p-ISSN : 2708-2121 | e-ISSN : 2708-3616
DOI(Journal): 10.31703/gsssr
DOI(Volume): 10.31703/gsssr/.2024(IX)
DOI(Issue): 10.31703/gsssr.2024(IX.I)

www.gsssrjournal.com

Global Strategic and Security Studies Review
surveilling humanity

GSSSR

GLOBAL STRATEGIC & SECURITY STUDIES REVIEW

VOL. IX, ISSUE I, WINTER (MARCH-2024)

HumanityPublications
sharing research
www.humapub.com
US | UK | Pakistan

Double-blind Peer-review Research Journal
www.gsssrjournal.com

Humanity Publications(HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Article Title

Cross Domain Deterrence in Asia Pacific and Indian Ocean Region

Global Strategic & Security Studies Review

p-ISSN: 2708-2121**e-ISSN:** 2708-3616
DOI(journal):10.31703/gsssr
Volume: IX (2024)
DOI (volume):10.31703/gsssr.2024(IX)
Issue: I (Winter-March 2024)
DOI(Issue): 10.31703/gsssr.2024(IX-I)

Home Page
www.gsssrjournal.com

Volume: IX (2024)
https://www.gsssrjournal.com/Current-issues

Issue: I-Winter (March-2024)
https://www.gsssrjournal.com/Current-issues/9/1/20234

Scope
https://www.gsssrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gsssr/submissions

Google Scholar

Visit Us

Abstract

Deterrence as a concept is deeply rooted in human nature and for a considerable time it was contested and jilted, yet it resurfaced in one way or the other. Nuclear weapons became the backbone of the concept of Deterrence. Due to the inherent dynamism of Revolution in Military Affairs, the supremacy of Nuclear is being challenged with the advent of the latest technologies which are acting as enablers and disruptors. The concept of Cross Domain Deterrence emerged a decade ago, took shape, and entered the strategic lexicon. It has enablers and drivers, while a gradual shift in this direction is visible. While remaining within the ambit of complex interdependence theory given by Robert O Keohane and Joseph S Nye. This article examines the applicability of Cross-Domain Deterrence in the Asia Pacific and Indian Ocean Region focusing on the US, China, India, and Pak to identify the need to look beyond the horizon and embrace the change..

Keywords: Deterrence, Cross Domain Deterrence, US, China, India, Pakistan and Strategic Stability

Authors:

Sheikh Ghulam Jilani:(Corresponding Author)
PhD Scholar, Department of Strategic Studies, National Defence University, Islamabad, Pakistan.
(Email:jilani1971@ndu.edu.pk)

Pages: 1-15
DOI:10.31703/gsssr.2024(IX-I).01
DOI link:https://dx.doi.org/10.31703/gsssr.2024(IX-I).01
Article link: http://www.gsssrjournal.com/article/A-b-c
Full-text Link: https://gsssrjournal.com/fulltext/
Pdf link: https://www.gsssrjournal.com/jadmin/Auther/31rvIolA2.pdf

Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Citing this Article

01		Cross Domain Deterrence in Asia Pacific and Indian Ocean Region						
		Author	Sheikh Ghulam Jilani		DOI	10.31703/gsssr.2024(IX-I).01		
Pages		1-15	Year	2024	Volume	IX	Issue	I
Referencing & Citing Styles	APA	Jilani, S. G. (2024). Cross Domain Deterrence in Asia Pacific and Indian Ocean Region. *Global Strategic & Security Studies Review*, *IX*(I), 1-15. https://doi.org/10.31703/gsssr.2024(IX-I).01						
	CHICAGO	Jilani, Sheikh Ghulam. 2024. "Cross Domain Deterrence in Asia Pacific and Indian Ