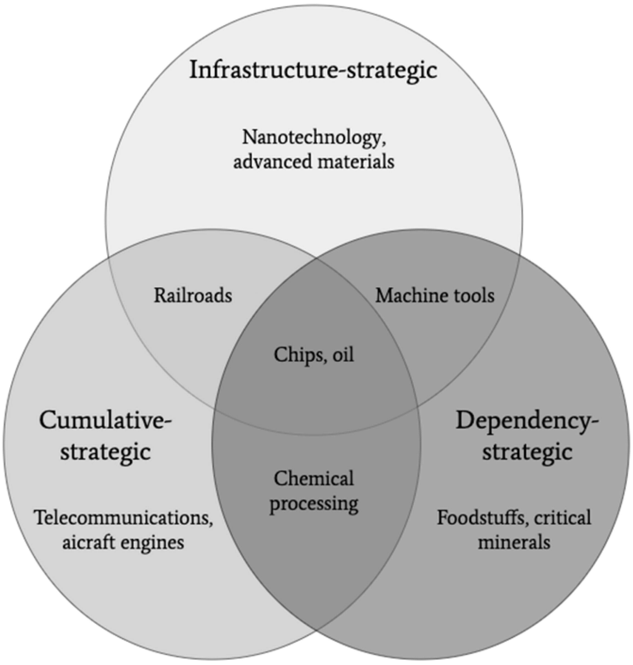

Fig. 2: The strategic logics in combination[147]

The question that remains is where one ends and the other begins. One might argue at the point of manufacture, but that is an insufficient answer. If, for example, the Chinese state were to attempt to strangle the supply of input CRMs necessary for the manufacture of the most state-of-the-art chips made by Taiwan Semi-Conductor Manufacturing Company (TSMC), it is entirely feasible to argue that not only are both the chips and the input minerals subject to dependency-strategic logic but so are all of the infrastructure-strategic logic assets that are affected by this shortage and the actual implementation of the restrictive Chinese policy as well.

Therefore, such a rigid framework violates the holistic approach necessitated by systems design, as explored in sub-section III-D.3. Subsequently, a research and implementation gap exists between the analysis of weaponized CRM supply-chains, risk, and systems thinking, which ought to be engaged.

H. Critical Infrastructure Sectors

This sub-section of the literature deals with different classifications and definitions of critical infrastructure and different associated sectors; it is split into three elements: a description of the literature investigating critical infrastructure, the definition and orientation of the European Union with regards to critical infrastructure and critical infrastructure risk management, and the parallel of these considerations in the United States.

Broadly, critical infrastructure pertains to those supply-chains and/or assets the absence of which would be catastrophic for the continued operation of a nation, be they related to economic activity, state organ operation, or the military apparatus[148]. In the context of highly interconnected contemporary systems, upon which the security of sovereign states are dependent, critical infrastructure is the subject of intense policy manifestation and risk management[149, 150]. This is especially true given the increased interdependence of critical infrastructure systems across national boarders[11], as bound by not only shared infrastructure but also shared supply-chains for the resources necessary for continual operation[149]. Such complex interdependence could result in what Barbar & Ali term a domino effect, where an attack or disruption to a critical infrastructure system could result in a subsequent knock on effect on other critical infrastructure sectors across one or more nations[149, 151].

Having now contextualized the concept in the more abstract, it is now necessary to explore the specific legal understandings of critical infrastructure. In this case, this literature review provides both an overview of U.S. and EU conceptualizations of critical infrastructure. As per the EU *DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, critical infrastructure is defined as[152],

> ”...an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service.”

These different critical infrastructure sectors as maintained by different critical entities - private or public sector legal entities that are identified by a Member State of the EU - an fall into any one of the eleven different critical infrastructure sectors, as can be seen in the Annex of the Directive. Critical infrastructure sectors are defined as belonging to either the energy, including electricity, oil, gas, hydrogen, and district heating and generation; transport, consisting of air, rail, water, road, and public transport; banking; financial market infrastructure; health; drinking water; waste water; digital infrastructure; public administration; and space sectors[152, 153]. It should be especially noted that this directive does not apply to critical entities concerned with national defense, except in edge cases where critical entities are only tangentially concerned with defense related infrastructure[152].

Risk management of supply-chains and critical infrastructure is a central concern for the EU[152] and other actors[149]. As the EU directive states[152], major crises such as the COVID 19 pandemic stressed supply-chains significantly[8], revealing or exacerbating weaknesses in critical infrastructure sectors that were hereto for unforeseen[8], especially regarding raw minerals and the mining sectors[154], as well

[11] The systems complexity incurred by this reality necessitates systems of systems (SOS) engineering thinking criteria, see Section III-D.3.

as increasing prices and price volatility[155] - the latter of which is a proxy for aggregate risk[124].

Failure to include defense in risk analysis and management of critical infrastructure is therefore puzzling. National defense is paramount and inherently intertwined with critical infrastructure. Not only were key pieces of infrastructure developed as the result of military R&D[156], but defense infrastructure frequently shares supply-chain dependencies with civilian critical infrastructure[157].

To account for this limited scope, other critical infrastructure frameworks were investigated. Another definition and delimitation of critical infrastructure is provided below in the form of the U.S. Cybersecurity and Infrastructure Security Agency's list, which remediates this limited scope by providing a much more comprehensive breakdown of critical infrastructure sectors, classifying them in the following manner as per Presidential Policy Directive 21 (PPD-21)[158, 159]:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems

When contrasted to the policies and frameworks of the EU, it is clear the U.S. employs a far more comprehensive approach when PPD-21 is further contextualized in relation to more recent policy developments regarding securing different supply chains that feed and are reliant upon different critical infrastructure sectors. This is especially true with regards to the *'Defense Industrial Base Sector'* with the publication of public documents such as the *'Securing Defense-Critical Supply Chains'* action plan that was developed in response to U.S. President Biden's Executive Order 14017[120].

In conclusion, critical infrastructure is a key classification that encompasses the assets and systems necessary for different nations' security, functioning, and prosperity. The different sectors of critical infrastructure are interrelated and differ in classification from block to block or nation to nation. As these sectors are both reliant upon and integral to different supply-chains, especially CRMs, it is necessary to consider the impact of risk on supply-chains as ultimately reflected in the behavior and operational status of these critical infrastructure sectors.

IV. Methodology and Theoretical Framework

A. Overview

As articulated in Section II, this paper creates a framework, from an offensive actor's perspective that seeks to attack the European Union, using the Design Science Research (DSR) paradigm. This paradigm seeks to create socio-technical systems[160] in the form of an instantiated artifacts[161]. In this particular instance, the instantiated artifact is a framework which provides a map of how to offensively leverage weaponized risk can be employed against supply-chains.

This iterative framework is to be multi-functional - it can be employed to investigate both offensive and defensive postures of different actors, both theoretical and real; it also may be iteratively employed to update scholarly knowledge regarding existing supply-chain vulnerabilities and their contextualization within a greater realist understanding of economic coercion and supply-chain warfare.

In other terms, the final outcome of this paper is a nascent design theory[12] or design framework that draws on existing knowledge to provide a structured approach to operationalizing weaponized risk.

An offensive actor's perspective is assumed for two reasons:

1) To bridge the gap between offensive frameworks that analyze supply-chain vulnerabilities and existing literature on how different geopolitical actors seek to mitigate or effectively induce risk in CRM supply-chains.
2) To gain further insight into potential vulnerabilities that are not easily conceptualized from a defensive perspective.

To meet the criteria set forth by DSR, the delivered framework will be defined in accordance with Johannesson & Perjons four components of a framework[162], which are:

1) "A number of logically related activities, with well-defined input and output."
2) "Guidelines for carrying out the activities."
3) "Guidelines for selecting research strategies and methods to be used in the activities."
4) "Guidelines for relating the research to an existing knowledge base."

[12] Referred to in DSR as a 'Level 2' contribution[160].

The proposed project adopts an empiricist, post positivist approach to creating a framework aligned with the dynamics of socio-technical systems. Because of asymmetric information, the very nature of risk and uncertainty demands such an approach due to the inability to grasp all probabilities of all events.

Subsequently, the following sub-sections deal with the following elements: the research questions that this paper seeks to answer; the definition of risk and models of risk adopted in the pursuit of creating the framework articulated above; the alignment of this framework within both the security studies field and the design science research framework as an novel contribution to both fields; the conceptualization of weaponized, or induced, risk and its bearings on risk management frameworks (of which the paper herein constitutes one); problem scope; how weaponized risk figures into both offensive and defensive realist narratives and understandings of the international order, as well as the relevance of this subject to the strategies that may be employed by different actors; the material and methods employed in the pursuit of the creation of the articulated artifact, including the data sources, types of data, data handling, measurement of aggregate risk, methods of risk disaggregation, and identification of different attack vectors.

To generate the framework presented by this paper, the following research questions were generated and answered in chronological order to provide a basis for both exploration of historical and contemporary exploitation of supply-chain risk, and to then identify how these examples may be applied to contemporary supply-chains. These questions are itemized as follows:

- RQ_1 To what extent have different attempts by states and their proxies to weaponize risk been successful?
- RQ_2 Which supply-chains exhibit potential for exploitation?

Answering RQ_1 allows for this paper to synthesize different case studies and examine the differing methods in which risk can be induced. In essence, it allows for the generation of different risk-induction techniques from proof by induction. Subsequently, with RQ_2, potential targets, and even novel techniques, can be explored through the examination of European Union economic and military supply-chains leading to a list of potential targets and attack vectors. However, since this framework deals with a hypothetical opponent, it would be difficult to appraise the feasibility of attacking different targets via the determined attack vectors without hypothesizing as to the tangible and intangible assets that an opponent could leverage.

B. Theoretical Framework

1) Alignment with the Security and Strategic Studies Fields

Pursuant to the requirements of the Charles University Masters of International Security Studies course, and inline with the field of Security Studies, as well with the field of Strategic Studies, the following sub-section outlines the ways in which this Master's dissertation provides novel contributions to the academic literature and broader strategic understanding of risk, supply-chains, and CRMs.

Risk as an analytical concept, despite its ubiquity in the fields of finance, economics, supply-chain management, engineering, and military thinking[13], is surprisingly absent as an employed tool even in light of its potential utility[163]. Such a striking absence provides an opportunity to broaden empirical understandings of risk, beyond purely military domains to include economic, cultural, and financial, as identified by authors such as Petersen[163]. This, in turn, allows for the investigations of security matters as they relate to specific state policies and practices in numerous fields from airport security to terrorism[163], especially in light of the rise of risk as a conceptual touchstone that appears to be superseding 'threats' and 'security' as dominant frameworks[163–165] due to an increasing lack of well defined rules on the international stage which transcend "space and time" and the limited scope of 'threats' as a concept in a post-Cold War context[166].

As previously discussed in Sections III-B.2 and III-D.5, there are no apparent applied frameworks that provide insights into how risk may be induced/weaponized to lessen an opponent's access to critical assets, namely CRMs, to which the opponents behavior is clearly bounded by different strategic logics. If it is in the interest of future researchers to investigate how aggregate actors may act in light of shifting access to CRMs, it is necessary to understand how an opponent may weaponize risk. Otherwise, strategic understanding of how the European union may react defensively will be diminished in applicability and scope.

Subsequently, when contextualized with a systems understanding of risk, it is clear that the non-linear nature of the supply-chains which underpin the provision of CRMs to different nations necessitate a holistic technical understanding of risk as demanded by the amorphous post-Cold War geopolitical field. The lack of existing implementations of risk in the field of security studies from a technical orientation also provides significant novelty and is therefore deemed to be a worth endeavor.

This is novelty rings true especially in regards to material realist conceptions of international relations and security. Mearsheimer, the great proponent of offensive realism, conceptualizes the anarchic international order and the desire of power by states as systems as arising from the hegemonic ambitions of state actors. Therefore, by assuming offensive realism as an axiomatic system condition, this paper

[13] See Section III-B

can more deftly construct a theoretical opponent with adequate justification for inducing risk in the supply-chains of different critical minerals.

In increasing uncertain times, where powerful political actors such as the United States, the EU, Japan, China, and others are increasingly defining their strategic orientations around access to different CRMs, and in light of the research gap identified in this paper's literature review, and the above paragraphs, a sufficient alignment with security studies as a field is established.

2) Alignment with Design Science Research

Design Science Research (DSR) is a systematic approach to designing prescriptive artifacts through a process of deliberate, holistic design to solve problems in applied, real-world, domains[167]. As an applied methodology, DSR is concerned with creating knowledge regarding the different permutations in which problems can be tackled and solutions made manifest[167]. This knowledge is manifested by novel, "constructs, models, methods, and instantiations," which directly cotribute to the solving of specific and/or general problems[160, 167]. This research paradigm is multi-disciplinary, and extends beyond engineering and systems to include economics, and other fields[167].

DSR operates initially from the identification of a *'problem space'* defined by the, *'phenomena of interest'* that exist within the bounds of the problem[167]. These phenomena include the[167], "...people, organizations, and existing or planned technologies." This conceptual environment contains in it the objectives, necessary activities, problems, and potential avenues of problem remediation - *as identified and held specifically by the stakeholders of the system* - and are bounded by the needs of said stakeholders, as contextualized by the current strategy and existing practices of the problem owner[167]. Furthermore, the needs of each stakeholder are, "...positioned relative to existing technology infrastructure, applications, communication architectures, and development capabilities."[167]

All of these considerations in interest are synthesized to generate a unified research problem that is to be solved by the designer or researcher that assumes the task. Only by doing so can stakeholder requirements, even if the stakeholder is theoretical, be satisfied and therefore be considered relevant research worth the endeavor[167].

As shown in Fig. 3, in DSR, three broad elements are of prime importance: environment, design, and knowledge base.

The environment, provides the relevance to the design, and the applicable knowledge provided for by the knowledge base contributes the necessary rigor for the design. These processes are iterative, with each successive pass through the design cycle contributing to both the knowledge base and changing the environment in which the design is situated[167].

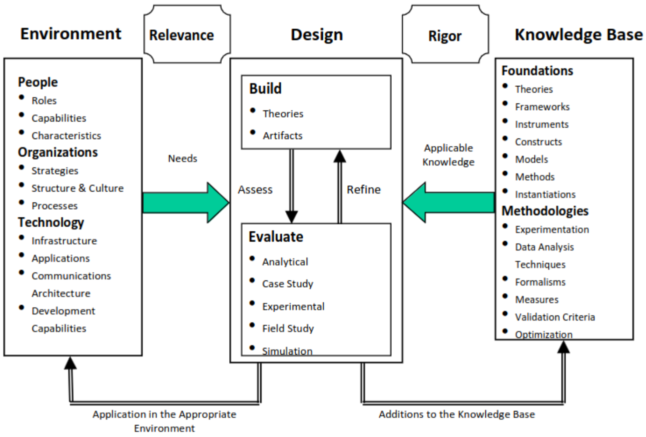

Fig. 3: Design Science Research Framework[167]

The activities for this model are separated into five processes, of which only four are relevant for this paper: problem identification and definition, defining the objective, creating the artifact (the framework), and applying the framework[167]. The implementation of these steps are found in Section IV-E.

The end contribution of these steps is called the artifact - the[160, 168], ”thing that has, or can be transformed into, a material existence as an artificially made object (e.g., model, instantiation) or process (e.g., method, software).” Through the conceptualization, design, implementation, and/or evaluation of this model, the design science research methodology generate what is referred to as *’design knowledge’*[167].

For a DSR project to be considered as contributing design knowledge of sufficient merit, the research project must either apply a novel solution to an existing problem, a novel solution to a novel problem, or an existing solution to a novel problem, as can be seen in the Fig 4.

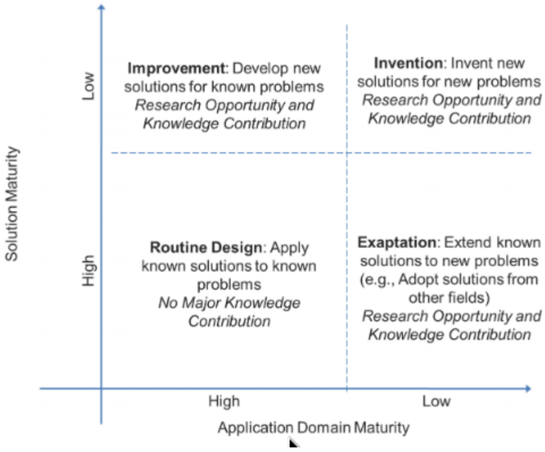
Improvement: Develop new solutions for known problems
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems
Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
Low
High
Solution Maturity
High
Low
Application Domain Maturity

Fig. 4: DSR Knowledge Contribution Framework[160]

The solution domain maturity is considered high; as discussed in the literature review, the concept and application of risk management and risk analysis in both security and other contexts is a well established practice. However, because risk analysis in a technical sense has seldom been applied as an overall framework with regards to critical rare earth minerals in an offensive orientation, let alone in the context of security studies as a field, this paper asserts that the application domain maturity is considered to be low. On that basis, therefore, the framework that is designed and implemented in this paper could be considered as contributing extrapolation as it's design knowledge contribution.

This particular paper contributes what is referred to as *'Level 2'* design knowledge, which can also be described as a *'nascant design theory'*, exemplified by artifacts such as[160], "...constructs, methods, models, design principles, technological rules."

3) Post-positivism and Risk

As risk analysis is inherently probabilistic, the framework and implementation to CRM supply-chains adopts an empiricist post-positivist approach. Such an approach necessarily integrates empirical evidence with a nuanced understanding of scientific theories, with the understanding that all knowledge is fallible and open to revision, as are all different contextualization of specific risk.

It is for this reason that post-positivism is employed as a part of this paper's conceptual understanding of risk, aligned with the adopted definition of risk provided for by ISO 31000, as post-positivism maintains that while objective truth exists, an understanding of it is inherently imperfect. This approach is particularly relevant in risk analysis, where empirical data must be interpreted within the context of complex and often uncertain environments - in other words, exactly those contexts where supply-chains are subject to risk in the geopolitical arena.

Additionally, the adoption of DSR more or less mandates this theoretical approach to risk analysis given the iterative nature of that methodology. Only through continual design and redesign can further design knowledge and contributions of sufficient rigor be created.

Thus, given the stipulations described in this sub-section, it is necessary to adopt an empirical approach, else there is no basis for using a probabilistic tool like risk for analysis, especially in complex systems where variables interact in unpredictable ways.

This approach aligns with the necessary problem definition and solution design mandated by stakeholder needs via the DSR methodology[14], and allows for a more rich orientation and attribution of risk to different actors in the supply-chain.

4) Adopted Definition of Risk

In this thesis, risk is defined by the following statement, copied exactly from ISO 31000:

[14] Section IV-B.2

> ”The effect of uncertainty on objectives, whether positive or negative.”[41]

This definition is adopted on the following two bases:

1) that the definition of risk provided by ISO 31000 aligns with the EC’s definition of risk, as defined by the EU directive 2022/2557, which states that[152],

   > ”Risk means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.”

2) and because in doing so, better alignment with the retooling of risk management techniques described in ISO 31010:2009 may be achieved.

It is critical to note that the one deviation between ISO 31000’s definition of risk and the definition put forth by the EU directive 2022/2557 is that the latter narrowly describes risk as being bound to only the negative consequences born by the stakeholders in critical infrastructure and related supply-chains, and being tied to an inciting incident. In essence, adopting such an understanding of risk narrowly limits the applicability of analysis in two manifestations. The first manifestation is that risk becomes somewhat linear in attributing its manifestations and the responsibility of who bears the consequences of risk.

Using EU directive 2022/2557’s risk definition bounds the effects of stakeholder and offensive actors actions to single-incidents and limits the conceptualization of weaponized risk by limiting the objectives of an attacker[15].

Narrowly defining risk as ’one-sided’ implies that any risk assumed may only manifest in a negative consequence. Subsequently, risk management on the part of defensive actors can only be tasked with mitigating adverse effects. Such a framing of risk violates best practices when dealing with the non-linear phenomena to which supply-chains are exposed, and implies that risk induction cannot fail by virtue of sufficient supply-chain resilience leading to improved resistance to attack.

Secondly, because risk is not necessarily discrete, the attribution of risk to single incidents limits the utility of risk models in understanding the actions and motivations of opponents. Adopting IS0 31000’s definition of risk, which does not have this stipulation allows for the attribution of risk-induction to multiple activities over an extended period of time.

5) The Conceptualization of Weaponized, or Induced, Risk

Referring back to Section III-D.5, the literature review found a lack of offensively orientated frameworks orientated around supply-chain risk. In any complex system that is owned or incorporates any number of stakeholders and their complex interrelations, the apportionment of risk is always a chief

[15] See Section IV-B.5

concern. Thus, when discussing how risk should be treat conceptually with an offensive perspective, the question must be asked as to whose risk is being increased as a direct or indirect result of the actions of one or more actors along a supply-chain, or even outside of it.

This question leads to the development and definition of the concept of weaponized, or induced, risk. Weaponized risk is defined as the following:

> The increase of either specific risk, and/or aggregate risk, in a supply-chain as the result of a deliberate course of action on the part of a state power, the organs of a state, or an aligned private entity beholden and/or loyal to a state. Weaponized risk is induced directly within the supply-chain or any adjacent system of sufficient importance.

Above all, this conceptualization of weaponized risk mandates that an increase of aggregate risk through specific risk must be deliberate - it must arise from a purposeful, deliberate set of actions on the part of one, or even more, actors. Weaponized risk does not, however, necessarily require a specific target as far as state actors go. So long as the supply-chain in its entirety exhibits an increase in either aggregate risk, or specific risk, that is sufficient.

Furthermore, extra emphasis must be allocated to two stipulations. The first is the understanding that weaponized risk need not necessarily be successful. It may be the case than an offensive actor will move to induce risk across a supply-chain with sufficient resilience in the form of absorptive, adaptive, and/or restorative capacity[16] to offset the increase in aggregate risk generated by an attack. Additionally, due to the non-linear nature of risk and complex supply-chains, weaponized risk as a concept must anticipate the reality that there also exists the theoretical condition where aggregate risk does not materially increase beyond manageable levels despite a sudden or significant spike in an instance or class specific risks.

Secondly, while risk weaponization inevitably deals with n^{th} order consequences, the effects of deliberately induced risk must not be too remote. Otherwise, when taken to the extreme, the concept of weaponized risk could essentially render any state action under an offensive realist framework as a form of weaponized risk. This would render the concept of weaponized risk as overly broad, subsequently severely the utility of the framework in future analysis. Therefore, for a particular instance risk weaponization to be considered as a valid example or implementation of the phenomenon, the policies or actions undertaken to induce such risk must either:

1) Exhibit provable motive on the part of the attacker to deliberately induce risk in a particular supply-chain.
2) or induce non-trivial damage to a supply-chain element or system.

[16] Refer to Hosseini et al.[67] and Section III-D.1

C. Scope and Delimitations

To prevent the excess bloat and to fulfill the requirements of this exercise, the system scope is narrowly bounded to examining how the supply-chains of CRMs may be exploited by an offensive actor against the European Union and its constituent states. The system scope is also narrowly limited to application of the framework to selected CRMs over the time period of the end of January, 2020 until the 31^{st} of December, 2023 - the duration of the COVID 19 pandemic. This time-frame was used under the assumption that periods of high stress reveal vulnerabilities in the supply-chains of different assets. As much can be inferred through the prices and volatility of the different CRM commodities identified in the EU CRM report.

Using Fig 5, the overall system context is illustrated, showing the orientation of the generic supply-chain *n* for an investigated mineral, creating a representation of the overall system scope that to which the instantiated framework is applied.

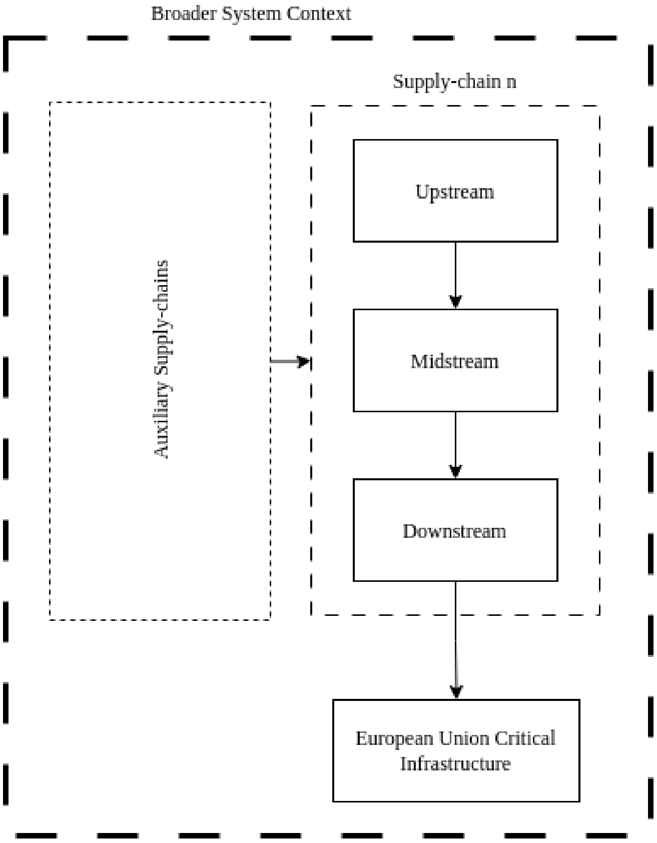

Fig. 5: System Scope

Mineral supply-chains are separated into two components: upstream and downstream[169]. Upstream components are those activities in the ”...production and sale concentrated and refined minerals,” including trading and transportation[169]. Downstream supply-chains are those processes that use mineral derivatives or refined minerals and also include trading and transportation[169]. For this paper, transportation previously assigned to upstream supply-chains is disentangled into a third category of the supply-chain: midstream.

The framework developed does not primarily concern itself with the very real potential of an opponent targeting the supply-chain of a CRM that acts a crucial input for a good manufactured in a third country upon which the European Union is reliant. That is to say the scope of the framework provided by this paper is concerned with the upstream, midstream, and downstream elements of different CRM supply-chains from extraction all the way to delivery to European soil. To expand the scope of the framework to targeting supply-chains globally to disrupt the flow of all manufactured goods reliant on selected CRMs would no longer constitute a framework in line with a 'mid-range' design theory[17], but either a policy prescription or grand theory.

The supply-chains for magnesium are aligned with various products that European critical infrastructure is reliant upon, but the scope of analysis is limited to the supply of magnesium itself, and those commodities which contribute to those supply-chains, nothing else.

The model provided in Fig 5 does not describe all of the stakeholders that assume risk in each sub-system, supply-chain, or unit of critical infrastructure as these are idiosyncratic to the specific supply-chain for each mineral and specific category of critical infrastructure. The identification of specific stakeholders is considered following the desegregation of risk and the investigation of specific risks pertinent to each specific minerals.

Additionally, this paper is not concerned with generating predictive hypothetical statements regarding the potential future actions of actors. The framework is not concerned with the potential actions of the Russian Federation, the People's Republic of China, or any other actual political actor and how they may seek to leverage risk to attack. To do so would be require the attribution of political will based on a historic pattern of behavior as exhibited both in strategic documents and strategic action. While this paper will draw on the contemporary and historical strategic documents and actions of different states as a road-map for how a hypothetical offensive actor may attack supply-chains, predictive statements regarding the future actions of political/national entities would fall outside of the scope of the four components of a framework identified by Johannesson & Perjons[162].

The nature of the actors identified as conceptual reference points in this framework is also crucial. In this particular, initial iteration of the framework, only the offensive actor is constructed as a hypothetical. The defensive actors, however, are not theoretical constructs. They are instead clearly delineated as those member states of the European Union who are subject to the CRMA.

[17] See IV-B.2

1) *Theoretical Aggressor*

The theoretical opponent which is constructed by this framework to act in an aggressive or offensive manner is defined as pursuing the following set of objectives:

1) The induction of risk that must be borne directly by the defensive object's stakeholders, resulting in either:
    a) A directly increased risk burden for a state in the European Union pertaining to a critical infrastructure sector.
    b) Indirectly increasing the risk burden for a state in the European Union, pertaining to a critical infrastructure sector, by increasing specific or aggregate risk held by critical supply-chain stakeholders outside of the European Union.
2) Induce risk directly to the supply-chain of selected CRMs themselves, not third-order risk

This reasoning is also why offensive realism is adopted as a conceptual framing for the final artifact presented in this thesis: by the very nature of realism, states are assumed to be the final resolution of different actors. With absolute certainty, this is both a necessary abstraction and a limitation of the model. By constructing such hypothetical actors, the nature of an aggressive opponent that seeks to leverage risk renders the different public and private actors acting within a state's boundaries as organs of said state. Thus, as entities separate from states, the ultimate framework provided by this thesis does not consider edge cases like private military companies (PMCs) or other non-state actors engaged in risk induction during operations, military or otherwise. Instead, non-state actors are reduced to either organs or tools, allowing for the reduction of framework complexity.

Adopting offensive realism also allows for the simplification of offensive actor motivations and actions. While an offensive realist understanding of nation-state behavior does not demand that they utilize risk weaponization to maximize risk for their opponents at all times in the short-medium term, it does allow for this particular model to bind the objectives of an offensive actor for aggregate risk maximization of their opponents' assets in the long term.

D. *Problem Definition*

This investigation and framework adopts the following statement as the definition of the primary problem that is addressed by the implementation of the methodology outline in Section IV-E:

> A lack of systemically orientated frameworks that address how an aggressive actor could seek to induce risk in critical supply-chains poses defensive risks to European critical infrastructure stakeholders. The risk management framework instantiated by the CRMA does not actively

consider how an opponent may seek to destabilize the supply-chains that the CRMA seeks to increase resilience.

E. Methodology - Stages of Processing and Analysis

Section IV-E is an overview of the different stages of analysis that are undertaken to provide the model generated by the activities of this paper, and how disaggregated risks are applied to the specific CRMs selected for analysis.

Analysis is split into six discrete stages. *Stage 1*, consists of the identification of minerals, *outlined in the Study on Critical Raw Minerals for EU 2023 Final Report*, that are at particular risk, as described by the *supply risk* (SR) and *economic importance* (EI) indices set forth in Annex II of the European Commission's *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020.*[13]. The top ten CRMs that are identified as the highest in SR and EI are selected for further selection.

It is important to note that this report truncates certain minerals into categories instead of individual commodities, most notably heavy rare earth elements (HREEs) and light rare earth elements (LREEs). The EU report on supply risk for CRMs also does not consider the different purities and forms that different minerals are processed into and shipped. Magnesium, for instance, comes in many different alloys and forms, be they powdered, ingots, or otherwise, and thus, a more granular analysis of these volatilities is warranted given their potential impact on the different risks in the upstream, midstream, and downstream portions of relevant supply-chains. Additionally, not all of the minerals encapsulated by the categories of HREEs and LREEs are analyzed due to missing price information.

In *Stage 2*, these minerals are then identified as potential targets for inducing risk events for future alignment with critical infrastructure sectors and desegregation in *Stage 3* and *Stage 4*. Since *SR* and *EI* fail to completely capture all aggregate risk due to not using price signals and relying on only one index for all political, legal, and cultural risk, this paper argues that it is necessary to quantify the aggregate risk through other measures in *Stage 2*.

This quantification is facilitated through examination of historical price volatility[18], as defined by the European Union's absolute historical volatility indices[170].

Subsequently, the initial list of candidate raw mineral targets is refined to one category of minerals. This selected candidate is then aligned with critical infrastructure sectors, in line with the European

[18] In line with Modern Portfolio Theory, where price volatility, actual or implied, is a proxy for aggregate risk[124].

Unions definitions, by delineating each different, notable, manufactured product reliant on each critical mineral[19].

Stage 4, the disaggregation of risks, involves creating a unified set of risk classifications that could affect every identified target for investigation across each critical infrastructure sector. Next, in *Stage 5*, each relevant supply-chain associated with the list of selected CRMs is analyzed for the disaggregated risks identified in *Stage 4*. Qualified or quantified risks are mapped to different vulnerabilities by identifying the producers and users of different strategic minerals and analyzing their operations.

Finally, *Stage 6* identifies different feasible vectors for future exploitation. Feasibility here is qualified based on previous examples of such actions and comparative analysis between previously attempted exploitation of vulnerabilities and the vulnerabilities the project identifies that have not yet been exploited.

Hereafter, the following sub-sections described in detail each of the six stages outlined previously in this part of the paper.

1) Identification of Critical Minerals and Target Selection, Including the Implementation of Price Volatility Analysis

Stage 1 and 2 of processing and analysis consists of the following elements:

1) Pre-selection of the top 10 mineral groups based on the *SR* index from the EU CRM report.
2) Desegregation of different mineral groups such as LREEs and HREEs into groupings based on different chemical elements.
3) Calculation of the annualized price volatilities for each specific mineral type within a mineral group across the investigated time-frame.
4) The creation of a simple aggregate risk index for each mineral group based on simple arithmetic means.

The first portion of processing and analysis relies on the ranking of the *SR* index from 2020, as this index is thought to be more representative of the aggregate risk that was revealed during the COVID 19 pandemic, rather than the preceding *SR* IIncindex values from 2017 or the *SR* index values from 2023. These values were directly taken from the EU 2023 CRM report as .png files, stitched together in GIMP, and then translated into a simple .csv file with Optical Character Recognition using Google's Tesseract[20]. Subsequently, the values of *SR* for 2020 were parsed and ranked in R[21].

As per the EU's *Methodological description and the interpretation of the volatility index for electricity markets*, this paper retools their absolute volatility index model for the price history of those minerals

[19] See Section IV-E.2

[20] For full documentation of the OCR program used, please see the GitHub directory[171].

[21] Consult Appendix X

with available price history as identified during first round of pre-selection.

The next step sources historical price data from the Institute for Rare Earths and Strategic Metals[172] to calculate an index which reflects the aggregate annualized risk for different minerals. As the sourced data does not provide price data for minerals as aggregate commodities, and instead only provides the data for specific forms of minerals[22], the annualized volatility was calculated for each individual available item.

Additionally, not all price information for different elements was available. The final candidate list of mineral groups the for calculation of annualized volatility is as follows:

- Cerium
- Cobalt
- Dysprosium
- Europium
- Gadolinium
- Gallium
- Germanium
- Holmium
- Lanthanum
- Magnesium
- Neodymium
- Niobium
- Praeseodymium
- Samarium
- Scandium
- Strontium
- Terbium
- Yttrium
- Ytterbium

Having now identified the mineral groups, the analysis proceeds to calculate annualized volatility in the following manner:

Suppose the X_i is the log difference of the price between two consecutive trading days in a year at time T over k trading days in a month, where the total number of trading days in a year is given by N. As per the manual from which this method is sourced, the N is given as 252 and k as 25. The expression below gives this relation as,

$$X_i = \log_{10} P_{dayT} - \log_{10} P_{dayT-1} \tag{2}$$

The average log difference, $\bar{X_k}$ is given by,

$$\bar{X_k} = \frac{\sum_k^{i=1} X_(i)}{k} \tag{3}$$

Therefore, the absolute volatility is given by the expression,

$$VOL_{T-k+1,T} = 100 * \sqrt{N} * \sqrt{\frac{\sum_{i=1}^{k} (X_i - \bar{X})^2}{k}} \tag{4}$$

This absolute volatility is calculated for each year during which the COVID-19 pandemic was active

[22] For example, 99.9$ pure Cerium Oxide instead of all Cerium products.

(30/1/2020-31/12/2023), see Appendix XI. Having identified now the price volatility index for each mineral permutation across the investigated time-period, a secondary index was required to rank each mineral type by volatility for final selection. A simple unweighted average was chosen for this purpose, as described by the below equations 5 and 6.

$$VOL_{avg,j} = n^{-1} \sum_{n=1}^{n} VOL_n \tag{5}$$

$$VOL_m = j^{-1} \sum_{j=1}^{j} VOL_{avg,j} \tag{6}$$

In the above expressions, $VOL_{avg,j}$ refers to the simple arithmetic mean of the annualized volatilities for a specific mineral sub-type j over n years[23]. VOL_m, meanwhile, is the simple arithmetic mean of all all $VOL_{avg,j}$ in mineral group m.

For more granular analysis, the Parkinson's Volatility estimator was used to calculate daily volatility using a five-day (trading) window. This volatility estimator uses historical high and low prices, instead of closing prices, to estimate the volatility of an asset or commodity over a period of time[173].

This was accomplished by calculating the volatility for day t by inputting price data from day $t-n-1$, where n is the size of the window. In this instance, five days was chosen as an appropriate window as it is the length of the trading week (Monday to Friday). This reworked version of Parkinson's volatility was provided by ChatGPT.

The Parkinson's volatility for day t is therefore,

$$\sigma_{P,t} = \sqrt{\frac{\sum_{i=t-n-1}^{t} (\log(\frac{H_i}{L_i}))^2}{4\log(2)}} \tag{7}$$

where in the above, H_i and L_i are the high and low prices for day i, respectively. The full R-script for both of these volatility measures can be found in Appendix XI.

2) *Stage 3 - The Alignment of the Aggregate Quantitative and Qualitative Risk with Different Critical Infrastructure Sectors*

By synthesizing the European Union's identified Critical Infrastructure sectors with the 'Defense Industrial Base' Critical Infrastructure sector identified by the U.S. PPD-21, a full spectrum of relevant sectors are generated which can be aligned with any disaggregated risk which is identified as having affected the supply-chain of a selected mineral and mineral group[24].

The criteria upon which these sectors are identified is simply: with the conspicuous exception

[23] See Appendix XII

[24] See Section IV-E.3

of defense related infrastructure, the language of the EU directive 2022/2557 clearly states that the management of risk for these sectors is of prime importance. A theoretical opponent that seeks to attack the European union by leveraging risk would, by the reasoning of Occam's Razor, be irrational to not take word of the legislation on face value. If European Union member states are bound by multilateral obligation to manage the risk of critical infrastructure sectors, it is a reasonable assumption that an opponent would target those pieces of EU critical infrastructure that EU members are obligated to assume risk for.

To that end, the selected mineral groups are investigated qualitatively by identifying their relevance as key inputs or outputs as functions of different critical infrastructure resident in European Union member states.

3) Stage 4 - The Disaggregation of Risks into Different Universal Categories

Risk disaggregation is roughly analogous to the portion of ISO 31000's Risk Identification process, wherein the framework seeks to identify different risks which may result in material consequences on the critical infrastructure and CRM supply-chains arising from risk induced by an opponent. In truth, the methods elected for use in this step are some what arbitrary, and thus this paper has elected to use a framework provided for by Farrell[1] that is orientated around project finance - a form of non-recourse financing for projects the exhibit high capital expenditure[174] that is designed to minimize risk[175]. Note that this is not the form of financing large projects, the sorts that involve assets associated with different supply-chains. However, it is a common method; and on the basis that part of project finance demands the allocation of risk to different parties[175], using Farrell's framework as a starting basis for risk disaggregation is prudent given the large swathe of risks to which high CAPEX investments, often in countries and locations with fluctuating and novel risks[175], is a fairly suitable adaptation of his model.

In his paper, Farrell identifies five broad categories of risk: start-up investment cost risk, operating business risk, technology risk, market risk, and political risk[1]. Concerned as this paper is with existing supply-chain vulnerabilities and the leveraging of risk against both investment and trade activities, the scope of risk disaggregation is limited to only operating business risk, technology risk, market risk, and political risk. The definitions and explanations of these risks are provided in Section VI, and are not identical to those used by Farrell due to overlapping definitions.

Of these, start-up risk is not applicable to the instantiated artifact of this paper on the account of two factors:

1) Removing this risk allows for a narrowing of scope that significantly simplifies analysis. If a particular risk is identified that could conceivably fall start-up investment cost risk, it can easily

be folded into one of the other four primary classes of risk.

2) The focus of this paper is on attacking existing supply-chains. While it is true that supply-chains are inherently non-linear, and are in a constant state of operation, maintenance, and amendment, the iterative nature of end framework ensures that future iterations by other authors can be updated to account for this class of risk.

Start-up investment cost risk notwithstanding, adapting the other four primary risks identified by Farrell as a the lowest resolution of risk disaggregation also maps well to the system context shown in fig. 5 on the basis that since any special purpose vehicle necessitates to assignment of risks to the stakeholder which can bear them the best[175]. Therefore, any model which categorizes the risks to which a special purpose vehicle - the legal entity which assumed to operations of the project - must be comprehensive and sensitive to the risks that a complex systems and its stakeholders are party to.

F. Stage 5 - Mapping of Specific Risk

Stage 5 can be broken down into three chronological elements: an analysis of the EU's dependencies on different CRMs; an overview of each selected mineral group, the specific mineral manifestations which have been identified as especially volatility, and the different industries and critical infrastructure which is reliant upon the selected mineral candidate; the investigation of specific risk to which each mineral is party to, individually or otherwise, based on historical empirical data or extrapolation from the desegregated risks described in Sections IV-E.3, VI, and the supply-chain characteristics found in Section V-E.

V. Mineral Profile of Selected Candidate - Magnesium

By calculating the mean annual volatility for each mineral group, magnesium was found to have the most price volatile group of commodities, as can be seen in the below bar chart. On this basis, it is selected as the candidate mineral for further investigation. Subsequently, this section consists of an in depth analysis of the material, production, and supply-chain properties of Magnesium.

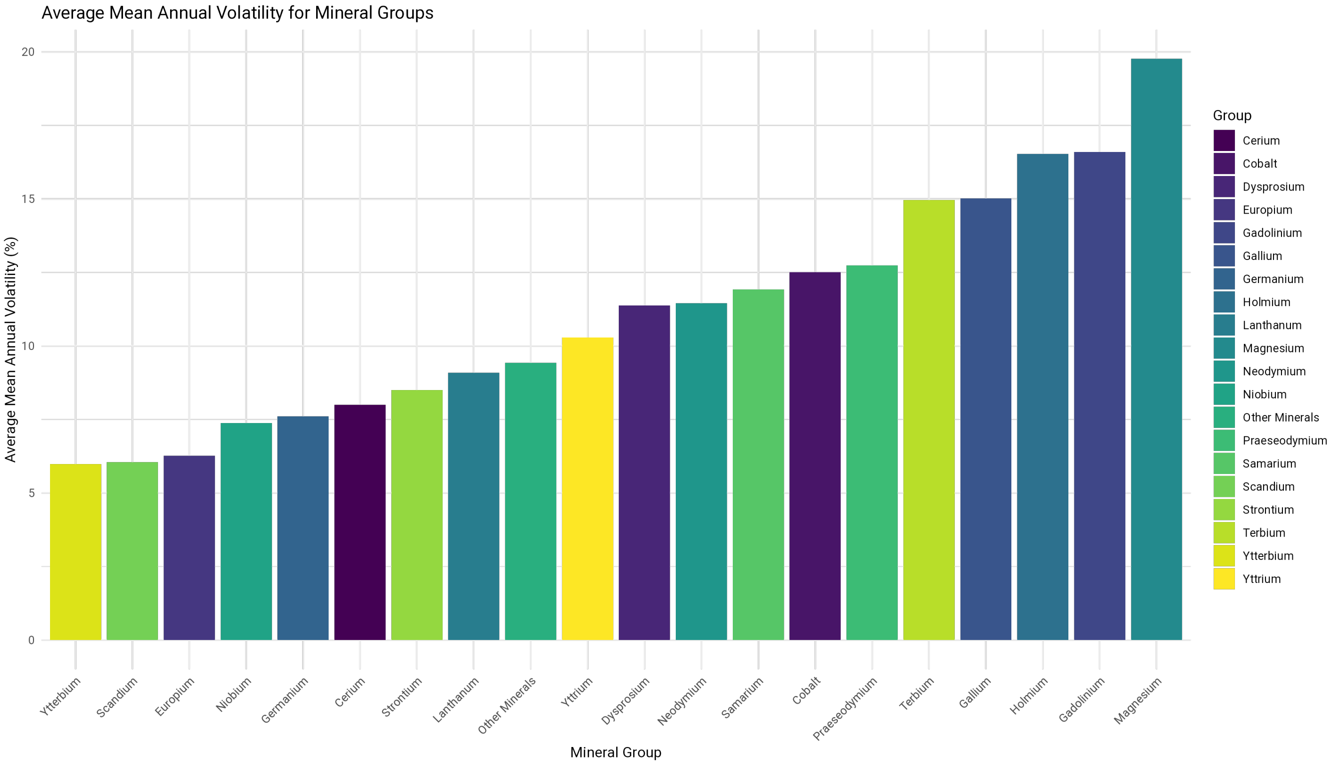

Fig. 6: Annual mean volatility of critical raw mineral groups

A. *Overview*

Magnesium (Mg) is an alkaline earth metal of key importance to the operation of both critical infrastructure and supply-chains. According to U.S. geological survey, it is the fifth most abundant mineral that can be found in the crust of the Earth and ranks third in sea water abundance[118, 176]. Notably, magnesium is a reactive element and does not occur in nature by its lonesome[177–179].

Broadly, according to the U.S. Geological Survey, there are two categories of magnesium commodities, magnesium metal and magnesium compounds, the latter of which includes magnesium chloride ($MgCl_2$), magnesium oxide (MgO), magnesium carbonate ($MgCO_3$), magnesium hydroxide ($MgOH_2$), magnesium oxide (dead-burned), magnesium sulfate ($MgSO_4$), magnesium sulfate kieserite ($MgSO_4 \cdot H_2O$), magnesium sulfate epsomite ($MgSO_4 \cdot 7H_2O$), magnesium chloride hexahydrate ($MgCl_2 \cdot 6H_2O$), and dolomite ($CaMg(CO_3)_2$)[180].

Magnesium metal, that is the pure form of Magnesium, can be either refined from Magnesium compounds, which posses their own unique applications, or from other mineral sources including magnesite ($MgCO_3$), brucite ($Mg(OH_2)$), serpentine ($Mg_3Si_2O_5(OH_4)$), olivine (Mg_2SiO_4), and talc ($Mg_3Si_4O_10(OH_2)$)[180].

As a mineral, the sourcing of Magnesium is by no means tightly limited to different geological hot spots. As the U.S. Geological Survey[181] states in their report 'Magnesium Metal - Mineral Commodities Survey,

> "Resources from which magnesium may be recovered range from large to virtually unlimited and are globally widespread."

Evaporite minerals bearing magnesium, dolomite, and serpentine - common sources of the mineral in its raw form - are present globally in copious quantities[181]. Additionally, as mentioned above, magnesium can be produced from salt brines with potential capacity in the billions of tonnes[181].

Broadly, there are three relevant production figures: primary production of magnesium metal that has been smelted, secondary production from recycling, and the production of magnesium compounds[181].

The vast majority of global magnesium exports originated from Chinese ports and production facilities, with 830 million tons produced in 2023 according to the U.S. Geological Survey - roughly 33.2 times as much as the next nearest producer, Kazakhstan[181].

The European Union is particularly dependent on Chinese magnesium as, per the *Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU - A foresight study*, China is stated to have a, " a quasi- monopolistic position," in the market[182].

County	2022	2023
United States	W	W
Brazil	22	22
China	933	830
Iran	5	5
Israel	22	22
Kazakhstan	27	25
Russia	21	20
Turkey	14	15
Ukraine	2	N/A
Total	1050	940

TABLE II: Total primary global production of Magnesium, not including the U.S (mt).[181]

B. Material Properties

The importance of Magnesium to modern manufacturing cannot be understated, due in part to its unique chemical and metallurgical properties[177]. When pure and unalloyed, Magnesium has one of the lowest densities of any metal used in structural applications[176, 177, 183] at $1.74 g/cm^3$[177][184].

Additionally, magnesium possesses other desirable characteristics, including greater ductility, castability, and specific strength that aluminum or steel[177, 185]; while boasting no toxicity, higher thermal and electrical conductivity, superior vibrational, dampening, and shock absorption capacity, when compared to competing materials[177, 186]. Magnesium also boasts the ability to be machined through any variety of commonly employed methods[177, 187, 188].

These advantages are, however, offset by numerous factors, including but not limited to magnesium's limited capacity to be cold worked, a low material toughness when unalloyed, the tendency of magnesium metal to shrink when cooled, its corrosion resistance, elastic modulus, a tendency to deform under stress via cold flow at increased temperatures, and the high reactivity of the element as discussed at the beginning of this section[188]. Magnesium's corrosion resistance properties are of particular concern, as there are two primary situations under which engineering design can be compromised: in the presence of metallic impurities when in an alloyed state, or in the presence of "aggressive electrolyte species."[177]

C. Applications of Magnesium Commodities

Broadly, this paper separates its identification of different magnesium applications into three sections: the application of pure magnesium to critical infrastructure, the application of magnesium alloys, and the application of magnesium compounds. This is segmentation is performed to easily demarcate the midstream elements of magnesium supply chains which are concerned with the shipping of pure magnesium, and those which are concerned with the derivatives of pure magnesium metal.

That is to say, while the upstream and midstream supply-chain elements of pure magnesium are (mostly) applicable the production of every substance discussed in sub-sections V-C.1, V-C.2, and V-C.3, it is necessary to disentangle these products so as to better grasp the complexity of magnesium as a group of commodities.

1) Pure Magnesium Metal and its Applications

The high reactivity of Magnesium means that the metal can be used in a variety of different chemical engineering applications - primarily as a reducing agent for other elements - to create both inorganic and organic compounds. For example, titanium production often relies upon the use of magnesium as a reducing agent to transform titanium tetrachloride ($TiCl_4$ to high-purity titanium metal via the Kroll process[189].

Organic chemistry is also a domain of application for magnesium, particularly as a component in Grignard reagents[190, 191]. These reagents are created when magnesium is reacted with with alkyl or aryl halides, lending themselves to a tool crucial to creating carbon-carbon bonds when synthesizing different organic compounds[191, 192]. Such compounds have wide scale applications ranging from polymers[193] and pharmaceuticals[194] to the manufacture of electronics and agricultural compounds[195].

2) Key Magnesium Alloys and their Applications

Magnesium is used in different alloyed forms across a wide variety of products, including electronics such as computers and servers[182, 196]; vehicles[176, 177]; energy storage applications[176]; biomedical technology[176, 177], with potential applications to orthopedics, cardiology, urology, and respirology[197]; aerospace and aeronautical technology[176, 177, 182, 196]; defense sector applications including drones[182]; and in many other fields[176, 177, 182].

Most production of magnesium alloys is done via liquid casting due to magnesium's performance compared to other cast metals[177]. Magnesium alloys are often processed in environs with low reactive risk, typically facilitated by inert gases, to prevent contamination with other elements during production[177, 196]. Various processes can be applied to increase the tensile strength and other desirable properties of magnesium alloys, including solid solution strengthening and second phase strengthening[177, 198].

Magnesium alloys can generally be processed as either cast, wrought or through additive manufacturing[199]. Cast magnesium alloys are, as their name implies, cast in liquid form and then solidified. Additives in the form of REE are often added for increased performance, and these cast alloys are often cold-worked subsequent to casting to improve material performance[177]. Wrought alloys are those materials that are shaped by some form of mechanical work, be it extrusion, forging, milling, or rolling to create the desired shape[199]. Wrought alloys are less frequently used compared to die-cast magnesium alloys[199, 200], are inherently less suited to higher volume production[201], and may not be suitable depending on the desired geometry of the end product[201]. Conversely, wrought magnesium alloys can exhibit superior material properties in the way of tensile strength and ductility at low-temperature thermal environments[199].

Magnesium alloys can also be used in their powered form with additive manufacturing techniques[202], where alloyed powders are fused in successive layers in a similar vein to 3D polymer printing to generate complex geometries at potentially high tolerances[203].

These magnesium alloys, whether wrought, cast, or powdered, come in a range of different groups dependent on their chemical composition. Pictured in the below figure is a plot of the yield strength of different alloy groups against their Erichsen Index, which measures ductility[204].

This paper identifies three main alloy classifications of interest: the Mg-Al-Zn, Mg-Al-Mn, and Mg-Re groups.

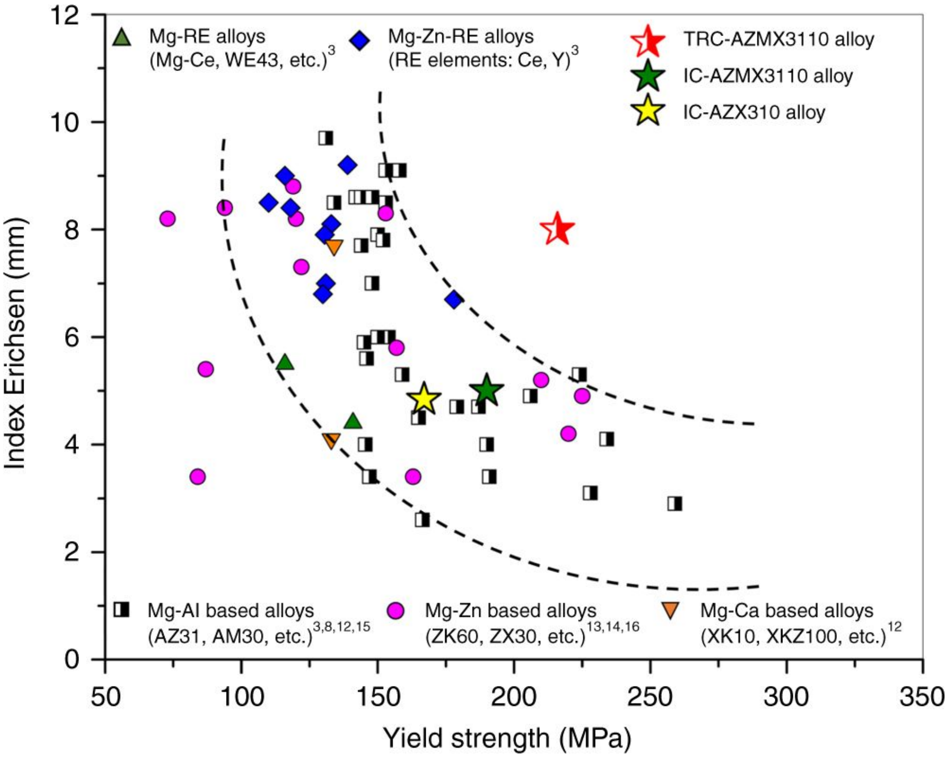

Fig. 7: Yield Strength v. Erichsen Index[204]

Both AZ91 and AZ31 are generally representative of the material behavior of similar magnesium alloys in the Mg-Al-Zn group[177, 205], the most commonly employed magnesium alloy family[177, 206]. Both zinc and aluminum constitute cost-effective alloying compounds for magnesium across different material phases due to their high solubility in liquid magnesium[177, 207].

Among the most common magnesium alloys, AZ91 exhibits high corrosion resistance, is easy to cast, and is generally a strong alloy.[177, 208]. AZ91 is so popular that it accounts for 90% of all cast magnesium products, partially due to its low density compared to competing alloys[177, 208]. By weight, AZ91 contains 9% aluminum and 0.7% zinc, which results in an alloy that can be employed in a large variety of manufacturing applications, from laptop chassis to steering wheels and a plethora of other products[177, 209].

AZ31 is another notable alloy for its good balance of strength, weight, and formability[177, 205]. AZ31 is commonly used in sheet and plate forms for applications in electronics and mobile devices, as well as in brackets for aeronautical purposes, benefiting from its excellent cold formability[177, 205].

Meanwhile, AM series alloys (Mg-Al-Mn) are employed in automotive applications at temperatures around 125 °C. Notable examples include AM50 and AM60B. These alloys exhibit lower strength but increased ductility compared to Mg-Al-Zn alloys[204].

Often referred to as the Mg-RE (magnesium-rare earth) group, other frequently employed magnesium alloys utilize a variety of LREEs and HREEs due to their heat-resistant material properties[177, 205, 210–212], albeit being limited by their financial cost and the limited supply of REEs[199]. Mg-Al alloys are frequently mixed with rare earth minerals, and their desirable grain structure and improved characteristics are well studied[199, 213].

A specific subset of Mg-RE alloys that does not face issues of financial cost while providing the strongest known wrought magnesium alloys are Mg-Zn-Zr (or ZK series) alloys, a subset of Mg-Zn alloys[199]. ZK60, an alloy of Magnesium, Zinc, Zirconium, and other elements, is an example of one such alloy and is known for fatigue resistance and tensile strength[177, 205, 210]. ZK alloys, in general, have applications as wrought alloys in automotive applications and the aerospace sector, where high-performance materials are essential while maintaining low mass[214].

3) Key Applications of Magnesium Compounds

To cover all the different uses of magnesium compounds would be beyond the scope of this paper, due to the specific focus on analyzing the vulnerabilities of magnesium metal production. Suffice to say, however, that magnesium compounds in general are used in the pharamceutical industry, as food additives, in rubber production, flue-gas desulfurization, wood pulp processing, and in chemical industrial processes[180].

To illustrate this ubiquity and wide scope of application, a useful example presents itself in the form of magnesium sulfate epsomite ($MgSO_4 \cdot 7H_2O$)[25]m which has used in diverse sectors as the production of concrete[215, 216]; in agriculture as a fertilizer for crops[217, 218]; dermatology[219]; and other medical applications, including the treatment of arrhythmia, eclampsia, asthma, and lead poisoning[220].

D. Critical End Products and Infrastructure

Based on the different applications of magnesium identified in the previous sub-sections, it is not an exaggeration to say the Magnesium supply-chain extends its tendrils into potentially every critical infrastructure sector. Without question, everything, from the electronics upon which nuclear power plants and electricity grids are reliant upon, to the potential applications in biomedical technology, to the aerospace and automotive sectors, key to the prosperity of many EU member states, can be construed as reliant upon the functioning and risk management of magnesium supply-chains.

Given the ubiquity of magnesium and magnesium product derivatives, it is necessary for the purposes of analysis to narrow the scope of investigation beyond general applications to specific classes of products. To align risk analysis of magnesium supply-chains with critical infrastructure, specific products that are aligned with the risk management practices and policies of the EU's critical infrastructure sectors, as well as the defense sector[26].

[25] Also referred to as Epsom salt.

[26] See Section IV-E.2

With good providence, this task is ameliorated by the European Commission's 2023 *'Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU – A foresight study'*, where the different CRMs identified by the report are correlated with fifteen different strategic technologies[182]. Magnesium, in particular is noted to be relevant to the production and operation of the following seven technologies[182]:

- Solar photovoltaics (PV)
- Data transmission networks
- Data storage and servers
- Smartphones, tablets and laptops
- Robotics
- Drones
- Space launchers and satellites

It must be noted that these technologies are identified as strategic, which pertains to technologies relevant to those materials that are tied to critical infrastructure, the European green transition, the defense sector, and the space sector as per the annex 1 of the ECMA[13]. Therefore, these identified technologies perfectly aligned with the amended critical infrastructure sectors selected in SectionIV-E.2

E. Supply-chain Characteristics

Consider the aggregate supply-chain for pure magnesium on a global scale. Each supply-chain can be generalized into a generic set of upstream, midstream, and downstream steps that exist in sequential order. The upstream portion is orientated around the mining of magnesium-bearing ores, the extraction of magnesium, removing impurities, and the subsequent processing into ingots or powders[182]. These processed forms of pure magnesium are shipped before their further employment in manufacturing or chemical industries[182]. These elements of the supply-chain constitute the midstream.

The extraction of magnesium for ores such as dolomite can be accomplished by either one of two methods: hydro-metallurgical extraction and thermal reduction[221], or hydro-metallurgical extraction and molten salt electrolysis[221]. Hydro-metallurgical extraction refers to the process in which metals are 'leached,' with organic and inorganic acids, or ammonium salt, from an ore into an aqueous solution[221]. This is a fairly cost-effective process with little economic impact[221].

Electrolysis, mentioned in the above paragraph, is a popular method of magnesium extraction following hydro-metallurgical extraction and is the exclusive method practiced in the United States[221]. This extraction method does not rely on ores and instead extracts magnesium from salt water brine[221]. According to Simaldi et al., electrolysis is "less labor and energy-intensive" but incurs greater capital expenditure[222].

By contrast, thermal reduction methods are much more financially expensive, energy-intensive, requiring higher temperatures, and impactful on the environment[221]. For example, the most common and notable thermal reduction method is the Pidgeon process[221], which is commonly employed in countries such as China[221, 222], is widely considered to be environmentally sub-optimal[221, 222], requires high energy input of around 366 $MJkg^{-1}$ of magnesium[223], and is limited in production volume arising from heat transfer inefficiencies[223]. Other thermal extractive processes include the, Bolzano[222], carbothermic, magnethermic, alumino-thermic, or Mintek processes[223].

Given the ubiquity of the Pidgeon process, a quick rundown of this method of magnesium production is provided below and summarized in Fig. 8.

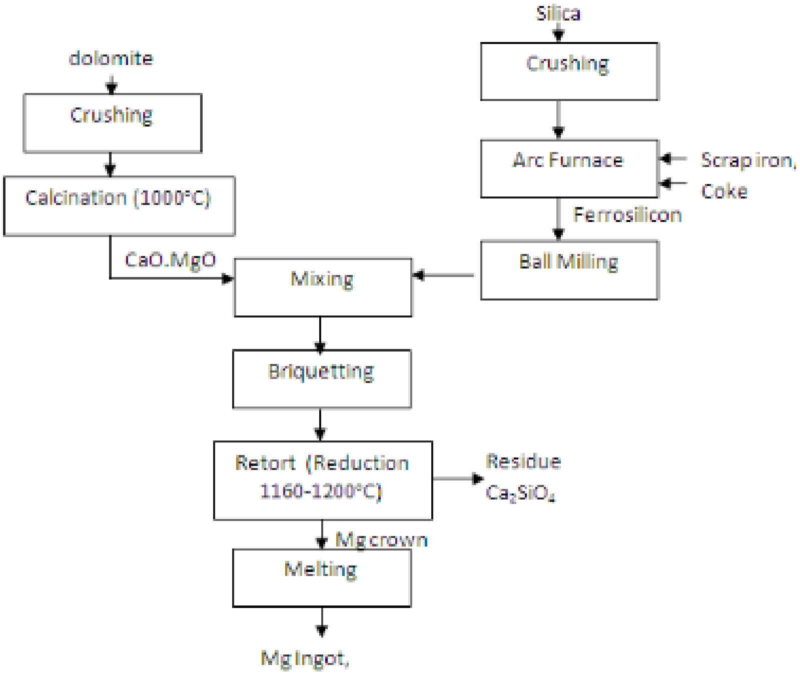

Fig. 8: Schematic Flowsheet of the Pidgeon Process[223, 224]

In the Pidgeon process, Dolomite is crushed and then processed in a rotary kiln at around $1000\circ C$ where the feed is calcined[223]. Ferrosilicon is produced by carbothermically reacting quartzite with silica in an arc furnace at 1600 $\circ C$, before both the calcined dolomite and ferrosilicon are briquetted and mixed[223]. The mixture of the two inputs is then processed in a $Ni — Cr$ stainless steel retort where the dolomite is reduced at high pressures of around 13 to 67 Pa[27] and temperatures of $1160\circ C$, producing magnesium vapor[223]. This vapor is then condensed via water cooling, producing low impurity magnesium that is subsequently melted down into ingots[223].

Following extraction, impurities are removed, and then the purified magnesium is cast into its final form before shipping to downstream actors for further utilization[182]. Casting is commonly done with

[27] Pascals

steel crucibles and transported in steel vessels[225].

Once shipped to the actor that uses raw magnesium in the manufacture of an alloy or some chemical process, the product can be recast through a variety of methods, including high-pressure die casting, hot chamber die casting, cold chamber die casting, vacuum die casting, super vacuum die casting, permanent mold casting, thixomolding, indirect squeeze casting, lost foam casting, or ablation casting, depending on the application[225]. Alternatively, magnesium alloys can be wrought through several methods, such as milling or forging, or printed with additive manufacturing methods.

As it pertains to magnesium, the midstream elements of the supply-chain are not particularly unique to magnesium, save for the fact that shipping magnesium requires diligent handling[226] given that the element poses significant thermal hazards[226].

F. Price History and Volatility Analysis

The following sub-section is derived of the results from the implementation of the quantitative portion of the methodology described in Section IV-E.1. This analysis is separated into three sections, the list of identified and selected mineral manifestations, an investigation on the relationship between the method of shipping and how that reflects on the aggregate risk captured in price volatility, and the breakdown of historical prices and their volatility over the COVID-19 pandemic.

1) Selected Mineral Manifestations

The following is a list of the selected forms of magnesium metal that were selected for analysis, based on the availability of datasets from the Institute for Rare Earths and Strategic Metals[172]:

- AM50A magnesium alloy
- AM60B magnesium alloy
- AZ911 Magnesium alloy
- 99.9% pure magnesium ingot
- 99.9% pure magnesium powder

The aggregate volatility for each selected mineral manifestation was calculated not just for each type, but for the specific port from which it was shipped, and the method of transport.

It should be noted that the limited selection of investigated commodities stemming from the limited dataset is a weakness of this analysis. Further iterations of this model should account for limited data.

2) Method of Delivery and Impact on Implications of Price Volatility

The available data the price of a commodity from one of four locations: India, Russia, China, or Rotterdam. As part of the dataset, the specific port of origin, as the port's name was only provided. Additionally, not all selected commodities were transported in the same manner. Some were shipped

Free-on-board (FOB) or Ex-works (EXW). Others were presumably transported over land routes, or were otherwise not identified as being transported by a particular method.

FOB is a term set forth by the International Chamber of Commerce, and can be split into two types: FOB Destination and FOB Shipping Point[227]. FOB Shipping Point describes a shipping practice whereby the seller assumes risk in the form of liabilities and costs for the following activities: the delivery of the good to a port, handling of the good at the port, but not loading of the good onto the ship; and customs at the point of shipping[227]. The ownership of the good is transferred to the buyer subsequently[227]. Thereafter, the buyer assumes costs and liabilities for the loading of the goods onto the ship, handling at the port of delivery, customs at the end location, and transportation to the buyer's inventory[227].

In FOB Destination, the seller additionally assumes liability and the financial cost for all activities until delivery at the specified destination of the buyer's inventory[227].

Ex-works, meanwhile, refers the commercial and legal practice that places the greater liability and cost on the buyer. The seller must only provide the goods to be shipped, relevant documentation, and inform the buyer of the goods being ready to ship[228]. Thereafter, the buyer assumes custodianship and all subsequent risk[228]. The price of a good ex-works, therefore, reflects the price of the good when it leaves the point of production or extraction[229].

The datasets taken from the Institute for Rare Earth and Strategic Metals do not distinguish between FOB Destination and FOB Shipping point. If all FOB prices are to assumed to be FOB Destination, then annualized price volatility better captures the aggregate risk represented by the entirety of midstream supply-chain operations. If all FOB prices are FOB Shipping point, then this price volatility still captures in some part the risks relevant to the midstream elements of the supply-chain, albeit to a lesser extent as price still reflects the willingness of the buyer to assume the risks of shipping themselves. The same is true for Ex-Works.

3) Breakdown of Findings

As can be seen in Fig. 9, the price increases of the magnesium commodities that were selected all tightly cluster together and, on first inspection, appear to visually mirror each other. It can therefore be speculated that the key drivers of aggregate risk did not significantly differ between commodities.

The only notable exception to this trend was the price of 99.9% magnesium ingots originating from Russian warehouses, where the prices of these commodities tend to appear less tightly correlated with overall price trends in magnesium. This clearly correlated with the Russian military invasion of Ukraine on the 22nd of February, 2022, where this visual divergence from magnesium as an overall group of commodities can be visually observed.

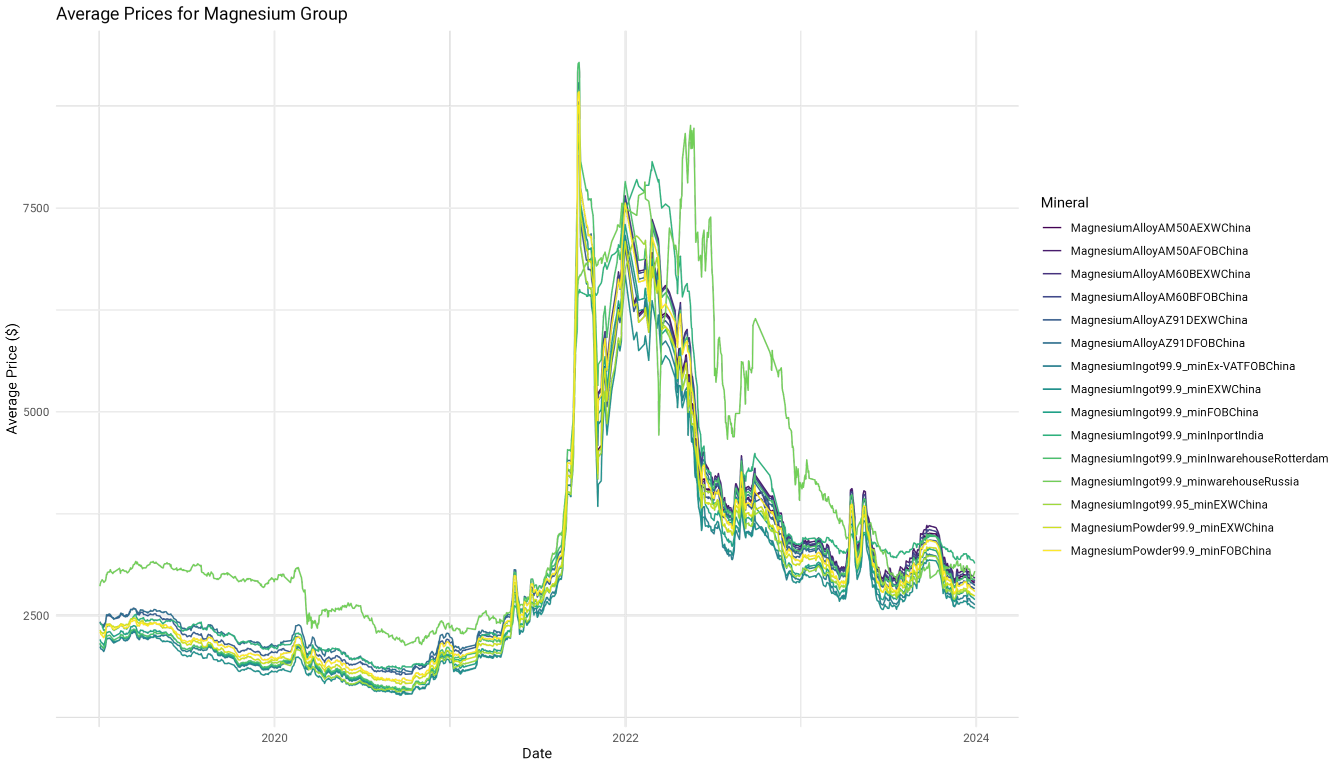

Fig. 9: Price history of investigated commodities

In general, there was a precipitous increase in the prices of all investigated Magnesium commodities from between 2021 and 2022, which is commensurate with increased stresses on global supply-chain operations, particularly arising from shortages in raw materials and the lag-time during which supply-chain resilience was tested while reorientation was occurring. The mining sector in general was negatively effected, arising from trade restrictions and, in some instances, the closure of mines from 2020 onwards[154].

Upstream activities such as smelting and mining were particularly impacted in 2020, originating primarily from logistical challenges instead of resultant knock-on effects from government COVID-19 policies[154]. Strangely, however, this did not result in nearly as marked an increase in prices for magnesium commodities from 2020 to 2021, only peaking twice at the beginning and end of the year, as the price increased from 2021 to 2022. Prices for magnesium did increase from 2020 to 2021, as did all metals except for gold and palladium[154].

When annualized price volatility is observed, however, there is a definite spike for the 2020-2021 period in all magnesium commodities, except for magnesium ingots from Russia, which peaked at in 2022. Aggregate risk can therefore be concluded to have materially increased for almost all magnesium commodities, and Russian magnesium ingots are isolated as an outlier for further study in risk analysis.

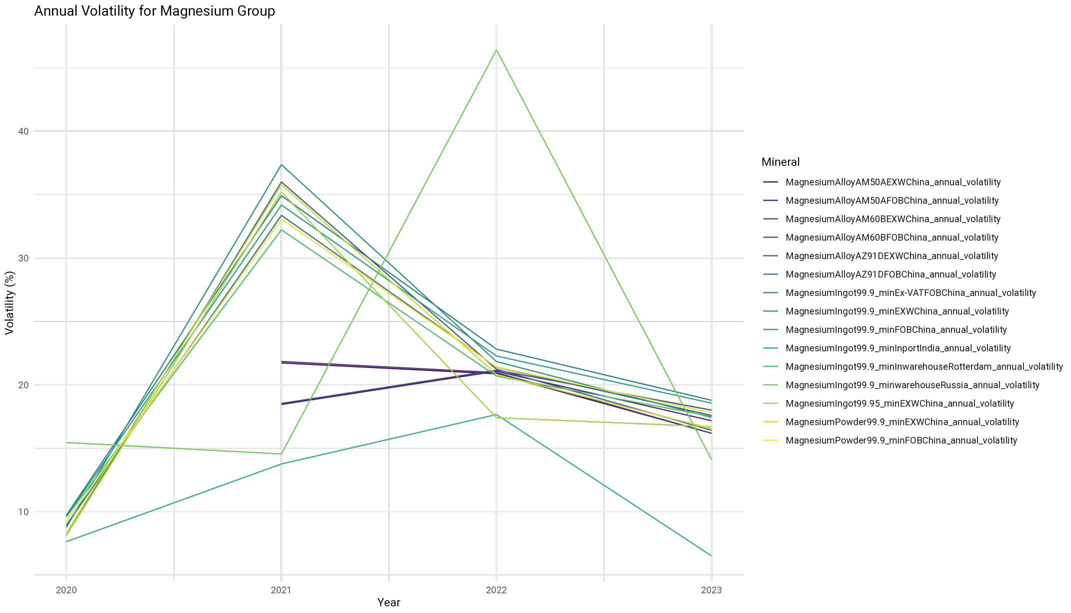

Fig. 10: Annualized Price Volatility

A more granular examination of daily price volatility shows that the largest spikes in volatility occurred in Q2, Q3, and Q4 of 2021, before the onset of the Ukrainian war.

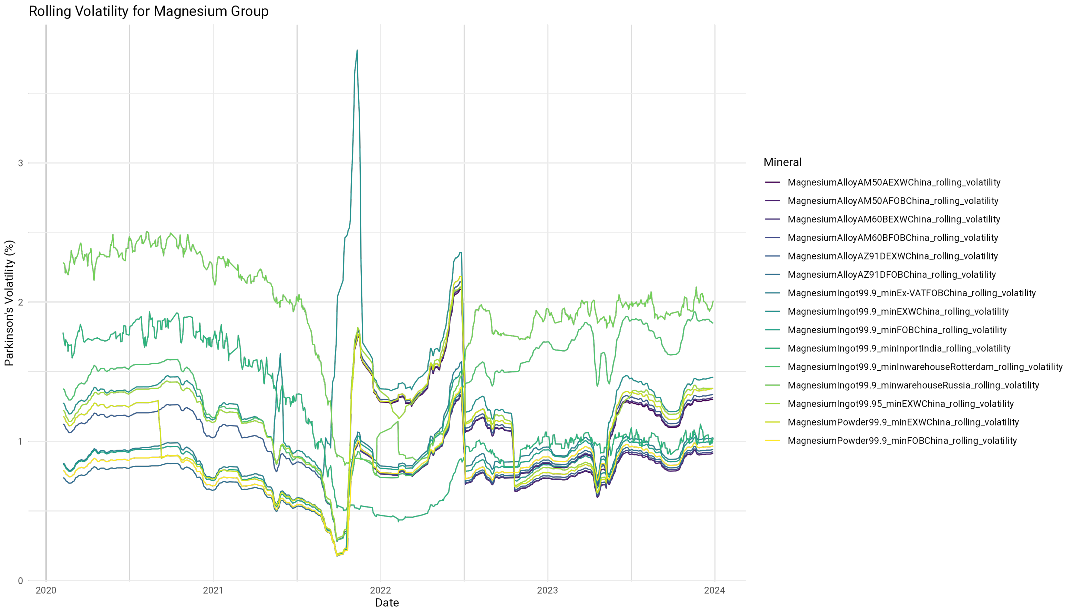

Fig. 11: Rolling Volatility

These price volatility increases can be partially explained by a supply crisis originating from the decreased production of Chinese magnesium ingots, partly from decreased power generation due to power rationing[230, 231]. From Q2 until the end of Q4 2021, Chinese coal supply was rationed arising from a confluence of factors, including supply-side shortages such as the cessation of coal mining activity, the impact of the COVID-19 pandemic on coal imports (particularly from Indonesia), flooding leading to reduced supply of coal by rail, decreased water supply stemming from meager precipitation, operational caps of 65-75% during China's 14th National Games to reduce smog for political reasons, and the cessation and decreased production of some mining operations as result of increased safety standards from as far back as 2020 due to a slew of miner deaths[230].

Price volatility and hikes for Chinese magnesium ingots and magnesium derivatives can also be attributed to demand-side issues. Provinces with heavy manufacturing output, notably Jiangsu, Zhejiang, Fujian and Guangdong, contributed to a 4.5% year-on-year increase in electricity consumption through Q1 to Q3, 2021[230], attributable to increased demand for[230],

> ”...machinery, consumables, electronics, chemical intermediates and construction materials.
machinery, consumables, electronics, chemical intermediates and construction materials.”

The effect of this supply reduction was deleterious on European production of manufactured goods and critical infrastructure[230]. Production shortages were pronounced notably because American and EU downstream actors re-shifted demand towards Chinese manufacturers from South East Asian alternatives[230]. Given the dependence of the EU on Chinese magnesium, it is highly likely that these particular supply chains were likewise impacted on the same basis. Certainly, given their ubiquity, the supply-chains for products that rely upon Chinese magnesium, even if processed in China, were disrupted.

Additionally, on the supply side, price volatility and price increases can be attributed to shipping bottlenecks in freight arising from insufficient capacity to procure containers, load said containers onto ships, and then ship goods to their port of call[230].

Therefore, risks related to the supply of electricity to industrial activities and midstream are heavily investigated when applying the analysis of disaggregated risks to magnesium-related supply-chains.

VI. MODEL OF DISAGGREGATED RISKS

The disentangling of one risk from another is difficult due to the non-linear interplay of supply-chain elements and actors. This is easily illustrated when referring the example of the impact of coal power shortages on the price of magnesium through Q2 to Q4 2021. Which risk precedes all others as the basis for overall classification when considering the cascade of effects that lead to lowered production capacity? Was it the internal political dimension of the administrative apparatus of the Chinese state which imposed price caps on the price of primary energy in the form of coal; was it the manifestation of environmental risk in the form of simultaneous drought and flooding; or was it the long-standing serious of embedded risks which led to insufficient freight capacity to meet downstream demand? As these cannot be disentangled from each other, the approach that has been taken in the disaggregation of risks is to classify portions of aggregate risk by the broadest possible definitions, to identify specific sub-categories of these risks and their manifestations in magnesium supply-chains, and then to draw links across these broad categories of risks to create a fuller picture of disaggregated risk.

The four generic disaggregated risks that have been selected are operating risk, technological risk, market risk, and political risk. Operating risk and technological risk are perhaps the most difficult to disentangle from each other, as it is difficult to separate the operation of supply-chains from the technology that underpins them.

A. Political risk

This paper defines political risk as a class of risk that encompasses those factors most closely associated with conventional security studies and strategic studies subject matters, including warfare. That is, political risk refers to the class of risk that are modulated through international institutions, state actors, and local governance. Note that, like all other four broad classes of risk, political risk intersects with the others, especially when it pertains to military action.

Political risk as a class is filtered through offensive realism. The actions of the actors which impact political risk are therefore conceptualized as reflective of the realist objectives of state actors as the primary reference point. This does not necessarily imply that all actors which affect political risk factors are necessarily rational at every single level of analysis, nor that their rationality is necessarily perfect. Rather, the aggregate behavior of state objectives is construed as rational.

The specific sub-classes of risk subsumed by the political risk label include the following six factors:

1) War, piracy, and other military action

Warfare is perhaps the most interesting factor in the way that military actions can have a pronounced effect on market risk, operating risk, and technological risk. Consider the deliberate employment of resources by the Russian army from it's initial invasion of Ukraine in 2022, where military assets were used to deliberately attack energy infrastructure resulting in 30% of the Ukrainian population lacking access to heat and electricity[232]. The total power generation capacity of Ukrainian energy infrastructure had been reduced by 63% to only 13.9GWh by the end of December, 2022[232]. By March, 2023, roughly 45% of the high-voltage substations in the country were under Russian military control. The impact of this on Ukrainian supply-chains cannot be understated, with only eight of twenty four industrial sectors reporting increases in production during 2022[232].

Wartime or military activities, especially aerial and naval warfare, can also have profound impacts on all elements of the supply-chain, particularly midstream activities. From piracy off in the Straights of Malacca[233–236] to the blockage of the Suez Canal in 2021[233], and the hostile actions of

Houthi rebels in the Bab El-Mandab straight from 2023 onwards[237–240], critical shipping lanes for commodities and products upon which critical infrastructure is reliant are all subject to disruption[233, 241, 242].

The question remains how to disentangle the impact of wartime activities from the technological and operational risks which can be exploited using wartime tactics. The answer that this framework arrives at is to designate wartime activity as a special or unique set of risks, derivative from political risk, and arbitrarily separate from operational and technological risks to which supply-chains are party to during *normal* or regular operation.

2) Expropriation

The expropriation of assets by national or state entities is a risk borne by both domestic and international actors, including states, if a particular portion of the supply-chain is partially funded through foreign capital. Additionally, because of the realist framework adopted by this paper, companies operating in foreign countries are partially representative of foreign national interests. Therefore, expropriation of assets is not only a risk assumed by private actors. The act of asset appropriation is subsequently a political one.

Expropriation of assets is distinct from nationalization in that it covers a wider set of activities that a state undertakes to acquire assets from supply-chain elements. Taxation, for example, is a form of expropriation, as is a state off-taker refusing to pay or service their contractual obligations, the imposition of price caps and price floors due to the creation of a welfare loss in microeconomic terms, and even licensing issues can be perceived as a form of expropriation.

The risks encapsulated by this sub-category are inherently political, stemming from not only the internal machinations of state actors but also because expropriation can be spurred by political actions of foreign actors, including activities such as sanctions[243].

It bears mentioning that expropriation of assets can have severe knock-on effects on legal and structural risks, sovereignty risk if (a) foreign state(s) are involved, and a slew of market and operational risks.

3) Nationalization

This risk is defined as, ”the taking of control by the government over assets and over a corporation, usually by acquiring the majority or the whole stake in the corporation.”[244]

This subset of risk comes in two forms as defined by the OECD, which records nationalization in two different instances, expropriation/confiscation or through financial recompense[244]. The first of these defines the activity in the following manner[244]:

> ”Nationalisation of private corporation by mean of confiscation is to be recorded as an uncompensated seizure, to be recorded in the other change in the volume of assets account.”

When a state nationalizes the assets of a firm, it need not be uncompensated. It can also be recorded as:[244]

> ”Nationalisation of a private corporation by mean of purchase of shares (at market price, by mutual agreement) is a financial transaction, to be recorded in the financial account.”

The distinction in this framework between expropriation and nationalization is that in the former, the state needs not to seize the entirety of a supply-chain actor. Different assets under the management of private and foreign state actors may be confiscated, but there is no requirement for the entirety of those assets to be seized. In nationalization, the entirety of that element of a supply-chain which is being acquired by a host state is taken under control.

4) Political stability risks

The link between political instability and supply-chain disruptions is undeniable[245–248]. Revolutions, domestic upsets, changing governments, civil-unrest, the influence of foreign actors on the behaviour of states within which key elements of supply-chains operate, these are the factors that dominate political stability risks and are a focus of investigation in Section VII.

5) Legal and Structural Risks

Legal and structural risks pertain to the regulatory frameworks which govern the fulfillment of contractual obligations between related actors in a supply-chain. This risk does not, however, pertain to the specific contractual agreements between actors, merely the frameworks which govern their enforcement. This class of risk also covers regulatory risk, including environmental regulation and licensing, which are subject to both either national and/or international law.

This includes the concept hereto for coined as sovereignty risk. The primacy of which country’s sovereignty defines the behavior of supply-chains over different geographic areas, as well as the interplay between inter-state logistical networks, is a crucial concern for supply-chain operation.

B. Market Risk

As defined by the European Banking Authority[249], market risk is defined as ”the risk of losses in on and off-balance sheet positions arising from adverse movements in market prices.” Under regulation (EU) 2019/876 of the EU Parliament and Council[250], market risk is additionally defined as ”...the risk of losses arising from movements in market prices, including in foreign exchange rates or commodity prices.” These definitions harmonize with the definition of market risk in the context of project financing special purpose vehicles, where Farrell defines market risk as the threats to the competitiveness of the firm in the market[1]. This definition is retooled for supply-chains to apply to all actors which service the supply-chain. Market risk is, therefore, defined as those classes of risk that threaten the competitiveness of the market as a whole. The lower the prices of magnesium prices on the market while maintaining a sufficient volume of product, the lower the market risk to which the supply-chain is a party.

The following are the primary sub-categories of risk that are encapsulated by market risk as a class.

1) Financial risk

These risks broadly pertain to the financial health of individual actors that act within the context of supply-chains. In other words, it refers to all those risk encapsulated by on-balance sheet positions held by various entities which are stakeholders within a supply-chain. Borrowing from a framework provided by Dentons[43], financial risks also include the contractual relations and the risks pertaining to contractual obligations of not just the producers, operators, and offtakers of the supply-chain, but also the financial institutions and other stakeholders which are marked by some form of fiduciary relationship as mediated through shareholder agreements, credit agreements, and other documents.

2) Counterparty risk

In the course of commercial activity between different actors, it may arise that a counterparty to a supply-chain operation will default on its contractual obligations[43]. More percisely, counterparty risk is defined as[249],

> ”...the risk that the counterparty to a transaction could default before the final settlement of the transaction cash flows.”

This class of risk is not narrowly limited only to counterparty credit risk, which is in the only context in which the concept is regulated in (EU) 2019/876[250]. Counterparty risk also includes the failure of suppliers, customers, insurers, and other parties to meet their contractual obligations[43] to legal private entities that operate within a supply-chain.

3) Supply and demand risk

As illustrated by the example of soaring magnesium commodity prices through Q2 to Q4, 2021, supply and demand risks constitute the classes of risk related to the failure of the market, even in only in the short term, to meet the needs of any actor downstream from the next.

Supply risk, as defined by the annexes to the CRMA, relates to the risks which would hinder the provision of transport or production to downstream actors based on aggregate production, import reliance, the availability of substitutes, and a variety of other factors including political stability via the proxy of the World Governance Index of a nation within the supply-chain[13]. This definition of supply risk poses an issue, in part because it subsumes other broad classes of risk as inputs into its calculation.

The definition of supply risk set forth by the CRMA is then a quantitative measure of supply risk, aggregating several factors. It is a form of risk aggregation that seeks to encapsulate all elements within the market to quantify the ability of the market to supply EU consumers with inputs. As some of these inputs have already been disaggregated into other broad classes of risk that seek to qualitatively describe risks contributing to the ability or inability of the market to supply selected commodities or products, this framework instead redefines supply risk to be those factors related to the depth of the market relative to the size of transactions, and the ability of midstream actors to provide cargo to relevant buyers, as well as receive and ship cargo from buyers.

This risk encapsulates a number of the nonlinear supply-chain chain phenomena identified by Blanco et al.[10][28], including self-interest in the case of supply dumping of commodities on the market, uncertainty of the supply of a commodity across a supply-chain arising from volatile supply contexts, congestion, and waste arising from the time-lag during which a supply-chain struggles to re-orientate resources.

It is also vital to consider that since supply risks are not narrowly limited to only the mineral commodities shipped by supply-chains, but also input goods and commodities, all of the strategic logics that are described in Section III-G.1 ought to be considered when evaluating how an opponent may seek to maximize supply-risks on a market level.

Demand risk, on the other hand, originated from downstream actors and is the risk that either demand is insufficient to justify or allow for the continuation of upstream operations, or that the aggregate demand for a commodity in different regional and global markets outstrips supply[251] arising from demand volatility or sub-optimal/inaccurate demand forecasting[251, 252].

4) Commodity price risk

Unforeseen fluctuations in the prices of different commodities can directly impact the ability of private entities within a supply-chain to be unable to meet their long-term and short-term debt obligations, as well as maintaining profitability, revenue, and firm value[253]. In the particular instance of supply-chain orientated around the production of a specific commodity, this risk extends beyond simply the price fluctuations of the commodity itself and extends to all commodities which act as inputs to upstream, midstream, and downstream activities.

5) Currency transaction risk

When trading commodities, goods, and services across international borders, the issue of currency transaction risk is a firm consideration for all actors within a supply-chain. The same phenomena of supply and demand risk and shocks which apply to the commodity why is provided for by a supply-chain apply to currency. This class of risk is only isolated as separate from supply and demand risks as that class of risk pertains to the mineral commodity being investigated.

Again, the depth of the market can pose an in issue for the supply-chain as a whole. If the liquidity

[28] See Section III-A

in a market is thin, that is insufficiently, a transaction which large relative to ordinary transactions in the market results in a scenario where an exchange will not be executed anywhere near the published nominal exchange rate[254, 255].

This class of risk is also especially pertinent for those actors who are affected by politically-motivated economic activities such as as sanctions. For example, Russian banks which are sanctioned and unable to use SWIFT for the execution of transactions in U.S. dollars[256, 257] must seek to engage in off-market transactions[255, 256] which similarly constrain the ability of Russian upstream and midstream actors to execute transactions[256], relegating them to currency exchange at below market rates[256].

C. Operating risk

Suppose market risks apply to the market in aggregate or portions of the global supply-chain. In that case, operating risks pertain to individual actors and their ability to maintain production sufficiently to meet upstream demand. All of the risks itemized in the market risk class affect individual actors within a supply-chain, and these operating risks are a class of risk that allows for re-contextualization for more granular analysis. Therefore, to reduce redundancy, this sub-section on operating risks is orientated only around the ability of an actor in a supply-chain to meet their contractual obligations from a technical perspective. This is distinct from the *technology* risks discussed in the next sub-section, which are technological risks pertaining to vulnerabilities in specific technologies.

1) Energy risk

The events which may arise which arise in the production, transmission, energy storage, distribution, transportation, and use of primary energy sources, that directly affect and individual actors ability to meet their contractual obligations or otherwise impede the operation of their activities. Of all the operational risks, energy related risks are perhaps the most intersection with market risks and political risks, due to the inherently politically-sensitive and strategic nature of primary energy.

2) Insufficient production capacity

Influenced by all other risks, and vice-versa, insufficient production capacity is simply the inability for upstream actors to provide sufficient volume of output to meet obligations. This sub-class of operating risks is distinct from low production volume despite sufficient capacity, which may arise from political, strategic, market conditions, or supply disruptions arising from adverse conditions.

3) Shipping and transport risk

For individual upstream, midstream, and downstream actors in a supply-chain, the ability to receive and send critical inputs is a key concern. All those events which effect the ability of logistical transport of commodities, goods, and services to an individual actor are subsumed by this class of risk.

D. *Technology risk*

The final class of risk is unique in that, while again intersecting with operational risk and political risk, the focus of this lotus of risk is on the vulnerabilities of technical components in a supply-chain may fail to provide sufficient absorptive, adaptive, and restorative capacity on a purely technical level. Technology risk is then representative of a perspective shift in analysis away from political, strategic, and market concerns, and instead the narrow focus on embedded technical subsystems. This perspective shift is applied categorically to each different element of an analyzed supply-chain regarding the elements of critical infrastructure which constitute its operation.

Technology risk is not distinct from operational risk, rather it is a perspective shift away from the effects and events which may impact operations to different risks which impact *how* operations proceed under adverse or sub-optimal conditions.

VII. Analysis - Application of Framework to Selected Supply-chain Elements and Identification of Attack Vectors

Pursuant to the framework established in the previous Section on disaggregated risks, the analysis portion of this paper applies the primary classes of risk established previously to magnesium and magnesium-adjacent supply-chains as filtered through the perspective of a malicious opponent seeking to induce risk in European Union actors. To frame such risks from such a perspective, the potential actions which are proposed are drawn from empirical and historical evidence of previous such actions or are extrapolated from such previous patterns of behaviour.

Analysis is broken into three sections, in accordance with the system scope described in SectionIV-C and Fig5, which are correspond to different potential attack vectors on the upstream, midstream, and downstream portions of magnesium supply-chains.

A. *Upstream Attacks*

Without the production of magnesium, there is insufficient supply for the market. If alternative sources cannot provide magnesium to downstream offtakers at the same or lower price, the quality of the commodity is inferior, or if an alternative supplier cannot have their output produced and shipped in a period of time greater than downstream offtakers can tolerate, then the overall effect on a targeted opponent is negative. This truism mandates then that whatever upstream attacks disrupt production must fundamentally ensure that whatever the chosen targets and methods, either the producer of the commodity experiences sufficient decreases in cash flow from operations over a long enough period of time to decrease their fitness in the market, or that whichever producers will assume responsibility to close the supply gap will either provide magnesium at higher prices.

Given the reliance of EU member states on Chinese-produced magnesium and associated derivative products[182], it is unlikely that an offensive actor that attacks magnesium production will fundamentally change that relationship to the detriment of EU critical infrastructure reliant upon that same commodity.

If the opponent chooses to attack Chinese production of magnesium to increase the commodity's price, that effect will most likely be transient on the balance of probabilities. The transient nature of such an effect does not mean that there will not be a negative effect on EU member states; rather, referring again to TABLE II, the likelihood that any alternative producer will displace the loss in Chinese production is low. Not the least of which because the Pidgin process employed by Chinese and other producers is significantly cheaper than alternative processes, electrolytic processes, or other thermal reduction processes like carbothermic, magnethermic, alumino- thermic, or Mintek processes[222, 223].

Instead, if one were to target magnesium production, it would be far more prudent to target producers in regions with little production relative to the overall market, operating in nations with few competitors and that employ more expensive methods. Here, American primary magnesium production posed a perfect target: there *was* only one producer in the country, US Magnesium LLC, which employed an electrolytic process to extract magnesium from salt brine[222, 223, 258]. US Magnesium LLC has since ceased production[258].

B. Midstream Attacks

As evidenced by the COVID-19 pandemic, global supply-chains were increasingly constricted by a lack of supply-chain resilience regarding transport infrastructure[9]. On this basis alone, reducing the ability of midstream actors to either be unable to meet their contractual obligations, leveraging counterparty risk, or be reticent to engage in new contractual agreements regarding magnesium supply-chains-related activities is, without question, a broad class of attack vectors that an opponent would and ought to seek to exploit to induce risk.

Ultimately, the goal of objective in potential midstream attacks is to either deny or constrain the ability of European downstream consumers of magnesium commodities to receive the goods that they have already purchased, to ensure that there is an insufficient supply of commodities on the market so as to induce higher prices (thereby denying or constraining the ability for European offtakers to acquire new assets), or to increase demand risk such that the midstream elements of the supply-chains are unable to meet fluctuations in demand due to poor forecasting.

The question remains as to how this could be accomplished. Via first-parties or proxies? Are there legal methods with which these objectives could be fulfilled, are there clandestine methods which could do the same, or is the direct application of kinetic energy a viable (perhaps) necessary option to accomplish this task? Given the theoretical and ambiguous nature of the constructed opponent outlined in Section IV-C.1, the answer in a practical sense to the viability of these queried positions is entirely dependent on the assets and tools available to the opponent.

C. Downstream Attacks

The purpose of downstream attacks is to target the distribution and sale of finished goods, which, as per section V-D, are goods related to the following classes of products: solar photovoltaics (PV), data transmission networks, data storage and servers, smartphones, tablets and laptops, robotics, drones, space launchers, and satellites. Downstream attacks can therefore be folded into two categories: those attacks which are materially the same as midstream attacks, and attacks which specifically target the sale of finished goods.

D. Vector I: Denial of Physical Assets

To deny physical assets is to render access to their use or ownership temporarily or permanently infeasible. Thus, this vector of attack is orientated around ensuring that between any set of stakeholders within a subsystem, at least one stakeholder is unable to meet their system obligations such that the effects of a specific risk are magnified outside of the overall supply-chains ability to absorb, adapt, or restore standard functionality to pre-attack levels of operation without significant cost in either the short, medium, or long term.

This vector is broadly applicable to all elements of the supply-chain, but particular emphasis is put on its applications to midstream elements of a supply-chain. Hereafter, this subsection separates potential ways in which this vector can be exploited into three levels of analysis corresponding to the three subsystems within a supply-chain.

1) Upstream

Disrupting the flow of production of magnesium depends on attacking either the mining of magnesium-bearing mineral rocks or the production and refinement of magnesium by producers. To physically deny access to assets is not only limited to the destruction of those assets but includes halting their normal function at required levels. Thus, to analyze potential manifestations for this vector of attack as applied to upstream operations in the magnesium supply-chain, the method of production, access of the production facility to primary energy, quantities of raw and semi-finished minerals which the producer can acquire, forecasting of downstream demand, and the relative cost of inputs are all considerations.

This analysis identifies three different classes of targets in the upstream production of magnesium: mining infrastructure, production infrastructure, and energy infrastructure. The first of these are all of those elements necessary to maintain mining operations at desirable levels. Production infrastructure, meanwhile, refers to those elements of either the electrolytic or thermal reduction processes employed by a magnesium producer that, when disrupted, would lead to a halt or slowing of production, however temporary. Finally, energy infrastructure is the upstream, midstream, and downstream elements of the supply-chains that ensure constant access to variable loads during peak production hours.

Referring back to Section V-E, the Pidgeon process is one of the most commonly employed methods of magnesium production and is widely utilized by Chinese firms[221, 223]. This process, which has only a 12% efficiency during the reduction stage using coal[223], provides insights into how an opponent may exploit production infrastructure to reduce productive output. One notable element of the Pidgeon process is that it requires two input streams, one for dolomite and one for silica, which is then processed into ferrosilicon[223]. Limiting access to the amount of heat that a production facility can produce consistently by restricting access to coal or electricity can result in even lower efficiency of magnesium output. The same principle applies to the electric arc furnace, which is utilized to react quartzite with silica to produce silicon. The reader should also note that scrap iron and coke are used during this step[223, 224]; reducing access to these secondary inputs will, therefore, also lead to lower production.

Affecting this reduction in access to production inputs could be accomplished through a variety of methods: industrial sabotage of relevant elements through destruction of assets, fomenting workplace dissatisfaction, creating protests and strikes in either mining operations or the actual production of magnesium, sanctioning access to primary energy or using political pressure to demand that greener sources of energy are used instead of primary energy sources like coal, or otherwise applying the use of kinetic force during wartime activities to reduce production.

2) Midstream and Downstream

To remove the ability of individual midstream and downstream actors to move commodities in their legal care physically is to halt the supply-chain for a single set of actors until the supply-chain reoriented itself to be able to move inventory. To remove the ability of all midstream actors to move commodities in their legal care is to halt the supply-chain entirely.

Empirical evidence shows that states frequently implement these attack vector objectives to seize economic advantage or strategic superiority over their foes. Perhaps the two most pertinent examples of the utilization of this attack vector were the 1956 Suez crisis, the Iran-Iraq war, the blockade of the Black Sea from 2014 onwards, and the Iranian use of Houthi proxies in attacking commercial vessels from 2023 onwards.

Consider the infamous 1956 Suez crisis, where President Nasser announced the nationalization of the Suez Canal on July 26^{th}[259]. The operative objective of this nationalization was to leverage strategic power over European and Israeli off-takers and finance the construction of the Aswan Dam. The effect of this event was that downstream actors found themselves having been party to the costs arising from a series of manifested risks from sovereignty risk to constrained supply of critical resources, notably petroleum[259]. Israel, in particular, found itself in the precarious position of having its ability to ferry goods across the canal completely halted[259].

Likewise, the Iran-Iraq war illustrates how the cessation of physical transport significantly impacts a state's ability to generate revenues and acquire vital energy resources to operate downstream activities. The aptly-dubbed "Tanker War" manifested in the targeting of ports by both sides in the conflict, leading to the resuscitation of overland transport of petroleum by Iraq and disruption of shipping traffic in the Straits of Hormuz, not just for active participants in the war, but for the shipping activities of unrelated commodities inbound for Iraqi and Iranian ports[260].

To disrupt midstream supply-chain activities for an opponent, therefore, does not necessarily rely upon direct targeting of kinetic energy upon the transportation of goods by an opponent. All actors that must ferry their goods through specific logistical corridors keenly feel the knock-on n^{th} order effects of supply-chain disruption.

This reality is further conditioned in two different cases: the impact of the Ukrainian war on Black Sea trade and the contemporary case of shipping supply-chain reorientation from inbound and outbound traffic through the Bab El-Mandab and, subsequently, the Suez Canal.

In the first instance, the outbound flow of commodities (notably grain and energy) significantly decreased from Ukraine[261]. In concert with this decrease in Ukrainian exports, several other countries in the Black Sea region significantly increased their exports over the same time period as the supply-chain adapted to the lack of supply and upstream demand[261]. As risk is neither inherently positive nor negative as a concept, it should be noted that attacking the supply of different commodities by reducing supply can have positive knock-on effects for other potential commodity suppliers.

Thus, for any potential risk induction to have a significantly deleterious effect on the supply of a commodity, resulting in a negative impact on downstream actors, the magnitude of the risk induced must be sufficient to affect all suppliers in a region or market. When the case of constricted supply in the Black Sea contrasts with the impact of the supply and price of transportation arising from attacks on international shipping in the Bab El-Mandab region by Houthi military action, this condition for the efficacy of risk induction can be observed.

As a direct retaliation to the Israeli Defense Force's *'Swords of Iron'* operation, starting from November 19^{th}, 2023, Yemeni Houthi Rebels began targeting naval cargo ships, including oil tankers, with ordinance[237] in the Bab El-Mandab straight. This logistical straight is crucial to the inbound shipping of critical raw minerals to European and Western ports, as 28.8% of global raw mineral supply passed through that same corridor in 2019[262]. This series of actions prompted the cessation of shipping through perhaps one of the most critical global logistical corridors by firms such as MAERSK, Frontline Ltd., EURONAV, and other companies[238, 239]. Instead, these logistical firms and others rerouted freight traffic around the Cape of Good Hope. This supply-chain adaptation was accompanied by increased shipping premiums[240], increased delivery times for CRMs and other commodities[240], and deleterious effects on ports along this alternative route, which became overburdened due to being unable to forecast such black swan events[263].

It is problematic and erroneous to directly attribute the impact of these attacks to increased magnesium price volatility, as the dataset used previously for the calculation does not go beyond the end of January 2024, and there is no appreciable trend that can observed on the impact of magnesium volatility or prices. What can be affirmatively stated, however, is that the effects of these supply-chain disruptions resulted in increased financial stress on both logistical firms such as Maersk, which recorded a decrease in profits partially attributable to these activities from $29.2 billion to $3.8 billion[264], and revenues for state actors such as Egypt, which reported a 40% drop in revenue from the Suez Canal[265]. These effects are not transient as shipping costs remain impacted as of July 8^{th}[266], and so this attack vector remains a valid tool that an opponent may seek to leverage.

These are all instances of using kinetic energy in military contexts between state/quasi-state actors or the threat of applying kinetic energy to deny supply-chains the physical movement of goods. Force majeure events that impact counterparty risk need not be military when discussing cessation of the physical flows of goods, nor are they necessarily limited to shipping as the only form of transport.

An opponent can leverage technology risks to disrupt midstream supply activities through covert methods that offer more plausible deniability. For example, ship tracking technology, which notifies surrounding vessels as to its presence, is a well-established tool that is mandated by the 2002 Safety of Life at Sea (SOLAS) convention for ships over 300 gross tonnage (GT)[267] that can lead to the disruption of supply-chains in the event of Automatic Identification System (AIS) failure or non-compliance.

On October 7^{th}, 2023, the Hong Kong-flagged vessel *Newnew Polar Bear* arrived at the Estonian Exclusive Economic Zone (EEZ) from China via the Arctic Circle returning from a round trip that it had started in Saint Petersburg that summer, soon after it's Russian escort, the nuclear-powered vessel *Sevmorput*[268]. *Newnew Polar Bear* established communications with the Estonian Transport Administration during a storm and promptly ceased contact. Both ships presumably turned off their AIS transponders in contradiction to the SOLAS convention. Subsequently, both fiber optic cables and the

Balticconnector pipeline were found to be damaged on October 11^{th} by an anchor[268]. Although not directly provable by the damaged actors, this behavior pattern is representative of a pattern of behavior by Russian research vessels that purportedly operate with their transponders off[268].

Therefore, it is clear that the sabotage of critical transport infrastructure can be affected just as much by technology-related attacks like cyberwarfare as by non-compliance with regulatory standards and established operational practices. A hypothetical opponent attacking infrastructure under the cloak of plausible deniability can deliberately ignore regulatory requirements regulating technology.

E. Vector II: Cyberattacks - Software and Hardware

Using malicious software to compromise complex embedded systems is a well-established practice, both by private and state actors[269, 270]. Of course, the use of software to temporarily disable critical infrastructure or otherwise gain intelligence is by no means a phenomenon limited to midstream activities[271–274]. What this set of practices does represent, however, is a multi-domain threat that remains easily accessible to actors who would otherwise have little ability to apply kinetic energy to attacking their targets due to limited resources or the context of the operating environment[275–277][29]; because midstream activities are so broad in scope and intertwine the supply-chains of so many disparate commodities or goods which are often transported together across different nodal points, cyberwarfare provides a unique opportunity to create out-sized damage to downstream actors relative to the resources employed.

Midstream shipping, in particular, despite constituting a series of economic activities that are historically resistant to change[278, 279], are increasingly using tools such as machine learning at key logistical junctures[278, 280], notably ports such as Hamburg[278, 280], Rotterdam[281], and Singapore[282]. These logistical hubs constitute valuable downstream targets for disruption by an opponent, and technological risks associated with newly implemented systems ought to be considered by an actor seeking to induce risk.

In the maritime shipping industry, different machine learning networks have been applied in the literature to potential problems, including voyage optimization, maintenance and repair, freight cost, fuel consumption, and security practices[283, 284]. As machine learning techniques disperse across an increasing amount of freight transportation systems, as they already are[285], the attack surface for a malicious state actor seeking to induce risk will also increase.

[29] It ought to be noted that as the power of a state increases, however, so does its cyberattack capabilities[275].

F. Vector III: Leveraging Sovereign and Contractual Risk

Perhaps the most interesting potential attack vector that a hypothetical opponent may seek to use is the leveraging of sovereign risk. That is, a hypothetical actor may seek to utilize international regulation, or lack thereof, to alter the behavior of either itself or other state actors within a supply-chain to affect contractual obligations.

Two examples of this risk are the legal dispute over the Kirkuk-Ceyhan oil pipeline and the threatened cessation of oil exports to Israel to Turkey via the Baku-Tiblisi-Ceyhan pipeline[30].

In the first instance, the Iraqi State Organization for Marketing of Oil (SOMO), on behalf of the Iraqi Ministry of Oil, entered legal arbitration in the ICC International Court of Arbitration against the Turkish state for violating the Iraq-Turkiye Pipeline Agreement for transporting and storing Iraqi Kurdish oil, absent authorization from the Iraqi state, from 2014 to 2023[286]. The issue at hand was that the Iraqi state did not recognize the sovereignty of Iraqi Kurdistan, and so the Turkish state, which sought to utilize Iraqi Kurdistan as a bulwark against the Kurdish Worker's Party in neighboring Syria by recognizing the sovereignty of that semi-autonomous Iraqi region, was perceived to have exported oil without consent from the Iraqi state proper and therefore violated sovereignty[286]. While the Iraqi litigation effort succeeded, resulting in a restitution payment of $15 billion, this came at significant economic cost as the cessation of Kurdish oil exports of 450,000 barrels per day (bpd) resulted in monthly financial losses over $1 billion, precipitating severe economic losses not just in Iraq, but also for the Iraqi Kurdish region, Turkey, international firms that had been operating out of the Iraqi Kurdish region, and the world market which saw a decrease in global oil supply[286].

The second example, which is discussed in detail in the application of this framework to supply-chain risk weaponization, relates to how despite the Intergovernmental Agreement (IGA) and Host Government Agreement (HGA), which govern the operation of oil transport of approximately 1.2 mbpd (million barrels per day) nominally hold the Turkish state to being unable to halt the flow of critical primary energy in the Mediterranean area, the ruling of the ICJ regarding Israeli military actions in Gaza may constitute a sufficiently robust legal framework to cease operation of the pipeline in so far as providing Israeli off-takers with petroleum via maritime transport[287].

Sovereignty risk, therefore, encapsulates not only the issue of which a nation's sovereignty determines the contractual agreements between actors but also how, even when constrained by the contractual surrender of sovereignty, international bodies can be used to reassert sovereignty to pursue political objectives.

Thus, it is possible to conceive of a scenario where an offensive actor, either through a proxy or on

[30] Originally built in 1977[286]

its own behalf, enters into a contractual obligation in the territory of another state and then covertly engages in behavior in violation of the sovereignty of another nation knowing fully that its subsequent withdrawal from that contractual agreement, either during arbitration or after, will significantly impact both the global supply of magnesium as a commodity and the revenue generated by the counterparty.

Alternatively, the offensive actor may enter a contractual obligation with a counterparty that it knows will, at some point, violate its contractual obligations. The offensive actor may even seek to promote the violation of this contractual violation by leveraging techniques such as sub-rose payments of elements of the counterparty to induce such behavior. In turn, arising from the contractual clauses to which both parties are subject, the aggressive actor may call upon legal enforcement for the other party to surrender its assets or even sovereignty in select instances.

This is by no means a purely hypothetical scenario that has never occurred, nor is this vector only constrained to midstream elements. For instance, in their examination of one hundred loan agreements between Chinese creditors and non-Chinese counterparties, Gelpern et al. found that supply-chain assets were routinely used as securities by Chinese parties[136] against non-repayment of loans.

This was in part facilitated by through confidentiality clauses, the severance of diplomatic communication if a loan was defaulted on, at-will termination of the contract by the creditor arising from perceived emergence of risk events considered unfavorable beyond typical contractual scope, and agreement to arbitrate disputes under Chinese law and legal jurisdiction[136]. Confidentiality clauses were also employed, complicating risk management during debt restructuring and additionally obscuring other financial risk[136].

Currency-related risk burdens were also employed as a form of weapon, as in the case of BANDES - Venezuelan state-owned bank - where a foreign currency account was used as a form of security against sovereign foreign debtors[136]. 70% of all contractual agreements investigated by Gelpern et al. that mandated special accounts required revenues derived from operations funded by such contractual agreements to be sent to such accounts[136]. BANDES was explicitly prevented from withdrawing funds from this special account up to 35 days before loan repayment, unlike China Development Bank, which could do so at any time[136].

In instances where cash repayments of debt obligations were infeasible, alternative forms of security were used instead of direct repayment, including mining rights, PP&E[31], and other financial assets[136].

G. Vector IV: Policy and Structural Production Dumping

Product dumping refers to an actor exporting a commodity at prices lower than the fair market value[288]. Releasing excess supply of a commodity at lower-than-market prices onto the market is

[31] Plant, property, and equipment

a well-tested method of removing competing producers from the market[289–291]. Two variations of dumping concern this section: policy dumping and structural dumping. The former term refers to a practice where direct subsidization and ”export bounties” by a state result in a ”discriminative” low export price for a commodity[288].

Meanwhile, structural dumping arises from the economies of scale of enabling industrial production of a commodity to seize monopoly power in a market or to maintain full production capabilities without reducing domestic prices for a commodity[288]. The result of both manifestations is that the structural dumper will export their commodity or good at below international market prices to maintain mass-manufacturing efficiencies/economies of scale and to earn return on investment on capital-intensive production assets[288].

This practice can be observed in the behavior of numerous commodity producers, so much so that it was noted in a 2023 notice by the U.S. International Trade Administration and Department of Commerce regarding Chinese magnesium exports that,[292],

> ”The U.S. Department of Commerce (Commerce) and the U.S. International Trade Commission (ITC) have determined that revocation of the antidumping duty (AD) order on pure magnesium from the People’s Republic of China would likely lead to continuation or recurrence of dumping and material injury to industry in the United States.”

Price dumping to attack European critical infrastructure is not a direct conventional attack that induces risk and increases operational costs for critical European infrastructure. Instead, due to the overwhelming reliance of European industry and infrastructure on very few producers of Magnesium[182], production dumping can be utilized by an opponent to induce risk in European critical infrastructure operators by removing potential substitutes for magnesium suppliers.

By increasing the supply of magnesium commodities in the market beyond profitable quantities, presuming the attacker can bear the financial and operating risks, other magnesium suppliers face an increased ability to service their operating costs and liabilities if the price of magnesium becomes too low. Thus, production dumping magnifies the financial weakness of individual firms and the regional market risks borne by certain producers.

H. Vector IV: Inducing Political Instability through Covert Action

Inducing political instability for strategic was a key cornerstone of clandestine operations during the Cold War[293, 294], perhaps most infamously during the year 1960, following a failed CIA coup in the Democratic Republic of the Congo[295], where the Belgian Sûreté, the CIA and Ngondo’s Congolese Sûreté under Mobutu Sese Seko and the Binza Group, conspired to remove the Prime Minister, Patrice

Lamumba, as an opponent[296–301]. In part, these actions were motivated by the desire to secure mineral control in Katanga and Kivu provinces for Société Générale de Belgique[302], which are to this day rich in Coltan, Cobalt, Diamonds, Uranium, REEs, and other resources[303, 304].

Inducing political instability for strategy was an essential cornerstone of clandestine operations during the Cold War[293, 294], perhaps most infamously during the year 1960, following a failed CIA coup in the Democratic Republic of the Congo[295], where the Belgian Sûreté, the CIA and Ngondo's Congolese Sûreté under Mobutu Sese Seko and the Binza Group, conspired to remove the Prime Minister, Patrice Lamumba as an opponent[296–301]. In part, these actions were motivated by the desire to secure mineral control in Katanga and Kivu provinces for Société Générale de Belgique[302], which are to this day rich in Coltan, Cobalt, Diamonds, Uranium, REEs, and other resources[303, 304].

A theoretical opponent can employ a variety of methods to achieve political instability, drawing upon historical implementation of cover tools including funding political parties as in Chile[294], political actions groups[294], acquiring control of media publications to disseminate favorable information or to control narratives[294], coups[294, 305], bribery[305], funding militant groups in opposition of the government in an area of interest or an invading force[306], sometimes through illicit activities such as the narcotics trade[307], and political assassination[305].

VIII. Discussion and Conclusion

By creating a generic framework for disaggregated risks that could be applied to any commodity supply-chain, and then identifying how an opponent may seek to induce these various classes and sub-classes of risk, this paper helps to broaden the understanding of risk from a technical perspective in the context of securing critical supply-chains which are crucial to the economic and military security of different EU member states. Doing so has created a durable and flexible framework that can be reapplied and refined in other contexts and further investigations. This, in turn, will allow for future investigations and analysis in the Security and Strategic Studies frameworks to apply risk as a concept from the perspective of those stakeholders in a supply-chain that are responsible for the construction and operation of those systems.

The five identified vectors of attack discussed in the previous section are, constrained by the scope of analysis, broad and by no means extensive. To examine each individually would require a much narrower focus on different elements of the magnesium supply-chain, how specific segments of the supply-chain contribute to the flow and maintenance of goods relevant to each European critical infrastructure sector, and the degree to which these goods and magnesium-derivative commodities are pertinent to the operations of these systems. An analyst cannot accomplish such a feat in a single iterative, chronological walk through the DSR design cycle. Instead, this paper provides a framework: a prescriptive model, which is amenable to change depending on the contextual circumstances and commodity to which it is applied, that re-orientates analysis of strategic thinking regarding how an opponent could conceive of how to target different supply-chains on the basis that stakeholders perceive the financing and operations of these supply-chain elements systematically.

Arising from the axiomatic realist objectives of the constructed opponent, outlined in Section IV-C.1, and in line with offensive realist axioms relating to the anarchic world order, state rationality, and the uncertainty of other actors in the geopolitical area, it is difficult to evaluate which attack present themselves as the most feasible. For one, even if an opponent is confident as to the potential retaliatory behavior of its target within certain confidence limits, the holistic nature of supply-chains ensures that it is difficult to target only a specific subset of supply-chain actors. Indeed, to ensure that nominal allies do not bandwagon with retaliatory efforts if an attack is attributed to the correct attacker, arrangements in the form of bilateral or multilateral risk management will need to be struck.

Secondly, the capabilities of a theoretical opponent that seeks to attack supply-chains, not just in material access to assets which may be used to disrupt supply-chain elements, but also the positioning of that actor in the supply-chain, underpin which and *when* attack vectors ought to be attacked for optimal (not necessarily maximum) risk induction. As all complex systems that regulate the behavior of supply-chains are time-bound, the timing of an attack becomes a critical component in when an attack vector will present itself.

Such conditions complicate an attacker's calculus and should be considered in future iterations of this model. Of course, if the same broad resolution of analysis is taken in a future iteration that examines an entire set of commodity and commodity derivative supply-chains. In that case, the same issue outlined in the first paragraph of this section holds when applied to timing supply-chain attacks and accounting for retaliation.

Another weakness of this model is that it does not frame the theoretical manifestation of the offensive actor's decision-making calculus. Whereas broader realist models such as Fearon's *'Rationalist Explanations for War'* provide a mathematical bargaining range month and algorithmic basis for the behaviors that determine whether or not a state is willing to go to war[308], which could be extended in application to the decision of if a state should attack a supply-chain, this framework does not have provisions for such considerations. However, using DSR protocols, there is no reason a future iteration of this model could not be adapted for such purposes, given the correct orientation of the system scope.

The decision not to incorporate such a mechanism into the framework presented in this paper was deliberate. Due to the complexity and number of different stakeholders in magnesium and magnesium-adjacent supply-chains, accounting for such a model without a narrower scope of analysis would result in a spiraling, monolithic model that would inevitably never be able to capture the complexity of the entire magnesium supply-chain system.

In conclusion, the disaggregated risk framework and subsequent application to upstream, midstream, and downstream elements of magnesium-related supply-chains provides a reorientation of perspective regarding how to defend against malicious, deliberate actions by aggressive actors against European supply-chains by accomplishing two objectives: first, orientating analysis of these elements in the context of security around the opponent's perspective on how risks may be exploited, and by conceptualizing risk in security contexts in the same manner that the systems which are targeted are themselves conceived, operated, and maintained by their stakeholders in accordance with best practices.

Future implementation of this framework should be orientated around the refinement of risk categories in line with further research regarding each relevant critical infrastructure and supply-chain element by refining the scope of application to narrower investigations to generate a greater explanatory understanding of how opponents may seek to disrupt supply-chain operations. Emphasis should also be focused on identifying other potential attack vectors and examining how those attack vectors identified in this paper may be expanded by future research in specificity by generating a procedural framework for that purpose or reviewing other relevant case studies for each specific vector.

REFERENCES

[1] L.M Farrell. “Principal-agency risk in project finance”. In: *International Journal of Project Management* 21.8 (2003), pp. 547–561. ISSN: 0263-7863. DOI: https://doi.org/10.1016/S0263-7863(02)00086-8. URL: https://www.sciencedirect.com/science/article/pii/S0263786302000868.

[2] Marcin Szczepański. *Resilience of global supply chains: Challenges and solutions.* Briefing PE 698.815. European Parliamentary Research Service, Nov. 2021. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698815/EPRS_BRI(2021)698815_EN.pdf.

[3] The White House. *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth.* 100-Day Reviews under Executive Order 14017. The White House, June 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[4] Christian Bogmans et al. *The Power of Prices: How Fast Do Commodity Markets Adjust to Shocks?* IMF Working Paper WP/24/77. Washington, DC: International Monetary Fund, 2024. URL: https://www.imf.org/-/media/Files/Publications/WP/2024/English/wpiea2024077-print-pdf.ashx.

[5] Elena Maria Diaz, Juncal Cunado, and Fernando Perez de Gracia. “Commodity price shocks, supply chain disruptions and U.S. inflation”. In: *Finance Research Letters* 58 (2023), p. 104495. ISSN: 1544-6123. DOI: https://doi.org/10.1016/j.frl.2023.104495. URL: https://www.sciencedirect.com/science/article/pii/S154461232300867X.

[6] Hillary C. Ezeaku, Simplice A. Asongu, and Joseph Nnanna. “Volatility of international commodity prices in times of COVID-19: Effects of oil supply and global demand shocks”. In: *The Extractive Industries and Society* 8.1 (2021), pp. 257–270. ISSN: 2214-790X. DOI: https://doi.org/10.1016/j.exis.2020.12.013. URL: https://www.sciencedirect.com/science/article/pii/S2214790X20303300.

[7] Joshua Aizenman et al. “Geopolitical shocks and commodity market dynamics: New evidence from the Russia-Ukraine conflict”. In: *European Journal of Political Economy* 85 (2024), p. 102574. ISSN: 0176-2680. DOI: https://doi.org/10.1016/j.ejpoleco.2024.102574. URL: https://www.sciencedirect.com/science/article/pii/S0176268024000764.

[8] Ellen Cristine Giese. "Strategic minerals: Global challenges post-COVID-19". In: *The Extractive Industries and Society* 12 (2022), p. 101113. ISSN: 2214-790X. DOI: https://doi.org/10.1016/j.exis.2022.101113. URL: https://www.sciencedirect.com/science/article/pii/S2214790X22000788.

[9] Rajeev K. Goel, James W. Saunoris, and Srishti S. Goel. "Supply chain performance and economic growth: The impact of COVID-19 disruptions". In: *Journal of Policy Modeling* 43.2 (2021), pp. 298–316. ISSN: 0161-8938. DOI: https://doi.org/10.1016/j.jpolmod.2021.01.003. URL: https://www.sciencedirect.com/science/article/pii/S0161893821000065.

[10] Edgar E Blanco et al. "Using discrete-event simulation for evaluating non-linear supply chain phenomena". In: *Proceedings of the 2011 Winter Simulation Conference (WSC)*. 2011, pp. 2255–2267. DOI: 10.1109/WSC.2011.6147937.

[11] Hiroyasu Inoue. "Propagation of International Supply-Chain Disruptions between Firms in a Country". In: *Journal of Risk and Financial Management* 14.10 (2021). ISSN: 1911-8074. DOI: 10.3390/jrfm14100461. URL: https://www.mdpi.com/1911-8074/14/10/461.

[12] European Commission. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020*. Tech. rep. Mar. 2023. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:903d35cc-c4a2-11ed-a05c-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[13] European Commission. *ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020*. Tech. rep. Mar. 2023, pp. 4–5. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:903d35cc-c4a2-11ed-a05c-01aa75ed71a1.0001.02/DOC_2&format=PDF.

[14] Meletios Bimpizas-Pinis, Tommaso Calzolari, and Andrea Genovese. "Exploring the transition towards circular supply chains through the arcs of integration". In: *International Journal of Production Economics* 250 (2022). Special Issue celebrating Volume 250 of the International Journal of Production Economics, p. 108666. ISSN: 0925-5273. DOI: https://doi.org/

10.1016/j.ijpe.2022.108666. URL: https://www.sciencedirect.com/science/article/pii/S0925527322002481.

[15] Xiao Xu et al. “Active management strategy for supply chain system using nonlinear control synthesis”. In: *International Journal of Dynamics and Control* 10 (Mar. 2022). DOI: 10.1007/s40435-021-00901-5.

[16] Mark A Vonderembse et al. “Designing supply chains: Towards theory development”. In: *International Journal of production economics* 100.2 (2006), pp. 223–238.

[17] Brunelle Marche et al. “Overview of phenomena occurring in supply chains during the emergence of innovation”. In: *Supply Chain Forum: An International Journal* 18.3 (2017), pp. 150–165. DOI: 10.1080/16258312.2017.1354649. eprint: https://doi.org/10.1080/16258312.2017.1354649. URL: https://doi.org/10.1080/16258312.2017.1354649.

[18] Borut Buchmeister, Darko Friscic, and Iztok Palcic. “Bullwhip Effect Study in a Constrained Supply Chain”. In: *Procedia Engineering* 69 (2014). 24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013, pp. 63–71. ISSN: 1877-7058. DOI: https://doi.org/10.1016/j.proeng.2014.02.204. URL: https://www.sciencedirect.com/science/article/pii/S1877705814002069.

[19] Hau L. Lee, V. Padmanabhan, and Seungjin Whang. “Information Distortion in a Supply Chain: The Bullwhip Effect”. In: *Management Science* 43.4 (1997), pp. 546–558. ISSN: 00251909, 15265501. URL: http://www.jstor.org/stable/2634565 (visited on 09/12/2023).

[20] Y. Yang et al. “The behavioural causes of bullwhip effect in supply chains: A systematic literature review”. In: *International Journal of Production Economics* 236 (2021), p. 108120. ISSN: 0925-5273. DOI: https://doi.org/10.1016/j.ijpe.2021.108120. URL: https://www.sciencedirect.com/science/article/pii/S0925527321000967.

[21] Xun Wang and Stephen M. Disney. “The bullwhip effect: Progress, trends and directions”. In: *European Journal of Operational Research* 250.3 (2016), pp. 691–701. ISSN: 0377-2217. DOI: https://doi.org/10.1016/j.ejor.2015.07.022. URL: https://www.sciencedirect.com/science/article/pii/S0377221715006554.

[22] Jay Wright Forrester. “Industrial dynamics”. In: *Journal of the Operational Research Society* 48.10 (1997), pp. 1037–1041.

[23] Francesca Gino and Gary Pisano. “Toward a Theory of Behavioral Operations”. In: *Manufacturing & Service Operations Management* 10 (Oct. 2008), pp. 676–691. DOI: 10.1287/msom.1070.0205.

[24] Christoph H. Loch and Yaozhong Wu. “Behavioral Operations Management”. In: *Foundations and Trends® in Technology, Information and Operations Management* 1.3 (2007), pp. 121–232. ISSN: 1571-9545. DOI: 10.1561/0200000009. URL: http://dx.doi.org/10.1561/0200000009.

[25] R. Lafrogne-Joussier, J. Martin, and I. Mejean. “Supply Shocks in Supply Chains: Evidence from the Early Lockdown in China”. In: *IMF Economic Review* 71 (2023), pp. 170–215. DOI: 10.1057/s41308-022-00166-8. URL: https://doi.org/10.1057/s41308-022-00166-8.

[26] Dmitry Ivanov et al. “Disruptions in supply chains and recovery policies: state-of-the art review”. In: *IFAC-PapersOnLine* 49.12 (2016). 8th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2016, pp. 1436–1441. ISSN: 2405-8963. DOI: https://doi.org/10.1016/j.ifacol.2016.07.773. URL: https://www.sciencedirect.com/science/article/pii/S2405896316310540.

[27] William Harris and Moufida Sadok. “How do professionals assess security risks in practice? An exploratory study”. In: *Security Journal* (July 2023). ISSN: 1743-4645. DOI: 10.1057/s41284-023-00389-y. URL: https://doi.org/10.1057/s41284-023-00389-y.

[28] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. “Taxonomy of Information Security Risk Assessment (ISRA)”. In: *Computers & Security* 57 (Nov. 2015). DOI: 10.1016/j.cose.2015.11.001.

[29] Nicola Gennaioli, Andrei Shleifer, and Robert Vishny. “Neglected Risks: The Psychology of Financial Crises”. In: *American Economic Review* 105.5 (May 2015), pp. 310–14. DOI: 10.1257/aer.p20151091. URL: https://www.aeaweb.org/articles?id=10.1257/aer.p20151091.

[30] Katharina Wolff, Svein Larsen, and Torvald Øgaard. “How to define and measure risk perceptions”. In: *Annals of Tourism Research* 79 (2019), p. 102759. ISSN: 0160-7383. DOI: https://doi.org/10.1016/j.annals.2019.102759. URL: https://www.sciencedirect.com/science/article/pii/S0160738319301161.

[31] Russell Winer and Peter Bernstein. “Against The Gods: The Remarkable Story of Risk”. In: *Journal of Marketing* 61 (July 1997), p. 112. DOI: 10.2307/1251793.

[32] C Ariel Pinto, Michael Mcshane, and Ipek Bozkurt. “System of systems perspective on risk: Towards a unified concept”. In: *International Journal of System of Systems Engineering* 3 (Apr. 2012), pp. 33–46. DOI: 10.1504/IJSSE.2012.046558.

[33] James L. Athearn. “What is Risk?” In: *The Journal of Risk and Insurance* 38.4 (1971), pp. 639–645. ISSN: 00224367, 15396975. URL: http://www.jstor.org/stable/251578 (visited on 02/07/2024).

[34] Mark R. Greene and James S. Trieschmann. *Risk management and insurance*. eng. 6th ed. Section: XI, 626 Seiten : Diagramme. Cincinnati, Oh.: South-Western Cincinnati, Oh., 1984. ISBN: 0-538-06540-0 978-0-538-06540-5.

[35] Robert M. Crowe and Ronald C. Horn. “The Meaning of Risk”. In: *The Journal of Risk and Insurance* 34.3 (1967), pp. 459–474. ISSN: 00224367, 15396975. URL: http://www.jstor.org/stable/250861 (visited on 09/09/2023).

[36] A.H. Willett. *The Economic Theory of Risk and Insurance*. Studies (S.S. Huebner Foundation for Insurance Education). University of Pennsylvania Press, 1954. URL: https://books.google.cz/books?id=-tzuAAAAMAAJ.

[37] Oliver G. Wood. “Evolution of the Concept of Risk”. In: *The Journal of Risk and Insurance* 31.1 (1964), pp. 83–91. ISSN: 00224367, 15396975. URL: http://www.jstor.org/stable/251211 (visited on 02/07/2024).

[38] Stephen F. LeRoy and Larry D. Singell. “Knight on Risk and Uncertainty”. In: *Journal of Political Economy* 95.2 (1987), pp. 394–406. URL: http://www.jstor.org/stable/1832078.

[39] Frank H. Knight. *Risk, uncertainty and profit*. eng. xiv, 381, [1] pages diagrams 21 cm. Boston: Houghton Mifflin Company Boston, 1921.

[40] Glyn A. Holton. “Defining Risk”. In: *Financial Analysts Journal* 60.6 (2004), pp. 19–25. ISSN: 0015198X. URL: http://www.jstor.org/stable/4480615 (visited on 09/09/2023).

[41] *ISO-31000:2018(E) Risk Management - Guidelines*. Standard. Geneva, CH: International Organization for Standardization, Feb. 2018. URL: https://www.iso.org/standard/65694.html.

[42] Securities and Exchange Commission. *What is risk?* URL: https://www.investor.gov/introduction-investing/investing-basics/what-risk.

[43] Dentons. In: *A Guide to Project Finance* (2013). URL: https://www.dentons.com/~/media/6a199894417f4877adea73a76caac1a5.ashx.

[44] Headquarters, Department of the Army. *Risk Management*. 2021st ed. Army Publishing Directorate, 2021, pp. 15–16. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34181-ATP_5-19-000-WEB-1.pdf.

[45] David Brooks and Hamish Cotton. “Security risk management in the Asia Pacific region: what are security professional using?” In: 2011. DOI: 10.4225/75/57A00F0DAC5C1. URL: https://api.semanticscholar.org/CorpusID:166278446.

[46] Jonathan M. Spring, Tyler Moore, and David Pym. “Practicing a science of security, a philosophy of science perspective”. In: *Proceedings of the New Security Paradigms Workshop (NSPW)*. ACM. Santa Cruz, CA, USA, Oct. 2017, p. 47.

[47] ISO. “Iso/iec 31010: 2009-Risk Assessment Techniques”. In: *International Organization for Standardization, Geneva-Switzerland* (2009).

[48] Committee of Sponsoring Organizations of the Treadway Commission. *From the cube to the rainbow double helix: a risk practitioner’s guide to the COSO ERM Frameworks*. Tech. rep. : 2nd Floor, Sackville House, 143-149 Fenchurch Street, London, EC3M 6BN: Institute of Risk Managment. URL: https://www.theirm.org/media/6885/irm-report-review-of-the-coso-erm-frameworks-v2.pdf.

[49] Anoma Edirimanna. “Enterprise Risk Management - International Standards and Frameworks”. In: *International Journal of Scientific and Research PublicatiSithipolvanichgul, J., (2016). Enterprise Risk Management and Firm Performance: Developing Risk Management Measurement in Accounting Practice. (Doctoral Dissertation, University of Edinburgh, London)ons (IJSRP)* 9 (July 2019), pp. 211–217. DOI: 10.29322/IJSRP.9.07.2019.p9130.

[50] Juthamon Sithipolvanichgul. “Enterprise risk management and firm performance : developing risk management measurement in accounting practice”. In: 2016. URL: https://api.semanticscholar.org/CorpusID:168721834.

[51] Abroon Qazi, John Quigley, and Alex Dickson. “Supply Chain Risk Management: Systematic literature review and a conceptual framework for capturing interdependencies between risks”. In: *2015 International Conference on Industrial Engineering and Operations Management (IEOM)*. 2015, pp. 1–13. DOI: 10.1109/IEOM.2015.7093701.

[52] Ou Tang and S. Nurmaya Musa. “Identifying risk issues and research advancements in supply chain risk management”. In: *International Journal of Production Economics* 133.1 (2011). Leading Edge of Inventory Research, pp. 25–34. ISSN: 0925-5273. DOI: https://doi.org/10.1016/j.ijpe.2010.06.013. URL: https://www.sciencedirect.com/science/article/pii/S0925527310002215.

[53] Sunil Chopra and Manmohan Sodhi. “Managing Risk to Avoid Supply-Chain Breakdown”. In: *MIT Sloan Management Review* (Sept. 2004).

[54] Martin Christopher and Helen Peck. “Building the Resilient Supply Chain”. In: *International Journal of Logistics Management* 15 (July 2004), pp. 1–13. DOI: 10.1108/09574090410700275.

[55] Xi Chen, Zhimin Xi, and Pengyuan Jing. “A Unified Framework for Evaluating Supply Chain Reliability and Resilience”. In: *IEEE Transactions on Reliability* 66.4 (2017), pp. 1144–1156. DOI: 10.1109/TR.2017.2737822.

[56] Jieping Liu. “Supply Chain Finance Business Risk Evaluation Scheme Based on Fuzzy Theory”. In: *2015 International Conference on Intelligent Transportation, Big Data and Smart City*. 2015, pp. 809–812. DOI: 10.1109/ICITBS.2015.204.

[57] Aida Elamrani, Loubna Benabbou, and Abdelaziz Berrado. “A framework for identification and classification of outsourcing related organizational risks in a pharmaceutical supply chain”. In: *2016 3rd International Conference on Logistics Operations Management (GOL)*. 2016, pp. 1–6. DOI: 10.1109/GOL.2016.7731667.

[58] Valery G. Semin et al. “A process model of risk management in the system of management of strategic sustainability of cargo motor transport enterprises”. In: *2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS)*. 2016, pp. 172–175. DOI: 10.1109/ITMQIS.2016.7751951.

[59] Peng Peng et al. “Reliable logistics networks design with facility disruptions”. In: *Transportation Research Part B: Methodological* 45 (Sept. 2011), pp. 1190–1211. DOI: 10.1016/j.trb.2011.05.022.

[60] Mahmut Parlar. “Continuous-review inventory problem with random supply interruptions”. In: *European Journal of Operational Research* 99.2 (1997), pp. 366–385. ISSN: 0377-2217. DOI: https://doi.org/10.1016/S0377-2217(96)00165-8. URL: https://www.sciencedirect.com/science/article/pii/S0377221796001658.

[61] Che Ruhana Isa Xiang Zou and Mahfuzur Rahman. “Valuation of enterprise risk management in the manufacturing industry”. In: *Total Quality Management & Business Excellence* 30.11-12 (2019), pp. 1389–1410. DOI: 10.1080/14783363.2017.1369877. eprint: https://doi.org/10.1080/14783363.2017.1369877. URL: https://doi.org/10.1080/14783363.2017.1369877.

[62] Jagjit Singh Srai Mukesh Kumar and Mike Gregory. “Risk management in plant investment decisions: risk typology, dimensions and process”. In: *Production Planning & Control* 27.9 (2016), pp. 761–773. DOI: 10.1080/09537287.2016.1166280. eprint: https://doi.

org/10.1080/09537287.2016.1166280. URL: https://doi.org/10.1080/09537287.2016.1166280.

[63] Byung Yong Jeong Seung Tae Yang and Myoung Hwan Park. “Analysis of occupational injuries and the risk management of automobile parts manufacturing work”. In: *International Journal of Occupational Safety and Ergonomics* 27.3 (2021). PMID: 31928161, pp. 884–895. DOI: 10.1080/10803548.2020.1715101. eprint: https://doi.org/10.1080/10803548.2020.1715101. URL: https://doi.org/10.1080/10803548.2020.1715101.

[64] Yu Tian Alexander E. Ellinger Haozhe Chen and Craig Armstrong. “Learning orientation, integration, and supply chain risk management in Chinese manufacturing firms”. In: *International Journal of Logistics Research and Applications* 18.6 (2015), pp. 476–493. DOI: 10.1080/13675567.2015.1005008. eprint: https://doi.org/10.1080/13675567.2015.1005008. URL: https://doi.org/10.1080/13675567.2015.1005008.

[65] John Johansen Yang Cheng Sami Farooq and Chris O’Brien. “The management of international manufacturing networks: a missing link towards total management of global networks”. In: *Production Planning & Control* 30.2-3 (2019), pp. 91–95. DOI: 10.1080/09537287.2018.1534273. eprint: https://doi.org/10.1080/09537287.2018.1534273. URL: https://doi.org/10.1080/09537287.2018.1534273.

[66] Marta Rinaldi et al. “A literature review on quantitative models for supply chain risk management: Can they be applied to pandemic disruptions?” In: *Computers & Industrial Engineering* 170 (2022), p. 108329. ISSN: 0360-8352. DOI: https://doi.org/10.1016/j.cie.2022.108329. URL: https://www.sciencedirect.com/science/article/pii/S0360835222003825.

[67] Seyedmohsen Hosseini, Dmitry Ivanov, and Alexandre Dolgui. “Review of quantitative methods for supply chain resilience analysis”. In: *Transportation Research Part E: Logistics and Transportation Review* 125 (2019), pp. 285–307. ISSN: 1366-5545. DOI: https://doi.org/10.1016/j.tre.2019.03.001. URL: https://www.sciencedirect.com/science/article/pii/S1366554518313589.

[68] B. Biringer, E. Vugrin, and D. Warren. *Critical Infrastructure System Security and Resiliency*. 1st. CRC Press, 2013. DOI: 10.1201/b14566.

[69] Samer Alhawari et al. “Knowledge-based risk management framework for information technology project”. In: *International Journal of Information Management* 32.1 (2012), pp. 50–65.

[70] Amulya Gurtu and Jestin Johny. "Supply Chain Risk Management: Literature Review". In: *Risks* 9.1 (2021). ISSN: 2227-9091. DOI: 10.3390/risks9010016. URL: https://www.mdpi.com/2227-9091/9/1/16.

[71] Guo Yuntao, Li Suike, and Bai Sijun. "Framework of comprehensive risk management system for the defense science and technology enterprises". In: *2011 International Conference on Business Management and Electronic Information*. Vol. 3. 2011, pp. 213–216. DOI: 10.1109/ICBMEI.2011.5920431.

[72] A. Ganguly, R. Nilchiani, and J. V. Farr. "Using a Systems Process to Assess the Potential for a Disruptive Technology". In: *Conference on Systems Engineering Research*. Los Angeles, CA, Mar. 2008.

[73] Anirban Ganguly, Mo Mansouri, and Roshanak Nilchiani. "A Risk Assessment Framework for analyzing risks associated with a Systems Engineering Process". In: *2010 IEEE International Systems Conference*. 2010, pp. 484–489. DOI: 10.1109/SYSTEMS.2010.5482460.

[74] Andrew Kinder, Michael Henshaw, and Carys Siemieniuch. "A model based approach to system of systems risk management". In: *2015 10th System of Systems Engineering Conference (SoSE)*. 2015, pp. 122–127. DOI: 10.1109/SYSOSE.2015.7151940.

[75] Oroitz Elgezabal and Holger Schumann. "Holistic Systems Engineering: Towards a cross-disciplinary standard". In: Nov. 2012, pp. 319–328. ISBN: 978-3-446-43435-6. DOI: 10.3139/9783446436039.032.

[76] Lukas Bretz, Lydia Kaiser, and Roman Dumitrescu. "An analysis of barriers for the introduction of Systems Engineering". In: *Procedia CIRP* 84 (2019). 29th CIRP Design Conference 2019, 08-10 May 2019, Póvoa de Varzim, Portgal, pp. 783–789. ISSN: 2212-8271. DOI: https://doi.org/10.1016/j.procir.2019.04.178. URL: https://www.sciencedirect.com/science/article/pii/S2212827119308005.

[77] Charles Keating et al. "System of Systems Engineering". In: *Engineering Management Review, IEEE* 15 (Sept. 2003), pp. 62–62. DOI: 10.1109/EMR.2008.4778760.

[78] Wolfgang Kröger. "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools". In: *Reliability Engineering & System Safety* 93 (Dec. 2008), pp. 1781–1787. DOI: 10.1016/j.ress.2008.03.005.

[79] Defense Acquisition University. *Systems Engineering Fundamentals: January 2001*. U.S. Government Printing Office, 2005. ISBN: 9780160732904. URL: https://books.google.cz/books?id=wlwBPQAACAAJ.

[80] David R. Mandel. *Toward a Concept of Risk for Effective Military Decision Making*. Technical Report DRDC Toronto TR 2007-124. Approved for release by K. C. Wulterkens, Chair, Document Review and Library Committee. Toronto: Defence Research and Development Canada, Dec. 2007. URL: https://www.researchgate.net/profile/David-Mandel-4/publication/235095366_Toward_a_Concept_of_Risk_for_Effective_Military_Decision_Making/links/00b7d528442a5a27de000000/Toward-a-Concept-of-Risk-for-Effective-Military-Decision-Making.pdf.

[81] Constantin Preda. “Defense Programs Risk Management Framework”. In: *Journal of Defense Resources Management* 3.2 (2012). Print, Pdf Version, pp. 51–56. URL: http://www.jodrm.eu/issues/volume3_issue2/04_preda.pdf.

[82] Kevin M. Bernhardt. “Risk and Decision Making in Military Operations”. Approved for public release. Distribution is unlimited. Master’s thesis. Monterey, California: Naval Postgraduate School, June 2020. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1114658.pdf.

[83] Hans Liwång. “Risk communication within military decision-making: pedagogic considerations”. In: *Defense & Security Analysis* 33.1 (2017), pp. 30–44. DOI: 10.1080/14751798.2016.1269389. eprint: https://doi.org/10.1080/14751798.2016.1269389. URL: https://doi.org/10.1080/14751798.2016.1269389.

[84] Hans Liwång, Marika Ericson, and Martin Bang. “An Examination of the Implementation of Risk Based Approaches in Military Operations”. In: *Journal of Military Studies* 5 (Dec. 2014). DOI: 10.1515/jms-2016-0189.

[85] Wade A. Germann and Heather S. Gregg. “Assessing Risk at the National Strategic Level: Visualization Tools for Military Planners”. In: *Parameters* 51.3 (2021). DOI: 10.55540/0031-1723.3078. URL: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3078&context=parameters.

[86] Jerry Vanvactor. “Risk mitigation through a composite risk management process: The U.S. Army risk assessment”. In: *Organization Development Journal* 25 (June 2007), pp. 133–138.

[87] Svetoslav Gaidow and Seng Boey. *Australian Defence Risk Management Framework: A Comparative Study*. Tech. rep. DSTO-GD-0427. Approved for public release. Edinburgh South Australia: DSTO Systems Sciences Laboratory, Feb. 2005. URL: https://apps.dtic.mil/sti/tr/pdf/ADA434592.pdf.

[88] Peter Layton. "SYSTEMATIZING SUPPLY CHAIN WARFARE". In: *Æther: A Journal of Strategic Airpower & Spacepower* 2.2 (2023), pp. 62–80. ISSN: 27716120, 27716139. URL: https://www.jstor.org/stable/48735692 (visited on 10/22/2023).

[89] B van Niekerk and T Ramluckan. "Economic Information Warfare: Feasibility and Legal Considerations for Cyber-Operations Targeting Commodity Value Chains". In: *Journal of Information Warfare* 18.2 (2019), pp. 31–48. ISSN: 14453312, 14453347. URL: https://www.jstor.org/stable/26894669 (visited on 09/08/2023).

[90] Gerald G. Brown et al. "Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses". In: *Emerging Theory, Methods, and Applications*. Chap. Chapter 4, pp. 102–123. DOI: 10.1287/educ.1053.0018. eprint: https://pubsonline.informs.org/doi/pdf/10.1287/educ.1053.0018. URL: https://pubsonline.informs.org/doi/abs/10.1287/educ.1053.0018.

[91] Shane Bilsborough. "The Strategic Implications of China's Rare Earths Policy". In: *Journal of Strategic Security* 5.3 (2012), pp. 1–12. ISSN: 19440464, 19440472. URL: http://www.jstor.org/stable/26463947 (visited on 10/19/2023).

[92] Matthew P. Funaiole, Brian Hart, and Aidan Powers-Riggs. "De-risking Gallium Supply Chains: The National Security Case for Eroding China's Critical Mineral Dominance". In: (2023). URL: http://www.jstor.org/stable/resrep52704 (visited on 10/20/2023).

[93] Lianbiao Cui et al. "Exploring the risk and economic vulnerability of global energy supply chain interruption in the context of Russo-Ukrainian war". In: *Resources Policy* 81 (2023), p. 103373. ISSN: 0301-4207. DOI: https://doi.org/10.1016/j.resourpol.2023.103373. URL: https://www.sciencedirect.com/science/article/pii/S0301420723000818.

[94] W. Julian Korab-Karpowicz. "Political Realism in International Relations". In: *The Stanford Encyclopedia of Philosophy* (2023). Ed. by Edward N. Zalta and Uri Nodelman. URL: https://plato.stanford.edu/archives/win2023/entries/realism-intl-relations/.

[95] Jeffrey W. Taliaferro. "Security Seeking under Anarchy: Defensive Realism Revisited". In: *International Security* 25.3 (2000), pp. 128–161. ISSN: 01622889, 15314804. URL: http://www.jstor.org/stable/2626708 (visited on 06/18/2024).

[96] Barry R. Posen. "The Best Defense". In: *The National Interest* 67 (2002), pp. 119–126. ISSN: 08849382, 19381573. URL: http://www.jstor.org/stable/42897407 (visited on 06/18/2024).

[97] Arnold Wolfers. “THE BALANCE OF POWER IN THEORY AND PRACTICE”. In: *Naval War College Review* 11.5 (1959), pp. 1–20. ISSN: 00281484, 24757047. URL: `http://www.jstor.org/stable/45139621` (visited on 06/19/2024).

[98] Partha Chatterjee. “The Classical Balance of Power Theory”. In: *Journal of Peace Research* 9.1 (1972), pp. 51–61. ISSN: 00223433. URL: `http://www.jstor.org/stable/422972` (visited on 06/19/2024).

[99] Hans J. Morgenthau. *Politics Among Nations*. 4th. New York: Knopf, 1967, pp. 4–14.

[100] Hans J. Morgenthau. *Dilemmas of Politics*. Chicago: University of Chicago Press, 1957, p. 270.

[101] Hans J. Morgenthau and Kenneth W. Thompson. *Principles and Problems of International Politics*. Ed. by Hans J. Morgenthau and Kenneth W. Thompson. New York: Knopf, 1950, p. 104.

[102] Robert O. Keohane. “Alliances, Threats, and the Uses of Neorealism”. In: *International Security* 13.1 (1988), pp. 169–176. ISSN: 01622889, 15314804. URL: `http://www.jstor.org/stable/2538899` (visited on 06/20/2024).

[103] Dominic D. P. Johnson and Bradley A. Thayer. “The evolution of offensive realism: Survival under anarchy from the Pleistocene to the present”. In: *Politics and the Life Sciences* 35.1 (2016), pp. 1–26. ISSN: 07309384, 14715457. URL: `https://www.jstor.org/stable/26372766` (visited on 06/17/2024).

[104] John J. Mearsheimer. “The False Promise of International Institutions”. In: *International Security* 19.3 (1994), pp. 5–49. ISSN: 01622889, 15314804. URL: `http://www.jstor.org/stable/2539078` (visited on 06/17/2024).

[105] C. Layne. *The Peace of Illusions: American Grand Strategy from 1940 to the Present*. Cornell studies in security affairs. Cornell University Press, 2006. ISBN: 9780801474118. URL: `https://books.google.cz/books?id=3Gzrfmkw80MC`.

[106] Robert Jervis. “Cooperation under the Security Dilemma”. In: *World Politics* 30.2 (Jan. 1978), pp. 167–214.

[107] Jeffrey W. Legro and Andrew Moravcsik. “Is Anybody Still a Realist?” In: *International Security* 24.2 (1999), pp. 5–55.

[108] Randall L. Schweller. “Neorealism’s Status Quo Bias: What Security Dilemma?” In: *Security Studies* 5.3 (1996), pp. 90–121.

[109] Fareed Zakaria. “Realism and Domestic Politics: A Review Essay”. In: *International Security* 17.1 (1992), pp. 177–198.

[110] Anthony Y. Ku et al. "Grand challenges in anticipating and responding to critical materials supply risks". In: *Joule* 8.5 (2024), pp. 1208–1223. ISSN: 2542-4351. DOI: https://doi.org/10.1016/j.joule.2024.03.001. URL: https://www.sciencedirect.com/science/article/pii/S2542435124001120.

[111] Weihuan Zhou, Victor Crochet, and Haoxue Wang. *Demystifying China's Critical Minerals Strategies: Rethinking 'De-risking' Supply Chains*. UNSW Law Research Paper No. 23-23. UNSW, Sept. 2023. DOI: 10.2139/ssrn.4578882. URL: https://ssrn.com/abstract=4578882.

[112] Victor Crochet and Weihuan Zhou. "Critical insecurities? The European Union's strategy for a stable supply of minerals". In: *Journal of International Economic Law* 27.1 (Feb. 2024), pp. 147–165. ISSN: 1369-3034. DOI: 10.1093/jiel/jgae003. eprint: https://academic.oup.com/jiel/article-pdf/27/1/147/56971740/jgae003.pdf. URL: https://doi.org/10.1093/jiel/jgae003.

[113] Amrish Ritoe. *The U.S. Defense Production Act: Why America needs to do more if it wants to secure a steady supply of critical minerals*. Tech. rep. 2022. URL: http://www.jstor.org/stable/resrep40387 (visited on 10/19/2023).

[114] Roderick G. Eggert. "Critical Minerals and Emerging Technologies". In: *Issues in Science and Technology* 26.4 (2010), pp. 49–58. ISSN: 07485492, 19381557. URL: http://www.jstor.org/stable/43315186 (visited on 10/19/2023).

[115] Walter Leal Filho et al. "Understanding Rare Earth Elements as Critical Raw Materials". In: *Sustainability* 15.3 (2023). ISSN: 2071-1050. DOI: 10.3390/su15031919. URL: https://www.mdpi.com/2071-1050/15/3/1919.

[116] Georgios Charalampides et al. "Rare Earth Elements: Industrial Applications and Economic Dependency of Europe". In: *Procedia Economics and Finance* 24 (2015). International Conference on Applied Economics (ICOAE) 2015, 2-4 July 2015, Kazan, Russia, pp. 126–135. ISSN: 2212-5671. DOI: https://doi.org/10.1016/S2212-5671(15)00630-9. URL: https://www.sciencedirect.com/science/article/pii/S2212567115006309.

[117] European Commission et al. *Study on the critical raw materials for the EU 2023 – Final report*. Publications Office of the European Union, 2023. DOI: doi/10.2873/725585.

[118] U.S. Department of the Interior, U.S Geological Survey. "Mineral commodity summaries 2023". English. In: Mineral Commodity Summaries (2023). Report, p. 210. DOI: 10.3133/mcs2023. URL: https://doi.org/10.3133/mcs2023.

[119] U.S. Department of Energy. *Critical Materials Assessment*. Tech. rep. Draft Report. U.S. Department of Energy, May 2023. URL: https://www.energy.gov/sites/default/files/2023-05/2023-critical-materials-assessment.pdf.

[120] Office of The Deputy Secretary of Defense. *Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden's Executive Order 14017*. Tech. rep. U.S. Department of Defense. URL: https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

[121] Congressional Research Service. *U.S.-Japan Critical Minerals Agreement*. Tech. rep. Updated May 20, 2024. Congressional Research Service, May 2024. URL: https://crsreports.congress.gov/product/pdf/IF/IF12517.

[122] Patrik Andersson. "Chinese assessments of "critical" and "strategic" raw materials: Concepts, categories, policies, and implications". In: *The Extractive Industries and Society* 7.1 (2020), pp. 127–137. ISSN: 2214-790X. DOI: https://doi.org/10.1016/j.exis.2020.01.008. URL: https://www.sciencedirect.com/science/article/pii/S2214790X19303454.

[123] Daisuke Sasatani. *Japan Publishes Draft 6th Strategic Energy Plan*. Voluntary Report - Voluntary - Public Distribution. Report Number: JA2021-0113. Tokyo, Japan, Aug. 2021. URL: https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=Japan%5C%20Publishes%5C%20Draft%5C%206th%5C%20Strategic%5C%20Energy%5C%20Plan_Tokyo_Japan_08-05-2021.pdf.

[124] Marcus Schulmerich. "The Efficient Frontier in Modern Portfolio Theory - Weaknesses and How to Overcome Them". In: *The Efficient Frontier in Modern Portfolio Theory Weaknesses and How to Overcome Them* (2013). URL: https://investmentsandwealth.org/getattachment/8ac04ae1-%20e30d-4c52-9015-c58b105e652c/IWM13JulAug-EfficientFrontierMPT.pdf.

[125] Yuchuan Chen. "Establishing a reserve system of strategic mineral resources in China". In: *Land Resources* 1 (2002), pp. 20–21.

[126] Yabin Qi. "Research on China's mineral resources reserve". In: *Korean Hum. Resour. Dev. Strategy Inst.* 6 (2002), pp. 53–54.

[127] Xin'an Zhang. "History and current status of foreign mineral resource reserves". In: *Land Resour. Inf.* 1 (2002), pp. 1–12.

[128] Ruijiang Wang. “Thoughts on Several Issues of Current Strategic Mineral Exploration Work in China”. In: *Geological Bulletin of China* 11 (2004), pp. 1074–1077.

[129] Anne-Marie Brady. *China as a polar great power*. Cambridge University Press, 2017.

[130] European Commission. “Communication from the Commission to the European Parliament and the Council”. In: *Official Journal C* 248 (2011). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008DC0699.

[131] Elizabeth Economy and Michael Levi. *By All Means Necessary: How China’s Resource Quest is Changing the World*. OUP Catalogue 9780199921782. Oxford University Press, Dec. 2014. ISBN: ARRAY(0x5b7f44d8). URL: https://ideas.repec.org/b/oxp/obooks/9780199921782.html.

[132] Foreign Policy Analytics. “Mining the Future: How China is set to dominate the next Industrial Revolution”. In: *Foreign Policy Magazine* (2019). URL: https://foreignpolicy.com/2019/05/01/mining-the-future-china-critical-minerals-metals/.

[133] Eva Bartekova and Rene Kemp. *Critical raw material strategies in different world regions*. MERIT Working Papers 2016-005. United Nations University - Maastricht Economic, Social Research Institute on Innovation, and Technology (MERIT), Jan. 2016. URL: https://ideas.repec.org/p/unm/unumer/2016005.html.

[134] Brahma Chellaney. *China’s Creditor Imperialism*. Dec. 2017. URL: https://www.project-syndicate.org/commentary/china-sri-lanka-hambantota-port-debt-by-brahma-chellaney-2017-12.

[135] Michal Himmer and Zdeněk Rod. “Chinese debt trap diplomacy: reality or myth?” In: *Journal of the Indian Ocean Region* 18.3 (2022), pp. 250–272. DOI: 10.1080/19480881.2023.2195280. eprint: https://doi.org/10.1080/19480881.2023.2195280. URL: https://doi.org/10.1080/19480881.2023.2195280.

[136] Anna Gelpern et al. “How China lends: A rare look into 100 debt contracts with foreign governments”. In: *Economic Policy* 21.7 (Nov. 2022). DOI: 10.1093/epolic/eiac054. URL: https://www.cgdev.org/publication/how-china-lends-rare-look-into-100-debt-contracts-foreign-governments.

[137] Wanjing Kelly Chen. “Sovereign Debt in the Making: Financial Entanglements and Labor Politics along the Belt and Road in Laos”. In: *Economic Geography* 96.4 (2020), pp. 295–314. DOI: 10.1080/00130095.2020.1810011. eprint: https://doi.org/10.1080/00130095.2020.1810011. URL: https://doi.org/10.1080/00130095.2020.1810011.

[138] Deborah Brautigam and Meg Rithmire. *The Chinese 'Debt Trap' Is a Myth*. Feb. 2021. URL: https://www.theatlantic.com/international/archive/2021/02/china-debt-trap-diplomacy/617953/?fbclid=IwAR2iNDXVyicLyEO3ma8fura5wdwcFysNvKxfD8NC7rpu9y6pcPWpfWB1GoI.

[139] Ajit Singh. "The myth of 'debt-trap diplomacy' and realities of Chinese development finance". In: *Third World Quarterly* 42.2 (2021), pp. 239–253. DOI: 10.1080/01436597.2020.1807318. eprint: https://doi.org/10.1080/01436597.2020.1807318. URL: https://doi.org/10.1080/01436597.2020.1807318.

[140] Dale C. Copeland. "Economic Interdependence and War: A Theory of Trade Expectations". In: *International Security* 20.4 (1996), pp. 5–41. ISSN: 01622889, 15314804. URL: http://www.jstor.org/stable/2539041 (visited on 06/12/2024).

[141] Andrew Glencross. "The geopolitics of supply chains: EU efforts to ensure security of supply". In: *Global Policy* (2024). hal-04571547. DOI: 10.1111/1758-5899.13388. URL: https://hal.science/hal-04571547/document.

[142] Henry Farrell and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion". In: *International Security* 44.1 (July 2019), pp. 42–79. ISSN: 0162-2889. DOI: 10.1162/isec_a_00351. eprint: https://direct.mit.edu/isec/article-pdf/44/1/42/2059077/isec_a_00351.pdf. URL: https://doi.org/10.1162/isec%5C_a%5C_00351.

[143] J.M. Klinger. "On the rare earth frontier". PhD dissertation. University of California, Berkeley, 2015. URL: https://escholarship.org/content/qt3cr045fs/qt3cr045fs.pdf.

[144] Z. Yang. "China just fought back in the semiconductor war. Here's what you need to know". In: *MIT Technology Review* (2023). [online]. URL: https://www.technologyreview.com/2023/07/10/1076025/china-export-control-semiconductor-material/.

[145] Financial Times. "China imposes export curbs on graphite". In: *Financial Times* (Oct. 2023). [online]. URL: https://www.ft.com/content/8af8c05c-8e54-40e9-9051-5a0b2b036c32.

[146] P. Kowalski and C. Legendre. *Raw materials critical for the green transition: production, international trade, and export restrictions*. OECD Trade Policy Paper. [online]. OECD, 2023. URL: https://www.oecd-ilibrary.org/docserver/c6bb598b-en.pdf?expires=1682342145%5C&id=id%5C&accname=guest%5C&checksum=FF3DF96C96C0E2CC3520E09AEF98090F.

[147] Jeffrey Ding and Allan Dafoe. “The Logic of Strategic Assets: From Oil to AI”. In: *Security Studies* 30.2 (2021), pp. 182–212. DOI: 10.1080/09636412.2021.1915583. eprint: https://doi.org/10.1080/09636412.2021.1915583. URL: https://doi.org/10.1080/09636412.2021.1915583.

[148] Jose M. Yusta, Gabriel J. Correa, and Roberto Lacal-Arántegui. “Methodologies and applications for critical infrastructure protection: State-of-the-art”. In: *Energy Policy* 39.10 (2011). Sustainability of biofuels, pp. 6100–6119. ISSN: 0301-4215. DOI: https://doi.org/10.1016/j.enpol.2011.07.010. URL: https://www.sciencedirect.com/science/article/pii/S0301421511005337.

[149] Fabio De Felice, Ilaria Baffo, and Antonella Petrillo. “Critical Infrastructures Overview: Past, Present and Future”. In: *Sustainability* 14.4 (2022). ISSN: 2071-1050. DOI: 10.3390/su14042233. URL: https://www.mdpi.com/2071-1050/14/4/2233.

[150] GD Bona et al. “Systematic human reliability analysis (SHRA): a new approach to evaluate human error probability (HEP) in a nuclear plant”. In: *International Journal of mathematical, engineering and management sciences* 6.1 (2021), pp. 345–362.

[151] Abdul Haseeb Khan Babar and Yousaf Ali. “Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point”. In: *Technology in Society* 68 (2022), p. 101809.

[152] European Parliament and the Council. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. Bulgarian, Spanish, Czech, Danish, German, Estonian, Greek, English, French, Irish, Croatian, Italian, Latvian, Lithuanian, Hungarian, Maltese, Dutch, Polish, Portuguese, Romanian, Slovak, Slovenian, Finnish, Swedish. Official Journal of the European Union. Text with EEA relevance. Dec. 27, 2022. URL: http://data.europa.eu/eli/dir/2022/2557/oj.

[153] SPEAR Project. *A Review of Critical Infrastructure Domains in Europe*. Retrieved 15 December 2023. 2021. URL: https://www.spear2020.eu/News/Details?id=120.

[154] Simon M. Jowitt. “COVID-19 and the Global Mining Industry”. In: *SEG Discovery* 122 (July 2020), pp. 33–41. ISSN: 1550-297X. DOI: 10.5382/SEGnews.2020-122.fea-02. eprint: https://pubs.geoscienceworld.org/segweb/segdiscovery/article-pdf/doi/10.5382/SEGnews.2020-122.fea-02/5098092/segn-122-3.pdf. URL: https://doi.org/10.5382/SEGnews.2020-122.fea-02.

[155] Qingqing Xu et al. "Volatility in metallic resources prices in COVID-19 and financial Crises-2008: Evidence from global market". In: *Resources Policy* 78 (2022), p. 102927. ISSN: 0301-4207. DOI: https://doi.org/10.1016/j.resourpol.2022.102927. URL: https://www.sciencedirect.com/science/article/pii/S0301420722003713.

[156] John Naughton. "The evolution of the Internet: from military experiment to General Purpose Technology". In: *Journal of Cyber Policy* 1.1 (2016), pp. 5–28. DOI: 10.1080/23738871.2016.1157619. eprint: https://doi.org/10.1080/23738871.2016.1157619. URL: https://doi.org/10.1080/23738871.2016.1157619.

[157] European Union Commission. *EU-NATO Task Force on the Resilience of Critical Infrastructure Final Assessment Report*. Tech. rep. Accessed online. European Union Commission, June 2023. URL: https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%5C%20Assessment%5C%20Report%5C%20Digital.pdf.

[158] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. *Identifying Critical Infrastructure During COVID-19*. Originally posted on March 19, 2024, and updated on August 13, 2024; Accessed online. Aug. 2024. URL: https://www.cisa.gov/topics/risk-management/coronavirus/identifying-critical-infrastructure-during-covid-19.

[159] The White House, Office of the Press Secretary. *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. Presidential Policy Directive/PPD-21. Accessed online. Feb. 2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[160] Shirley Gregor and Alan Hevner. "Positioning and Presenting Design Science Research for Maximum Impact". In: *MIS Quarterly* 37 (June 2013), pp. 337–356. DOI: 10.25300/MISQ/2013/37.2.01.

[161] Alan Hevner et al. "Design Science in Information Systems Research". In: *Management Information Systems Quarterly* 28 (Mar. 2004), pp. 75–.

[162] Paul Johannesson and Erik Perjons. "A Method Framework for Design Science Research". In: *An Introduction to Design Science*. Cham: Springer International Publishing, 2014, pp. 75–89. ISBN: 978-3-319-10632-8. DOI: 10.1007/978-3-319-10632-8_4. URL: https://doi.org/10.1007/978-3-319-10632-8_4.

[163] Karen Lund Petersen. "Risk analysis – A field within security studies?" In: *European Journal of International Relations* 18.4 (2012), pp. 693–717. DOI: 10.1177/1354066111409770. eprint: https://doi.org/10.1177/1354066111409770. URL: https://doi.org/10.1177/1354066111409770.

[164] Mikkel Vedby Rasmussen. *The risk society at war: terror, technology and strategy in the twenty-first century*. Cambridge University Press, 2006.

[165] Christopher Coker. *War in an Age of Risk*. John Wiley & Sons, 2013.

[166] M. J. WILLIAMS. "(In)Security Studies, Reflexive Modernization and the Risk Society". In: *Cooperation and Conflict* 43.1 (2008), pp. 57–79. ISSN: 00108367, 14603691. URL: http://www.jstor.org/stable/45084567.

[167] Jan vom Brocke, Alan Hevner, and Alexander Maedche. "Introduction to Design Science Research". In: Sept. 2020, pp. 1–13. ISBN: 978-3-030-46780-7. DOI: 10.1007/978-3-030-46781-4_1.

[168] Göran Goldkuhl. "Anchoring Scientific Abstractions—Ontological and Linguistic Determination Following Socio-Instrumental Pragmatism". In: *European Conference on Research Methods in Business and Management*. Reading, UK, 2002, pp. 29–30.

[169] Philipp C. Sauer and Stefan Seuring. "Extending the reach of multi-tier sustainable supply chain management – Insights from mineral supply chains". In: *International Journal of Production Economics* 217 (2019). Recent issues and future directions on effective multi-tier supply chain management for sustainability, pp. 31–43. ISSN: 0925-5273. DOI: https://doi.org/10.1016/j.ijpe.2018.05.030. URL: https://www.sciencedirect.com/science/article/pii/S0925527318302329.

[170] European Union Energy Agency. *Methodological description and interpretation of the volatility index for electricity markets*. Tech. rep. Oct. 2014. URL: https://energy.ec.europa.eu/system/files/2014-10/volatility_methodology_0.pdf.

[171] Faisal Shafait and Ray Smith. "Table detection in heterogeneous documents." In: *Document Analysis Systems*. Ed. by David S. Doermann et al. ACM International Conference Proceeding Series. ACM, July 7, 2010, pp. 65–72. ISBN: 978-1-60558-773-8. URL: http://dblp.uni-trier.de/db/conf/das/das2010.html#ShafaitS10.

[172] Institute for Rare Earths and Strategic Metals. *Prices*. Database. Feb. 2024. URL: https://ise-metal-quotes.com/price-logged-in.php.

[173] Michael Parkinson. “The Extreme Value Method for Estimating the Variance of the Rate of Return”. In: *The Journal of Business* 53.1 (1980), pp. 61–65. ISSN: 00219398, 15375374. URL: http://www.jstor.org/stable/2352357 (visited on 07/20/2024).

[174] International Finance Corporation. *Project finance in developing countries*. Lessons of Experience S. Washington, D.C., DC: World Bank Publications, May 1999.

[175] João Pinto. “What is Project Finance?” In: 01 (2014). URL: https://EconPapers.repec.org/RePEc:cap:wpaper:012014.

[176] Jianyue Zhang et al. “Magnesium research and applications: Past, present and future”. In: *Journal of Magnesium and Alloys* 11.11 (2023). Magnesium and Its Alloys for Better Future - JMA 10th Anniversary, pp. 3867–3895. ISSN: 2213-9567. DOI: https://doi.org/10.1016/j.jma.2023.11.007. URL: https://www.sciencedirect.com/science/article/pii/S2213956723002694.

[177] Jovan Tan and Seeram Ramakrishna. “Applications of Magnesium and Its Alloys: A Review”. In: *Applied Sciences* 11.15 (2021). ISSN: 2076-3417. DOI: 10.3390/app11156861. URL: https://www.mdpi.com/2076-3417/11/15/6861.

[178] MA Shand. “History of magnesia”. In: *The chemistry and technology of magnesia. John Wiley & Sons, Inc., Hoboken, NJ, USA* (2006), pp. 1–4.

[179] Leszek A Dobrzański, George E Totten, and Menachem Bamberger. “The importance of magnesium and its alloys in modern technology and methods of shaping their structure and properties”. In: *Magnesium and its alloys*. CRC Press, 2019, pp. 1–28.

[180] Deborah A. Kramer. *Magnesium, its Alloys and Compounds*. Open-File Report 01-341. U.S. Geological Survey, 2001. URL: https://pubs.usgs.gov/of/2001/of01-341/of01-341.pdf.

[181] *Magnesium Metal - Mineral Commodity Summaries*. Tech. rep. U.S. Geological Survey, Jan. 2024. URL: https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-magnesium-metal.pdf.

[182] S. Carrara et al. *Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU - A foresight study*. Tech. rep. EUR 31437 EN. JRC Science for Policy Report, 2023. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC31437.

[183] B.L Mordike and T Ebert. “Magnesium: Properties — applications — potential”. In: *Materials Science and Engineering: A* 302.1 (2001), pp. 37–45. ISSN: 0921-5093. DOI: https://doi.

org/10.1016/S0921-5093(00)01351-4. URL: https://www.sciencedirect.com/science/article/pii/S0921509300013514.

[184] Charles Moosbrugger. *Engineering properties of magnesium alloys*. ASM International, 2017.

[185] Mustafa Kemal Kulekci. “Magnesium and its alloys applications in automotive industry”. In: *The International Journal of Advanced Manufacturing Technology* 39.9 (Nov. 2008), pp. 851–865. ISSN: 1433-3015. DOI: 10.1007/s00170-007-1279-2. URL: https://doi.org/10.1007/s00170-007-1279-2.

[186] H. Hornberger, S. Virtanen, and A.R. Boccaccini. “Biomedical coatings on magnesium alloys – A review”. In: *Acta Biomaterialia* 8.7 (2012), pp. 2442–2455. ISSN: 1742-7061. DOI: https://doi.org/10.1016/j.actbio.2012.04.012. URL: https://www.sciencedirect.com/science/article/pii/S1742706112001596.

[187] Tao Wu and Kemin Zhang. “Corrosion and Protection of Magnesium Alloys: Recent Advances and Future Perspectives”. In: *Coatings* 13.9 (2023). ISSN: 2079-6412. DOI: 10.3390/coatings13091533. URL: https://www.mdpi.com/2079-6412/13/9/1533.

[188] B. Mordike and T. Ebert. “Magnesium properties - Applications - Potential”. In: *Materials Science and Engineering: A* 302 (Apr. 2001). DOI: 10.1016/S0921-5093(00)01351-4.

[189] Kotaro Nakamura et al. “Titanium Sponge Production Method by Kroll Process at OTC”. In: *MATERIALS TRANSACTIONS* 58.3 (2017), pp. 319–321. DOI: 10.2320/matertrans.MK201634.

[190] Dietmar Seyferth. “The Grignard Reagents”. In: *Organometallics* 28.6 (Mar. 2009), pp. 1598–1605. ISSN: 0276-7333. DOI: 10.1021/om900088z. URL: https://doi.org/10.1021/om900088z.

[191] Raphael Mathias Peltzer et al. “The Grignard Reaction – Unraveling a Chemical Puzzle”. In: *Journal of the American Chemical Society* 142.6 (Feb. 2020), pp. 2984–2994. ISSN: 0002-7863. DOI: 10.1021/jacs.9b11829. URL: https://doi.org/10.1021/jacs.9b11829.

[192] K. Peter C. Vollhardt and Neil E. Schore. *Organic chemistry : structure and function*. English. Seventh edition. New York, NY: W.H. Freeman and Company, 2014. ISBN: 1464120277; 9781464120275.

[193] Graham Hayes et al. “Polymers without Petrochemicals: Sustainable Routes to Conventional Monomers”. In: *Chemical Reviews* 123.5 (Mar. 2023), pp. 2609–2734. ISSN: 0009-2665. DOI: 10.1021/acs.chemrev.2c00354. URL: https://doi.org/10.1021/acs.chemrev.2c00354.

[194] Masayuki UMENO and Mitsuo HAMADA. "Applications of the Grignard Reaction." In: *Journal of Synthetic Organic Chemistry, Japan* 38.12 (1980), pp. 1196–1209. DOI: 10.5059/yukigoseikyokaishi.38.1196.

[195] Tadashi Banno, Yoshiki Hayakawa, and Masayuki Umeno. "Some applications of the Grignard cross-coupling reaction in the industrial field". In: *Journal of Organometallic Chemistry* 653.1 (2002), pp. 288–291. ISSN: 0022-328X. DOI: https://doi.org/10.1016/S0022-328X(02)01165-8. URL: https://www.sciencedirect.com/science/article/pii/S0022328X02011658.

[196] Anil Kumar, Santosh Kumar, and N.K. Mukhopadhyay. "Introduction to magnesium alloy processing technology and development of low-cost stir casting process for magnesium alloy and its composites". In: *Journal of Magnesium and Alloys* 6.3 (2018), pp. 245–254. ISSN: 2213-9567. DOI: https://doi.org/10.1016/j.jma.2018.05.006. URL: https://www.sciencedirect.com/science/article/pii/S2213956718300331.

[197] Rakeshkumar Karunakaran et al. "Additive manufacturing of magnesium alloys". In: *Bioactive Materials* 5.1 (2020), pp. 44–54. ISSN: 2452-199X. DOI: https://doi.org/10.1016/j.bioactmat.2019.12.004. URL: https://www.sciencedirect.com/science/article/pii/S2452199X19300726.

[198] Jian-Feng Nie. "Precipitation and Hardening in Magnesium Alloys". In: *Metallurgical and Materials Transactions A* 43.11 (Nov. 2012), pp. 3891–3939. ISSN: 1543-1940. DOI: 10.1007/s11661-012-1217-2. URL: https://doi.org/10.1007/s11661-012-1217-2.

[199] Sihang You et al. "Recent research and developments on wrought magnesium alloys". In: *Journal of Magnesium and Alloys* 5.3 (2017), pp. 239–253. ISSN: 2213-9567. DOI: https://doi.org/10.1016/j.jma.2017.09.001. URL: https://www.sciencedirect.com/science/article/pii/S2213956717300464.

[200] Karl U Kainer. *Magnesium alloys and technology*. John Wiley & Sons, 2003.

[201] Engineering Product Design. "What is Sand casting? How does it work? Pros & Cons casting". In: *EngineeringProductDesign.com* (2023). URL: https://engineeringproductdesign.com/knowledge-base/what-is-sand-casting/.

[202] Shambhu Kumar Manjhi et al. "Additive manufacturing of magnesium alloys: Characterization and post-processing". In: *International Journal of Lightweight Materials and Manufacture* 7.1 (2024), pp. 184–213. ISSN: 2588-8404. DOI: https://doi.org/10.1016/j.ijlmm.

2023.06.004. URL: https://www.sciencedirect.com/science/article/pii/S2588840423000379.

[203] P. Durai Murugan et al. “A current state of metal additive manufacturing methods: A review”. In: *Materials Today: Proceedings* 59 (2022). International Conference Virtual Conference on Technological Advancements in Mechanical Engineering, pp. 1277–1283. ISSN: 2214-7853. DOI: https://doi.org/10.1016/j.matpr.2021.11.503. URL: https://www.sciencedirect.com/science/article/pii/S2214785321075258.

[204] T. T. T. Trang et al. “Designing a magnesium alloy with high strength and high formability”. In: *Nature Communications* 9.1 (June 2018), p. 2522. ISSN: 2041-1723. DOI: 10.1038/s41467-018-04981-4. URL: https://doi.org/10.1038/s41467-018-04981-4.

[205] Anna Dziubińska et al. “The Microstructure and Mechanical Properties of AZ31 Magnesium Alloy Aircraft Brackets Produced by a New Forging Technology”. In: *Procedia Manufacturing* 2 (2015). 2nd International Materials, Industrial, and Manufacturing Engineering Conference, MIMEC2015, 4-6 February 2015, Bali, Indonesia, pp. 337–341. ISSN: 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2015.07.059. URL: https://www.sciencedirect.com/science/article/pii/S2351978915000608.

[206] Trevor Abbott. “Casting technologies, microstructure and properties”. In: *Magnesium and its alloys*. CRC Press, 2019, pp. 29–45.

[207] Hidetoshi Somekawa. “Effect of Alloying Elements on Fracture Toughness and Ductility in Magnesium Binary Alloys; A Review”. In: *MATERIALS TRANSACTIONS* 61.1 (2020), pp. 1–13. DOI: 10.2320/matertrans.MT-M2019185.

[208] S Fujisawa and A Yonezu. “Mechanical property of microstructure in die-cast magnesium alloy evaluated by indentation testing at elevated temperature”. In: *Recent Advances in Structural Integrity Analysis—Proceedings of the International Congress (Apcf/Sif-2014)*. 2014, pp. 422–426.

[209] Avinash Srinivas et al. “Study on mechanical properties of AZ91 magnesium alloy”. In: *Materials Today: Proceedings* 54 (2022). 5th International Conference on Advanced Research in Mechanical, Materials and Manufacturing Engineering-2021, pp. 291–294. ISSN: 2214-7853. DOI: https://doi.org/10.1016/j.matpr.2021.09.171. URL: https://www.sciencedirect.com/science/article/pii/S221478532105968X.

[210] Yoshihito Kawamura et al. “Rapidly Solidified Powder Metallurgy $Mg_{97}Zn_1Y_2$ Alloys with Excellent Tensile Yield Strength above 600 MPa”. In: *MATERIALS TRANSACTIONS* 42.7 (2001), pp. 1172–1176. DOI: 10.2320/matertrans.42.1172.

[211] Sameer Kumar Devarakonda. “Magnesium and Its Alloys in Automotive Applications – A Review”. In: *American Journal of Materials Science and Technology* 4 (Jan. 2015), pp. 12–30. DOI: 10.7726/ajmst.2015.1002.

[212] L. L. Rokhlin. “Advanced Magnesium Alloys with Rare-Earth Metal Additions”. In: *Advanced Light Alloys and Composites*. Ed. by R. Ciach. Dordrecht: Springer Netherlands, 1998, pp. 443–448. ISBN: 978-94-015-9068-6. DOI: 10.1007/978-94-015-9068-6_58. URL: https://doi.org/10.1007/978-94-015-9068-6_58.

[213] N. Hort, Y. Huang, and K.U. Kainer. “Intermetallics in Magnesium Alloys”. In: *Advanced Engineering Materials* 8.4 (2006), pp. 235–240. DOI: https://doi.org/10.1002/adem.200500202. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/adem.200500202. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/adem.200500202.

[214] Qiang Yang et al. “ZK60 based alloys with high-strength and high-ductility: A review”. In: *Resources Chemicals and Materials* 2.2 (2023), pp. 151–166. ISSN: 2772-4433. DOI: https://doi.org/10.1016/j.recm.2023.03.002. URL: https://www.sciencedirect.com/science/article/pii/S2772443323000144.

[215] Meenakshi. “Effect of Epsom Salt Concentration and Dry-Mix Composition on Bonding Properties of Magnesium Oxysulfate”. In: *Asian Journal of Chemistry* 35.4 (Aug. 2023), pp. 869–876. DOI: 10.14233/ajchem.2023.26992. URL: https://asianpubs.org/index.php/ajchem/article/view/35_4_10.

[216] Yongshan Tan et al. “Review of reactive magnesia-based cementitious materials: Current developments and potential applicability”. In: *Journal of Building Engineering* 40 (2021), p. 102342. ISSN: 2352-7102. DOI: https://doi.org/10.1016/j.jobe.2021.102342. URL: https://www.sciencedirect.com/science/article/pii/S2352710221001984.

[217] Radoslaw Poglodzinski, Przemyslaw Barlog, and Witold Grzebisz. “Effect of nitrogen and magnesium sulfate application on sugar beet yield and quality”. In: *Plant, Soil and Environment* 67.9 (2021), pp. 507–513. ISSN: 12141178. DOI: 10.17221/336/2021-PSE. URL: https://pse.agriculturejournals.cz/artkey/pse-202109-0003.php.

[218] Mehmet Senbayram et al. “Role of magnesium fertilisers in agriculture: plant–soil continuum”. In: *Crop and Pasture Science* 66.12 (2015), pp. 1219–1229. DOI: 10.1071/CP15104. URL: https://doi.org/10.1071/CP15104.

[219] A. Chakraborty. “Bathing Practices in Dermatology: Uses and Implications for Patient Management”. In: *Indian Dermatology Online Journal* 14.5 (2023), pp. 686–691. DOI: 10.4103/idoj.idoj_40_23. URL: https://doi.org/10.4103/idoj.idoj_40_23.

[220] Abdullah M. Al Alawi et al. “Chapter Six - Magnesium: The recent research and developments”. In: *The Latest Research and Development of Minerals in Human Nutrition*. Ed. by N.A. Michael Eskin. Vol. 96. Advances in Food and Nutrition Research. Academic Press, 2021, pp. 193–218. DOI: https://doi.org/10.1016/bs.afnr.2021.01.001. URL: https://www.sciencedirect.com/science/article/pii/S1043452621000012.

[221] Yessica González et al. “Hydrometallurgical processing of magnesium minerals – A review”. In: *Hydrometallurgy* 201 (2021), p. 105573. ISSN: 0304-386X. DOI: https://doi.org/10.1016/j.hydromet.2021.105573. URL: https://www.sciencedirect.com/science/article/pii/S0304386X21000220.

[222] George Simandl et al. “Magnesium - Raw Materials, Metal Extraction and Economics - Global Picture”. In: Jan. 2007. URL: https://cmscontent.nrs.gov.bc.ca/geoscience/publicationcatalogue/External/EXT096.pdf.

[223] Winny Wulandari, Geoffrey Brooks, and M Akbar Rhamdhani. “Magnesium: current and alternative production routes”. In: Aug. 2010.

[224] A. Mayer. “Plant for Production of Magnesium by the Ferrosilicon Process”. In: *Trans. AIME* 159 (1944), pp. 363–376.

[225] Alan A. Luo. “Magnesium casting technology for structural applications”. In: *Journal of Magnesium and Alloys* 1.1 (2013), pp. 2–22. ISSN: 2213-9567. DOI: https://doi.org/10.1016/j.jma.2013.02.002. URL: https://www.sciencedirect.com/science/article/pii/S2213956713000030.

[226] Vincent Vlies. “Hazardous Materials Transport”. In: *International Encyclopedia of Transportation* (May 2021), pp. 304–310. DOI: 10.1016/b978-0-08-102671-7.10143-5.

[227] Maersk. *Free on Board (FOB) Incoterms® explained*. Aug. 2023. URL: https://www.maersk.com/logistics-explained/customs-and-compliance/2023/10/05/free-on-board-shipping.

[228] AIT Worldwide Logistics. *Incoterms EXW: Ex Works*. 2023. URL: https://www.aitworldwide.com/resources/incoterms/incoterms-exw-ex-works/.

[229] European Commission. *Glossary term: Ex works price*. 2023. URL: https://trade.ec.europa.eu/access-to-markets/en/glossary/ex-works-price.

[230] Jenny Zhang. *Understanding China's 2021 Power Crunch - The Causes of a Crisis*. Mar. 2022. URL: https://www.amcham-shanghai.org/en/article/understanding-chinas-2021-power-crunch.

[231] Keith Bradsher. *China's Power Problems Expose a Strategic Weakness*. Oct. 2021. URL: https://www.nytimes.com/2021/10/13/business/china-electricity-shortage.html.

[232] Julia E. Sullivan and Dmitriy Kamensky. "Putin's power play: Russia's attacks on Ukraine's electric power infrastructure violate international law". In: *The Electricity Journal* 37.2 (2024), p. 107371. ISSN: 1040-6190. DOI: https://doi.org/10.1016/j.tej.2024.107371. URL: https://www.sciencedirect.com/science/article/pii/S104061902400006X.

[233] Zheng Wan et al. "Analysis of the impact of Suez Canal blockage on the global shipping network". In: *Ocean & Coastal Management* 245 (2023), p. 106868. ISSN: 0964-5691. DOI: https://doi.org/10.1016/j.ocecoaman.2023.106868. URL: https://www.sciencedirect.com/science/article/pii/S0964569123003939.

[234] Kornwika POONNAWATT. "Multilateral cooperation against maritime piracy in the Straits of Malacca: From the RMSI to ReCAAP". In: *Marine Policy* 152 (2023), p. 105628. ISSN: 0308-597X. DOI: https://doi.org/10.1016/j.marpol.2023.105628. URL: https://www.sciencedirect.com/science/article/pii/S0308597X23001550.

[235] Zhaoyang He et al. "Assessment of global shipping risk caused by maritime piracy". In: *Heliyon* 9.10 (2023), e20988. ISSN: 2405-8440. DOI: https://doi.org/10.1016/j.heliyon.2023.e20988. URL: https://www.sciencedirect.com/science/article/pii/S2405844023081963.

[236] Nur Jale Ece. "A Threat to Maritime Trade: Analysis of Piracy Attacks Between 2015 and 2022 and the Period of COVID-19". In: *JEMS Maritime Sci* 12.1 (2024). doi: 10.4274/jems.2023.00377, pp. 50–63. DOI: 10.4274/jems.2023.00377. eprint: https://dx.doi.org/10.4274/jems.2023.00377. URL: https://dx.doi.org/10.4274/jems.2023.00377.

[237] Gregory Brew. *The Costs the Houthis Are Poised to Inflict on the Global Economy*. Dec. 2023. URL: https://time.com/6548968/houthi-rebels-shipping-attacks-red-sea-disrupt-global-economy-costs/.

[238] Reuters. "https://www.reuters.com/world/middle-east/shipping-firms-avoid-red-sea-houthi-attacks-increase-2023-12-18/". In: *Reuters* (Jan. 2024). URL: https://www.reuters.

com/world/bab-al-mandab-shipping-lane-target-israel-fights-hamas-2023-12-12/.

[239] Ahmad Ghaddar. "Houthi attacks in the Bab al-Mandab Strait hit global trade". In: *Reuters* (Dec. 2023). URL: https://www.reuters.com/world/bab-al-mandab-shipping-lane-target-israel-fights-hamas-2023-12-12/.

[240] S&P Global Inc. "Red Sea shipping attacks raise tanker insurance costs as security risks escalate". In: (Dec. 2023). URL: https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/120623-red-sea-shipping-attacks-raise-tanker-insurance-costs-as-security-risks-escalate.

[241] Chengpeng Wan et al. "Analysis of risk factors influencing the safety of maritime container supply chains". In: *International Journal of Shipping and Transport Logistics* 11.6 (2019), pp. 476–507.

[242] Georgina Mccartney and Arathy Somasekhar. "Oil tankers continue Red Sea movements despite Houthi attacks". In: *Reuters* (Jan. 2024). URL: https://www.reuters.com/markets/commodities/oil-tankers-continue-red-sea-movements-despite-houthi-attacks-2024-01-09/.

[243] Hoon Lee, David Lektzian, and Glen Biglaiser. "The Effects of Economic Sanctions on Foreign Asset Expropriation". In: *Journal of Conflict Resolution* 67.2-3 (2023), pp. 266–296. DOI: 10.1177/00220027221118250. eprint: https://doi.org/10.1177/00220027221118250. URL: https://doi.org/10.1177/00220027221118250.

[244] Jean-Pierre Dupuis. "Privatisation and Nationalisation". In: (Oct. 2005). Paper presented at the fourth meeting of the Task Force on Harmonization of Public Sector Accounting (TFHPSA), hosted by the International Monetary Fund. URL: https://www.imf.org/external/np/sta/tfhpsa/2005/09/pandn.pdf.

[245] Muhammad Asif, Rajiv Padhye, and Prem Chhetri. "Do Political Disruptions Affect Supply Chain Performance? A Qualitative Case Study of the Textile Supply Chain in Pakistan". In: *Journal of International Logistics and Trade* 17 (Sept. 2019), pp. 77–88. DOI: 10.24006/jilt.2019.17.3.002.

[246] Xianhang Qian and Shanyun Qiu. "Political risk and corporate international supply chain". In: *Journal of International Money and Finance* 137 (2023), p. 102899. ISSN: 0261-5606. DOI: https://doi.org/10.1016/j.jimonfin.2023.102899. URL: https://www.sciencedirect.com/science/article/pii/S0261560623001006.

[247] Doreen Mukunde. "Navigating Uncertainty: Strategies to Mitigate Geopolitical Risks in Global Supply Chains". In: *SSRN Electronic Journal* (Jan. 2024). DOI: 10.2139/ssrn.4683958.

[248] Lukasz Bednarski et al. "Geopolitical disruptions in global supply chains: A state-of-the-art literature review". In: *Production Planning & Control* (Nov. 2023). DOI: 10.1080/09537287.2023.2286283.

[249] European Banking Association. *Market, counterparty and CVA risk*. Accessed: 2024-07-22. n.d. URL: %5Curl%7Bhttps://www.eba.europa.eu/regulation-and-policy/market-counterparty-and-cva-risk%7D.

[250] European Parliament and Council of the European Union. "REGULATION (EU) 2019/876 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposures to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012". In: *Official Journal of the European Union* (July 2019). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0876.

[251] L. Avelar-Sosa, J.L. García-Alcaraz, and J.P. Castrellón-Torres. "The Effects of Some Risk Factors in the Supply Chains Performance: A Case of Study". In: *Journal of Applied Research and Technology* 12.5 (2014), pp. 958–968. ISSN: 1665-6423. DOI: https://doi.org/10.1016/S1665-6423(14)70602-9. URL: https://www.sciencedirect.com/science/article/pii/S1665642314706029.

[252] R. Bhatnagar and A. S. Sohal. "Supply chain competitiveness: measuring the impact of location factors, uncertainty and manufacturing practices". In: *Technovation* 25 (2005), pp. 443–456.

[253] Söhnke Bartram. "The Impact of Commodity Price Risk on Firm Value - An Empirical Analysis of Corporate Commodity Price Exposures". In: *Multinational Finance Journal* 9 (Dec. 2005). DOI: 10.17578/9-3/4-2.

[254] Chiara Banti, Kate Phylaktis, and Lucio Sarno. "Global Liquidity Risk in the Foreign Exchange Market". In: *Journal of International Money and Finance* 31 (Oct. 2011). DOI: 10.2139/ssrn.1954749.

[255] Laurent L. Jacque. "Management of Foreign Exchange Risk: A Review Article". In: *Journal of International Business Studies* 12.1 (1981), pp. 81–101. ISSN: 00472506, 14786990. URL: http://www.jstor.org/stable/154420 (visited on 07/24/2024).

[256] Andreas Nölke. *The weaponization of global payment infrastructures: A strategic dilemma.* SAFE White Paper Series 89. Leibniz Institute for Financial Research SAFE, 2022. URL: https://ideas.repec.org/p/zbw/safewh/89.html.

[257] Caileigh Glenn. "Lessons in Sanctions-Proofing from Russia". In: *The Washington Quarterly* 46.1 (2023), pp. 105–120. DOI: 10.1080/0163660X.2023.2188829. eprint: https://doi.org/10.1080/0163660X.2023.2188829. URL: https://doi.org/10.1080/0163660X.2023.2188829.

[258] Solomon Cefai, Leticia Simionato, and Julienne Raboca. *US magnesium production will be competitive without anti-dumping duties in long-run: Magrathea.* July 2024. URL: https://www.fastmarkets.com/insights/us-magnesium-production-will-be-competitive-without-anti-dumping-duties-in-long-run-magrathea/.

[259] william m. wright et al. "a conflict analysis of the suez canal invasion of 1956". In: *conflict management and peace science* 5.1 (1980), pp. 27–40. ISSN: 07388942, 15499219. URL: http://www.jstor.org/stable/26273229 (visited on 07/26/2024).

[260] R O'Rourke. "The Tanker War". In: *United States Naval Institute Proceedings* 114.5 (May 1988). Journal article, p. 1023. URL: https://www.usni.org/magazines/proceedings/1988/may/tanker-war.

[261] Silviu Nate et al. "Impact of the Russo-Ukrainian war on Black Sea trade: Geoeconomic challenges". In: *Economics & Sociology* 17 (Mar. 2024), pp. 256–279. DOI: 10.14254/2071-789X.2024/17-1/16.

[262] Lincoln F. Pratson. "Assessing impacts to maritime shipping from marine chokepoint closures". In: *Communications in Transportation Research* 3 (2023), p. 100083. ISSN: 2772-4247. DOI: https://doi.org/10.1016/j.commtr.2022.100083. URL: https://www.sciencedirect.com/science/article/pii/S2772424722000336.

[263] Reuters. "Ships rerouted by Red Sea crisis face overwhelmed African ports". In: *Reuters* (Dec. 2023). URL: https://www.reuters.com/business/ships-rerouted-by-red-sea-crisis-face-overwhelmed-african-ports-2023-12-22/.

[264] AFP. *Maersk reports massive drop in net profits, warns of uncertainty due to Houthi attacks in Red Sea.* Accessed: 2024-02-08, 10:50 am. Feb. 2024. URL: https://www.timesofisrael.com/liveblog_entry/maersk-reports-massive-drop-in-net-profits-warns-of-uncertainty-due-to-houthi-attacks-in-red-sea/.

[265] Reuters Staff. *Egypt's Suez Canal revenues down 40% due to Houthi attacks*. Jan. 2024. URL: https://www.reuters.com/markets/commodities/egypts-suez-canal-revenues-down-40-due-houthi-attacks-2024-01-11/.

[266] Dirk Kaufmann. *Rising shipping costs hit global trade hard*. July 2024. URL: https://www.dw.com/en/rising-shipping-costs-hit-global-trade-hard/a-69586965.

[267] Martin Svanberg et al. "AIS in maritime research". In: *Marine Policy* 106 (2019), p. 103520. ISSN: 0308-597X. DOI: https://doi.org/10.1016/j.marpol.2019.103520. URL: https://www.sciencedirect.com/science/article/pii/S0308597X18309667.

[268] Mihkel Kärmas. *Balticconnector case more sabotage than an accident, experts say*. Feb. 2024. URL: https://news.err.ee/1609255413/balticconnector-case-more-sabotage-than-an-accident-experts-say.

[269] Delbert Tran. "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack". In: *Yale Journal of Law and Technology* 20 (2018), p. 376. URL: https://api.semanticscholar.org/CorpusID:160019643.

[270] Thomas J. Holt et al. "Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention". In: *Criminology & Public Policy* 22.4 (2023), pp. 825–848. DOI: https://doi.org/10.1111/1745-9133.12646. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/1745-9133.12646. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12646.

[271] Kutub Thakur et al. "Impact of Cyber-Attacks on Critical Infrastructure". In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. 2016, pp. 183–186. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.22.

[272] Ana Kovacevic and Dragana Nikolic. "Cyber attacks on critical infrastructure: Review and challenges in Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance". In: Jan. 2015, pp. 1–18. ISBN: ISBN13: 9781466663244, ISBN10: 1466663243. DOI: 10.4018/978-1-4666-9619-8.ch018.

[273] Lis Piotr and Mendel Jacob. "Cyberattacks on critical infrastructure: An economic perspective". In: *Economics and Business Review* 5.2 (June 2019), pp. 24–47. DOI: 10.18559/ebr.2019.2.2. URL: https://ideas.repec.org/a/vrs/ecobur/v5y2019i2p24-47n2.html.

[274] Chalermpong Senarak. “Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases”. In: *Maritime Economics & Logistics* 26 (Dec. 2023), pp. 1–26. DOI: 10.1057/s41278-023-00276-8.

[275] Lance Y. Hunter, Craig Douglas Albert, and Eric Garrett. “Factors That Motivate State-Sponsored Cyberattacks”. In: *The Cyber Defense Review* 6.2 (2021), pp. 111–128. ISSN: 24742120, 24742139. URL: https://www.jstor.org/stable/27021379 (visited on 07/26/2024).

[276] Daniel Hughes and Andrew M. Colarik. *Predicting the Proliferation of Cyber Weapons into Small States*. Oct. 2016. URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/969646/predicting-the-proliferation-of-cyber-weapons-into-small-states/.

[277] Matteo Crosignani, Marco Macchiavelli, and André F. Silva. “Pirates without borders: The propagation of cyberattacks through firms’ supply chains”. In: *Journal of Financial Economics* 147.2 (2023), pp. 432–448. ISSN: 0304-405X. DOI: https://doi.org/10.1016/j.jfineco.2022.12.002. URL: https://www.sciencedirect.com/science/article/pii/S0304405X2200246X.

[278] Ziaul Haque Munim et al. “Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions”. In: *Maritime Policy & Management* 47.5 (2020), pp. 577–597. DOI: 10.1080/03088839.2020.1788731. eprint: https://doi.org/10.1080/03088839.2020.1788731. URL: https://doi.org/10.1080/03088839.2020.1788731.

[279] Berit Dangaard Brouer, Christian Vad Karsten, and David Pisinger. “Big data optimization in maritime logistics”. In: *Big data optimization: Recent developments and challenges* (2016), pp. 319–344.

[280] Leonard Heilig, Eduardo Lalla-Ruiz, and Stefan Voß. “Digital transformation in maritime ports: analysis and a game theoretic framework”. In: *NETNOMICS: Economic Research and Electronic Networking* 18.2 (Dec. 2017), pp. 227–254. ISSN: 1573-7071. DOI: 10.1007/s11066-017-9122-x. URL: https://doi.org/10.1007/s11066-017-9122-x.

[281] Pinakhi Suvadarshini and Pinak Dandapat. “Digitalizing the maritime supply chain: The case of Rotterdam’s port call operations”. In: *Journal of Information Technology Teaching Cases* 13.2 (2023), pp. 170–174. DOI: 10.1177/20438869221126730. eprint: https://doi.org/10.1177/20438869221126730. URL: https://doi.org/10.1177/20438869221126730.

[282] Amazon Staff. *The Maritime Port Authority of Singapore Sets Sail with Its First Artificial Intelligence and Machine Learning Hub, Built On AWS*. Apr. 2024. URL: https://www.aboutamazon.sg/news/aws/the-maritime-port-authority-of-singapore-sets-sail-with-its-first-artificial-intelligence-and-machine-learning-hub-built-on-aws.

[283] Emre Akyuz, Kadir Cicek, and Metin Celik. “A Comparative Research of Machine Learning Impact to Future of Maritime Transportation”. In: *Procedia Computer Science* 158 (2019). 3rd WORLD CONFERENCE ON TECHNOLOGY, INNOVATION AND ENTREPRENEURSHIP”INDUSTRY 4.0 FOCUSED INNOVATION, TECHNOLOGY, ENTREPRENEURSHIP AND MANUFACTURE” June 21-23, 2019, pp. 275–280. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2019.09.052. URL: https://www.sciencedirect.com/science/article/pii/S1877050919312128.

[284] Georgios Makridis, Dimosthenis Kyriazis, and Stathis Plitsos. “Predictive maintenance leveraging machine learning for time-series forecasting in the maritime industry”. In: *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*. 2020, pp. 1–8. DOI: 10.1109/ITSC45102.2020.9294450.

[285] Kalliopi Tsolaki et al. “Utilizing machine learning on freight transportation and logistics applications: A review”. In: *ICT Express* 9.3 (2023), pp. 284–295. ISSN: 2405-9595. DOI: https://doi.org/10.1016/j.icte.2022.02.001. URL: https://www.sciencedirect.com/science/article/pii/S2405959522000200.

[286] Mohamad Hasan Sweidan. *Oil, politics, and sovereignty: The Iraq-Turkiye legal dispute*. July 2023. URL: https://thecradle.co/articles-id/6339.

[287] Suat Delgen. *Pipeline v genocide: How Turkiye can legally block oil exports to Israel*. June 2024. URL: %5Curl%7Bhttps://thecradle.co/articles-id/25327%7D.

[288] Kaname Akamatsu. “THE ESSENTIALS OF DUMPING AND UNFAIR COMPETITION WITH REFERENCE TO THE JAPANESE EXPORT SITUATION”. In: *The Annals of the Hitotsubashi Academy* 5.1 (1954), pp. 22–36. ISSN: 04392841. URL: http://www.jstor.org/stable/43751444 (visited on 07/28/2024).

[289] Jacob Viner. “Dumping as a Method of Competition in International Trade. I”. In: *The University Journal of Business* 1.1 (1922), pp. 34–53. ISSN: 15256979. URL: http://www.jstor.org/stable/2354748 (visited on 07/27/2024).

[290] Sikhwari Tshivhasa Tshedza and Yende Nsizwazonke Ephraim. “An Analysis of China’s ’Dumping’ of Cheap Products in South Africa in the Perspective of Import Substitution Policy”.

In: *Journal of African Foreign Affairs* 8.1 (2021). Accessed: 2024-07-27, pp. 115–129. URL: https://www.jstor.org/stable/27159653.

[291] Minghao Li, Wendong Zhang, and Chad Hart. "What ave We Learned from China's Past Trade Retaliation Strategies?" In: *Choices* 33.2 (2018), pp. 1–8. ISSN: 08865558, 21622884. URL: http://www.jstor.org/stable/26487436 (visited on 07/28/2024).

[292] International Trade Administration. *Pure Magnesium From the People's Republic of China: Continuation of Antidumping Duty Order*. Federal Register. Document Citation: 88 FR 33862, Agency/Docket Number: A-570-832, Document Number: 2023-11146, Pages: 33862-33863 (2 pages). May 2023. URL: https://www.federalregister.gov/documents/2023/05/25/2023-11146/pure-magnesium-from-the-peoples-republic-of-china-continuation-of-antidumping-duty-order.

[293] Lindsey A. O'Rourke. "The Strategic Logic of Covert Regime Change: US-Backed Regime Change Campaigns during the Cold War". In: *Security Studies* 29.1 (2020), pp. 92–127. DOI: 10.1080/09636412.2020.1693620. eprint: https://doi.org/10.1080/09636412.2020.1693620. URL: https://doi.org/10.1080/09636412.2020.1693620.

[294] James A. Barry. *Guideposts from Just-War Theory: Managing Covert Political Action*. Tech. rep. 3. Digital Document. Center for the Study of Intelligence, 1992. URL: https://www.cia.gov/resources/csi/static/Managing-Covert-Political-Action.pdf.

[295] Stephen R. Weissman. "An Extraordinary Rendition". In: *Intelligence and National Security* 25.2 (2010), pp. 198–222. DOI: 10.1080/02684527.2010.489277. eprint: https://doi.org/10.1080/02684527.2010.489277. URL: https://doi.org/10.1080/02684527.2010.489277.

[296] Emmanuel Gerard and Bruce Kuklick. *Death in the Congo: Murdering Patrice Lumumba*. Harvard University Press, 2015. ISBN: 9780674725270. URL: http://www.jstor.org/stable/j.ctt21pxknd (visited on 11/29/2023).

[297] L. Devlin. *Chief of Station, Congo: Fighting the Cold War in a Hot Zone*. PublicAffairs, 2008. ISBN: 9780786732180. URL: https://books.google.cz/books?id=_X44DgAAQBAJ.

[298] Jean-Marie Mutamba Makombo. *Autopsie du gouvernement au Congo-Kinshasa: Le Collège des Commissaires généraux (1960-1961) contre Patrice Lumumba*. French. Editions L'Harmattan, 2015, p. 18. ISBN: 9782336392158.

[299] Stuart A. Reid. "How the U.S. Issued its First Ever Order to Assassinate a Foreign Leader". In: *POLITICO Magazine* (Oct. 2023). Accessed: 2023-11-30. URL: https://www.politico.

com/news/magazine/2023/10/17/patrice-lumumba-congo-washington-00121755.

[300] Martin Kettle. “President ’ordered murder’ of Congo leader”. In: *The Guardian* (Aug. 2000). URL: https://www.theguardian.com/world/2000/aug/10/martinkettle.

[301] K. Martial Frindethie. *From Lumumba to Gbagbo: Africa in the Eddy of the Euro-American Quest for Exceptionalism*. McFarland, 2016, p. 231.

[302] Alvin W. Wolfe. “The African Mineral Industry: Evolution of a Supranational Level of Integration”. In: *Social Problems* 11.2 (1963). Anthropology Faculty Publications. 5, pp. 153–164. DOI: 10.2307/799222. URL: https://digitalcommons.usf.edu/ant_facpub/5.

[303] P. Anderson. “Cobalt and Corruption: The Influence of Multinational Firms and Foreign States on the Democratic Republic of the Congo”. In: *Journal for Global Business and Community* 14.1 (2023). URL: https://doi.org/10.56020/001c.72664.

[304] Georges Kasay et al. “Rare Earth Element Deposits and Their Prospects in the Democratic Republic of Congo”. In: *Mining Metallurgy & Exploration* 39 (Feb. 2022), pp. 625–642. DOI: 10.1007/s42461-022-00551-x.

[305] United States Congress. *The Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Foreign and Military Intelligence*. Committee report no. 94-755. Archived from the original on June 26, 2003. Washington, D.C.: United States Congress, 1976, p. 392.

[306] Edward Alexander Gibbs. “Agency without an adversary: The CIA and covert actions in the nineteen-eighties and beyond”. PhD thesis. University of Nevada, Las Vegas, 1995. DOI: 10.25669/0qwu-4pw. URL: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1529&context=rtds.

[307] Robert Lawless. In: *Journal of Third World Studies* 21.2 (2004), pp. 282–284. ISSN: 87553449. URL: http://www.jstor.org/stable/45198510 (visited on 07/30/2024).

[308] James D. Fearon. “Rationalist Explanations for War”. In: *International Organization* 49.3 (1995), pp. 379–414. ISSN: 00208183, 15315088. URL: http://www.jstor.org/stable/2706903 (visited on 04/30/2023).

IX. Appendix - Summary

Using Design Science Research (DSR) and Systems Engineering Principles (SEP), and pursuant to the requirements of Charles University's Faculty of Social Sciences Security Studies program, in Section III, this thesis first interrogated the literature regarding the nature of risk; existing legislation and political orientation of different actors around supply-chains, critical infrastructure, and critical raw minerals (CRMs); reviewed literature regarding supply-chains themselves and relevant models; outlined the fundamental concepts behind realism, and also investigated literature regarding the strategic logics that dictate state attitudes to CRMs.

Next, the paper provided both a theoretical outline (Section IV-B) where the thesis was aligned with the Security Studies and Strategic Studies fields. An explanation and orientation of DSR was additionally provided, and a risk definition that the paper would adopt was presented. The theoretical outline would continue to define weaponized risk as,

> The increase of either specific risk, and/or aggregate risk, in a supply-chain as the result of a deliberate course of action on the part of a state power, the organs of a state, or an aligned private entity beholden and/or loyal to a state. Weaponized risk is induced directly within the supply-chain or any adjacent system of sufficient importance,

as well as the behavior of the aggressing actor, along with their objectives.

Subsequently, the methodology outlined six different steps that were to be carried out in sequential order: identification of initial mineral candidates, refinement and selection criteria for the investigated final candidate (magnesium) using price volatility measures, alignment of risk with critical infrastructure sectors, disaggregation of risks, mapping of specific risks to the magnesium supply-chain, and then identification of attack vectors.

These steps were fulfilled first in Section V, where the material properties, a picture of global supply, derivative products, supply-chain characteristics, products reliant on magnesium supply-chains, and supply-chain behaviour during the COVID-19 pandemic.

In Section VI, the framework of disaggregated risk was presented as consisting of four main classes of risk: political, market, operating, and financial risk.

Analysis identified five attack vectors in Section VII. The first vector was split into upstream, and midstream/downstream components. In the upstream portion, the paper drew upon the Pidgeon process as a frame of reference for analysis, identifying the leveraging of energy risk to reduce outputs, as well as industrial sabotage through the destruction of assets, fomenting workplace disturbances, and the use of political pressure to demand the use of greener energy sources.

The midstream and downstream portions of this attack vector emphasized the utility of an aggressive actor in halting supply-chain operations for a duration of time before the supply-chain could reorientate itself. The paper demonstrated this by examining the 1967 Suez Crisis, the Tanker War during the conflict between Iraq and Iran, the cessation of Ukrainian exports from the Black Sea, and the use of munitions by Houthi rebels to hold logistical corridors. This portion of the analysis also drew upon the potential sabotage of the Blaticconnector pipeline to illustrate how both technology risks can be utilized to sabotage midstream operations through non-compliance with best practices.

The second vector, cyberattacks, emphasized how midstream operations can suffer induced risk given an increased attack surface through greater utilization of advanced machine learning technology, itself a risk management tool.

The third vector is perhaps the most notable. It first outlines two examples where sovereign risk were utilized. First, an review of Turkish and Iraqi actions regarding Turkish dual recognition of Iraqi and Kurdish sovereignty was used to extract revenue from Kirkuk-Ceyhan despite contractual violations, and then how the halting petroleum goods despite settlement of arbitration ruling in favor of the aggrieved party lead to a massive short fall in critical revenue. The second example pertains to how Turkish stakeholders could lever the actions of their Israeli counterparties to extract themselves from contractual concessions which would otherwise mandate the uninterrupted flow of petroleum products from the Baku-Tiblisi-Ceyhan to Israeli offtakers.

From there, drawing upon the example contracts from Gelpern et al.[136], the paper showed how an attack can use binding contractual agreements to ensure that a counterpart surrenders their sovereignty in the case of default of certain loan agreements or unfavorable actions, with emphasis put on currency risks and the mandating of alternative repayment in the form of assets as a form of security against contract non-performance.

The next vector investigated was the implementation of policy and structural dumping by an actor within the supply-chain to provide magnesium at below-market prices, thereby negatively effecting the competitiveness of alternative suppliers. This is a practice that is prevalent to such an extent that the U.S. Department of Commerce and U.S International Trade Commission stated in a note[292] that without antidumping duties against Chinese magnesium suppliers, there would be a "...continuation or recurrece of dumping practices and material injury to industry in the United States."

Given the reliance of European critical infrastructure on Chinese magnesium[182], such activity would only further increase reliance on an ever-shrinking number of alternative suppliers.

The final vector identified how covert action could be used to induce political risk in different disparate supply-chain elements, first drawing upon Belgian and American action against then Congolese Prime Minister Patrice Lumumba and then identifying different clandestine methods that have been used to leverage political unrest in a variety of other instances. These methods include assassination, the use of propaganda through media organizations, the funding of militants through cash or narcotics, and coups.

Finally, in Section **??**, the paper first discussed how the specificity of the five identified attack vectors was limited to broad categories of activities arising from the system-scope. The purpose of this paper was to create an iterative framework for further implementation and investigation, which it did, but this limited scope precluded more granular analysis.

Additionally, this section discussed that future iterations and implementations of this framework should focus on what supply-chains can be targeted and when. This is especially pertinent given the time-bound nature of complex systems like supply-chains. A further limitation was that the construction of a theoretical opponent was limited in this iteration of the framework and application: future efforts should outline the capabilities of the attacker to gain a better estimation of attack vector feasibility. This would also allow other research to investigate the decision-making process of an attacker, especially regarding how they could mitigate their own risk arising from their attacks concerning other actors in the supply-chain.

Finally, the paper concludes with the acknowledgment that further research ought to be more constrained in scope and that other attack vectors ought to be investigated.

X. APPENDIX - SUPPLY RISK RANKING

```
    library(readxl)
library(lubridate)
library(plotrix)
library(vcdExtra)
library(car)
library(lmtest)
library(purrr)
library(tidyverse)
#Import Datasets
raw<-read.table(”~/Documents/thesis/datasets/output_base.csv”, header = TRUE, sep = ”,”) #EU CRM summary


refined_table<-raw%>%filter(Material %in% c(”Aluminium”, ”Antimony”, ”Baryte”, ”Beryllium”, ”Bismuth”,                    ”Boron”, ”Cobalt”, ”Coking coal”, ”Copper”, ”Feldspar”, ”Fluorspar”, ”Gallium”, ”Germanium”, ”Hafnium”, ”Helium”, ”HREES”, ”Indium”, ”Lithium”, ”LREEs”, ”Magnesium”, ”Natural graphite”, ”Natural Rubber”, ”Nickel”, ”Niobium”, ”PGMs”, ”Phosphate rock”, ”Phosphorus”, ”Scandium”, ”Silicon metal”, ”Strontium”, ”Tantalum”, ”Titanium metal”, ”Tungsten”, ”Vanadium”)) %>% select(Material, SR_2020, SR_2023, EI_2020, EI_2023)

# Assuming ’refined_table’ is your filtered dataset

# Find top 10 highest values for SR_2020
top_10_SR_2020 <- refined_table %>%
  select(Material, SR_2020) %>%
  arrange(desc(SR_2020)) %>%
  slice_max(order_by = SR_2020, n = 10)

# Find top 10 highest values for SR_2023
top_10_SR_2023 <- refined_table %>%
  select(Material, SR_2023) %>%
  arrange(desc(SR_2023)) %>%
  slice_max(order_by = SR_2023, n = 10)
# Rename the year-specific columns to a common name in both data frames
top_10_SR_2020 <- top_10_SR_2020 %>%
  rename(SR_Value = SR_2020)

top_10_SR_2023 <- top_10_SR_2023 %>%
  rename(SR_Value = SR_2023)

# Add a column to each data frame to indicate the year
```

```
top_10_SR_2020$Year <- ”2020”
top_10_SR_2023$Year <- ”2023”


# Combine and print the tables
top_10_combined <- rbind(top_10_SR_2020, top_10_SR_2023)

# Print the combined table
print(top_10_combined)

# Add a ranking column to both data frames
top_10_SR_2020$Rank <- 1:nrow(top_10_SR_2020)
top_10_SR_2023$Rank <- 1:nrow(top_10_SR_2023)

# Rename the columns to have unique names, except for the common key (Rank)
colnames(top_10_SR_2020) <- c(”Material_2020”, ”SR_2020”, ”Rank”)
colnames(top_10_SR_2023) <- c(”Material_2023”, ”SR_2023”, ”Rank”)

# Merge the data frames side by side based on the Rank column
combined_table <- merge(top_10_SR_2020, top_10_SR_2023, by = ”Rank”)

# Print the combined table
print(combined_table)
```

XI. Appendix - Annual Volatility Calculation

```
library(tidyverse)
library(lubridate)
library(readr)
library(purrr)
library(RColorBrewer)
library(ggplot2)
run_annual_volatility_analysis <- function(base_directory, output_directory, start_date, end_date, k, N) {
  calculate_annualized_volatility <- function(log_returns) {
    mean_log_return <- mean(log_returns)
    variance_log_return <- sum((log_returns - mean_log_return)^2) / k
    annualized_volatility <- sqrt(variance_log_return * (N / k)) * 100
    return(annualized_volatility)
  }
```

```
 #Takes price .csv files, computes log returns, and runs them through the calculate_annualized_volatility function
# Also outputs annual volatility .csv files
  process_file <- function(file_path) {
    data <- read_csv(file_path) %>%
      mutate(
        Date = ymd(Date),
        Log_Return = log((`Max. Price` + `Min. Price`) / 2 / lag((`Max. Price` + `Min. Price`) / 2)),
        Year = year(Date)
      ) %>%
      filter(Date >= ymd(start_date) & Date <= ymd(end_date)) %>% # Apply date range filter
      na.omit()

    data_by_year <- data %>%
      group_by(Year) %>%
      summarise(Log_Returns = list(Log_Return), .groups = 'drop')

    annual_volatility_by_year <- data_by_year %>%
      rowwise() %>%
      mutate(Annual_Volatility = calculate_annualized_volatility(Log_Returns)) %>%
      select(-Log_Returns)

    identifier <- str_remove(basename(file_path), "\\.csv$")
    write_csv(annual_volatility_by_year, file.path(output_directory, paste0(identifier, "_annual_volatility.csv")))
  }
#If the output directory exists, save the _annual_volatility.csv files there
  if (!dir.exists(output_directory)) {
    dir.create(output_directory)
  }

  file_paths <- list.files(base_directory, pattern = "\\.csv$", full.names = TRUE)
  walk(file_paths, process_file)
}


categorize_minerals <- function(mineral_name, patterns_df) {
  category <- "Other Minerals" # Default category
  for (i in seq_len(nrow(patterns_df))) {
    patterns <- strsplit(trimws(patterns_df$Pattern[i]), "\\|")[[1]] # Split patterns by '|'
    for (pattern in patterns) {
      if (grepl(pattern, mineral_name, ignore.case = FALSE)) {
        category <- patterns_df$Category[i]
        break  # Break inner loop
      } else {
        print(paste(”Pattern not matched:”, pattern, ”with mineral name:”, mineral_name)) # Debug print, technically redundant
      }
    }
    if (category != ”Other Minerals”) {
      break  # Break outer loop if a category is found
    }
  }
  print(paste(”Final category for”, mineral_name, ”is”, category)) # Debug print
  return(category)
}

#This function calculates the mean prices for each date, and than graphs it.
analyze_and_plot_prices_by_group <- function(price_directory, patterns_file, plot_output_directory) {
  patterns_df <- read.csv(patterns_file)

  price_paths <- list.files(price_directory, pattern = ”\\.csv$”, full.names = TRUE)

  group_data_list <- list()

  # Define the date range
  start_date <- as.Date(”2019-01-01”)
  end_date <- as.Date(”2023-12-31”)

  for (price_path in price_paths) {
    mineral_data <- read_csv(price_path, show_col_types = FALSE) %>%
      mutate(Date = ymd(Date), Avg_Price = (‘Max. Price‘ + ‘Min. Price‘) / 2) %>%
      # Filter data within the specified date range
      filter(Date >= start_date & Date <= end_date)

    base_filename <- gsub(”\\.csv$”, ””, basename(price_path))
    mineral_group <- categorize_minerals(base_filename, patterns_df)

    if (!mineral_group %in% names(group_data_list)) {
      group_data_list[[mineral_group]] <- tibble()
    }

    mineral_data$Mineral <- base_filename
    group_data_list[[mineral_group]] <- bind_rows(group_data_list[[mineral_group]], mineral_data)
  }

  if (!dir.exists(plot_output_directory)) {
    dir.create(plot_output_directory, recursive = TRUE)
  }
  #Plotting
  for (mineral_group in names(group_data_list)) {
    p <- ggplot(group_data_list[[mineral_group]], aes(x = Date, y = Avg_Price, color = Mineral)) +
      geom_line() +
      labs(title = paste(”Average Prices for”, mineral_group, ”Group”),
           x = ”Date”, y = ”Average Price ($)/unit”) +
      theme_minimal() +
      scale_color_viridis_d() +
        theme(legend.position = ”right”) + #move legend to the right
        guides(color = guide_legend(ncol = 1)) #ensure all legend entries are shown

    file_name <- paste0(gsub(”[ˆ[:alnum:]_]”, ””, mineral_group), ”_avg_price.png”)
    print(paste(”Saving file:”, file_name)) # For debugging

    ggsave(filename = file.path(plot_output_directory, file_name),
           plot = p, device = ”png”, width = 14, height = 8) # Increase plot size
  }
}

plot_volatility <- function(volatility_data_directory, patterns_file, plot_output_directory) {
  patterns_df <- read_csv(patterns_file)


  file_paths <- list.files(volatility_data_directory, pattern = ”\\.csv$”, full.names = TRUE)
  group_data_list <- list()

  for (volatility_path in file_paths) {
    volatility_data <- read_csv(volatility_path, col_types = cols(Year = col_integer(), Annual_Volatility = col_double()))
    base_filename <- gsub(”\\.csv$”, ””, basename(volatility_path))
    mineral_group <- categorize_minerals(base_filename, patterns_df)

    if (!mineral_group %in% names(group_data_list)) {
      group_data_list[[mineral_group]] <- tibble()
    }

    volatility_data$Mineral <- base_filename
    group_data_list[[mineral_group]] <- bind_rows(group_data_list[[mineral_group]], volatility_data)
  }

  if (!dir.exists(plot_output_directory)) {
    dir.create(plot_output_directory, recursive = TRUE)
  }
  #Actually plotting
  for (mineral_group in names(group_data_list)) {
    p <- ggplot(group_data_list[[mineral_group]], aes(x = Year, y = Annual_Volatility, color = Mineral, group = Mineral)) +
      geom_line() +
      labs(title = paste(”Annual Volatility for”, mineral_group, ”Group”),
           x = ”Year”, y = ”Volatility (%)”) +
      theme_minimal() +
      scale_color_viridis_d() +
      theme(legend.position = ”right”) +  # Move legend to the right
      guides(color = guide_legend(ncol = 1)) # Ensure all legend entries are shown

    file_name <- paste0(gsub(”[^[:alnum:]_]”, ””, mineral_group), ”_volatility.png”)
    print(paste(”Saving file:”, file_name))  # For debugging

    ggsave(filename = file.path(plot_output_directory, file_name),
           plot = p, device = ”png”, width = 14, height = 8) # Increase plot size
  }
}

# Main function to analyze and plot volatility and price data
run_annual_volatility_analysis(”/home/contractor-think/Documents/thesis/datasets/original_datasets/”, ”/home/contractor-think/Documents/thesis/datasets/outputs/”, ”2020-01-30”, ”2023-12-31”, 21, 252)
analyze_and_plot_prices_by_group(”/home/contractor-think/Documents/thesis/datasets/original_datasets”, ”/home/contractor-think/Documents/thesis/datasets/patterns.csv”, ”/home/contractor-think/Pictures/backup/prices”)
plot_volatility(”/home/contractor-think/Documents/thesis/datasets/outputs”, ”/home/contractor-think/Documents/thesis/datasets/patterns.csv”, ”/home/contractor-think/Pictures/backup/volatility”)
```

XII. Appendix - Aggregate Volatility Index for Mineral Groups

```r
    library(tidyverse)
library(lubridate)
library(readr)
library(purrr)
library(RColorBrewer)
library(ggplot2)

categorize_minerals <- function(mineral_name, patterns_df) {
  category <- "Other Minerals" # Default category
  for (i in seq_len(nrow(patterns_df))) {
    patterns <- strsplit(trimws(patterns_df$Pattern[i]), "\\|")[[1]] # Split patterns by '|'
    for (pattern in patterns) {
      if (grepl(pattern, mineral_name, ignore.case = FALSE)) {
        category <- patterns_df$Category[i]
        break # Break inner loop
      } else {
        print(paste("Pattern not matched:", pattern, "with mineral name:", mineral_name)) # Debug print, technically redundant
      }
    }
    if (category != "Other Minerals") {
      break # Break outer loop if a category is found
    }
  }
  print(paste("Final category for", mineral_name, "is", category)) # Debug print
  return(category)
}

# Function to calculate mean annual volatility and save to CSV
calculate_and_save_mean_volatility <- function(base_directory, output_directory) {
  file_paths <- list.files(base_directory, pattern = "_annual_volatility\\.csv$", full.names = TRUE)

  process_file <- function(file_path) {
    data <- read_csv(file_path)
    mean_volatility <- data %>%
      filter(!is.na(Annual_Volatility)) %>%
      summarise(mean_annual_volatility = mean(Annual_Volatility)) %>%
      pull(mean_annual_volatility)

    base_filename <- gsub("_annual_volatility\\.csv$", "", basename(file_path))
    result <- tibble(Mineral = base_filename, Mean_Annual_Volatility = mean_volatility)

    write_csv(result, file.path(output_directory, paste0(base_filename, ”_mean_volatility.csv”)))
  }

  if (!dir.exists(output_directory)) {
    dir.create(output_directory, recursive = TRUE)
  }

  walk(file_paths, process_file)
}

# Function to calculate mean annual volatility and save to CSV
calculate_and_save_mean_volatility <- function(base_directory, output_directory) {
  file_paths <- list.files(base_directory, pattern = ”_annual_volatility\\.csv$”, full.names = TRUE)

  process_file <- function(file_path) {
    data <- read_csv(file_path)
    mean_volatility <- data %>%
      filter(!is.na(Annual_Volatility)) %>%
      summarise(mean_annual_volatility = mean(Annual_Volatility)) %>%
      pull(mean_annual_volatility)

    base_filename <- gsub(”_annual_volatility\\.csv$”, ””, basename(file_path))
    result <- tibble(Mineral = base_filename, Mean_Annual_Volatility = mean_volatility)

    write_csv(result, file.path(output_directory, paste0(base_filename, ”_mean_volatility.csv”)))
  }

  if (!dir.exists(output_directory)) {
    dir.create(output_directory, recursive = TRUE)
  }

  walk(file_paths, process_file)
}

# Function to read results, categorize, average, and plot
read_and_plot_mean_volatility <- function(volatility_data_directory, patterns_file, plot_output_directory) {
  patterns_df <- read_csv(patterns_file)
  file_paths <- list.files(volatility_data_directory, pattern = ”_mean_volatility\\.csv$”, full.names = TRUE)

  process_file <- function(file_path) {
    data <- read_csv(file_path)
    mineral_name <- data$Mineral[1]
    mean_volatility <- data$Mean_Annual_Volatility[1]
    mineral_group <- categorize_minerals(mineral_name, patterns_df)

    tibble(Mineral = mineral_name, Group = mineral_group, Mean_Annual_Volatility = mean_volatility)
  }

  volatility_data <- map_df(file_paths, process_file)

  group_averages <- volatility_data %>%
    group_by(Group) %>%
    summarise(Average_Mean_Annual_Volatility = mean(Mean_Annual_Volatility, na.rm = TRUE)) %>%
    ungroup()

  plot_volatility_group_averages <- function(group_averages, plot_output_directory) {
    p <- ggplot(group_averages, aes(x = reorder(Group, Average_Mean_Annual_Volatility), y = Average_Mean_Annual_Volatility, fill = Group)) +
      geom_bar(stat = ”identity”, position = ”dodge”) +
      labs(title = ”Average Mean Annual Volatility for Mineral Groups”,
           x = ”Mineral Group”, y = ”Average Mean Annual Volatility (%)”) +
      theme_minimal() +
      theme(axis.text.x = element_text(angle = 45, hjust = 1)) +
      scale_fill_viridis_d()

    file_name <- ”group_averages_mean_annual_volatility.png”

    ggsave(filename = file.path(plot_output_directory, file_name),
           plot = p, device = ”png”, width = 14, height = 8)
  }

  if (!dir.exists(plot_output_directory)) {
    dir.create(plot_output_directory, recursive = TRUE)
  }

  plot_volatility_group_averages(group_averages, plot_output_directory)
}

# Combined function to execute both steps
```

```
process_and_plot_mean_volatility <- function(base_directory, patterns_file, intermediate_output_directory, plot_output_directory) {
  calculate_and_save_mean_volatility(base_directory, intermediate_output_directory)
  read_and_plot_mean_volatility(intermediate_output_directory, patterns_file, plot_output_directory)
}

process_and_plot_mean_volatility("/home/contractor-think/Documents/thesis/datasets/outputs","/home/contractor-think/Documents/thesis/datasets/patterns.csv","/home/contractor-think/avg_outputs_dir","/home/contractor-think/Pictures/avg_vol")
```

XIII. Appendix - Parkinson's volatility calculation with a five day window

```
    library(lubridate)
library(readr)
library(purrr)
library(dplyr)
library(zoo)
library(stringr)
library(ggplot2)
# Define the Parkinson's Volatility Function
parkinsons_volatility <- function(high_prices, low_prices) {
  # Calculate the logarithmic range
  log_range <- log(high_prices / low_prices)

  # Calculate the squared logarithmic range
  squared_log_range <- log_range^2

  # Calculate the mean of the squared logarithmic ranges
  mean_squared_log_range <- mean(squared_log_range, na.rm = TRUE)

  # Calculate Parkinson's volatility
  parkinson_volatility <- sqrt(mean_squared_log_range / (4 * log(2)))

  # Convert to percentage
  parkinson_volatility_percentage <- parkinson_volatility * 100

  return(parkinson_volatility_percentage)
}

# Define the Rolling Volatility Function
calculate_rolling_volatility <- function(high_prices, low_prices, window_size) {
  rollapplyr(
    data = seq_along(high_prices),
    width = window_size,
    FUN = function(i) parkinsons_volatility(high_prices[i], low_prices[i]),
    by.column = FALSE,
    fill = NA
  )
}

# Function to identify largest increases in volatility on a quarterly basis
identify_largest_increases <- function(volatility_data) {
  volatility_data <- volatility_data %>%
    mutate(
      Quarter = floor_date(Date, "quarter")
    ) %>%
    group_by(Quarter) %>%
    mutate(
      Volatility_Change = Rolling_Volatility - lag(Rolling_Volatility)
    ) %>%
    filter(!is.na(Volatility_Change)) %>%
    arrange(Quarter, desc(Volatility_Change)) %>%
    slice(1) %>%
    ungroup()

  return(volatility_data)
}

run_rolling_volatility_analysis <- function(base_directory, output_directory, start_date, end_date, window_size) {
  process_file <- function(file_path) {
    data <- read_csv(file_path) %>%
      mutate(
        Date = ymd(Date)
      ) %>%
      filter(Date >= ymd(start_date) & Date <= ymd(end_date)) %>% # Apply date range filter
      na.omit()

    dates <- data$Date
    high_prices <- as.numeric(data$`Max. Price`)
    low_prices <- as.numeric(data$`Min. Price`)

    # Calculate rolling Parkinson's volatility in percentage
    rolling_volatility <- calculate_rolling_volatility(high_prices, low_prices, window_size)

    result <- tibble(Date = dates, Rolling_Volatility = rolling_volatility)

    identifier <- str_remove(basename(file_path), "\\.csv$")
    write_csv(result, file.path(output_directory, paste0(identifier, "_rolling_volatility.csv")))
  }

  if (!dir.exists(output_directory)) {
    dir.create(output_directory, recursive = TRUE)
  }

  file_paths <- list.files(base_directory, pattern = "\\.csv$", full.names = TRUE)
  walk(file_paths, process_file)
```

```
}

categorize_minerals <- function(mineral_name, patterns_df) {
  category <- ”Other Minerals” # Default category
  for (i in seq_len(nrow(patterns_df))) {
    patterns <- strsplit(trimws(patterns_df$Pattern[i]), ”\\|”)[[1]]  # Split patterns by '|'
    for (pattern in patterns) {
      if (grepl(pattern, mineral_name, ignore.case = FALSE)) {
        category <- patterns_df$Category[i]
        break  # Break inner loop
      } else {
        print(paste(”Pattern not matched:”, pattern, ”with mineral name:”, mineral_name))  # Debug print
      }
    }
    if (category != ”Other Minerals”) {
      break  # Break outer loop if a category is found
    }
  }
  print(paste(”Final category for”, mineral_name, ”is”, category))  # Debug print
  return(category)
}




plot_volatility <- function(volatility_data_directory, patterns_file, plot_output_directory) {
  patterns_df <- read_csv(patterns_file)

  file_paths <- list.files(volatility_data_directory, pattern = ”_rolling_volatility\\.csv$”, full.names = TRUE)
  group_data_list <- list()

  for (volatility_path in file_paths) {
    volatility_data <- read_csv(volatility_path, col_types = cols(Date = col_date(), Rolling_Volatility = col_double()))
    base_filename <- gsub(”_rolling_volatility\\.csv$”, ””, basename(volatility_path))
    mineral_group <- categorize_minerals(base_filename, patterns_df)

    if (!mineral_group %in% names(group_data_list)) {
      group_data_list[[mineral_group]] <- tibble()
    }

    volatility_data$Mineral <- base_filename
    group_data_list[[mineral_group]] <- bind_rows(group_data_list[[mineral_group]], volatility_data)
  }

  if (!dir.exists(plot_output_directory)) {
    dir.create(plot_output_directory, recursive = TRUE)
  }

  for (mineral_group in names(group_data_list)) {
    p <- ggplot(group_data_list[[mineral_group]], aes(x = Date, y = Rolling_Volatility, color = Mineral, group = Mineral)) +
      geom_line() +
      labs(title = paste("Rolling Volatility for", mineral_group, "Group"),
           x = "Date", y = "Volatility (%)") +
      theme_minimal() +
      scale_color_viridis_d() +
      theme(legend.position = "right") + # Move legend to the right
      guides(color = guide_legend(ncol = 1)) # Ensure all legend entries are shown

    file_name <- paste0(gsub("[^[:alnum:]_]", "", mineral_group), "_rolling_volatility.png")
    print(paste("Saving file:", file_name)) # For debugging

    ggsave(filename = file.path(plot_output_directory, file_name),
           plot = p, device = "png", width = 14, height = 8) # Increase plot size
  }
}

run_rolling_volatility_analysis("/home/contractor-think/Documents/thesis/datasets/original_datasets","/home/contractor-think/Documents/rolling_vol_dec", "2023-12-01", "2024-01-30", 2)
plot_volatility("/home/contractor-think/Documents/rolling_vol_dec","/home/contractor-think/Documents/thesis/datasets/patterns.csv","/home/contractor-think/Pictures/dec_vol")
```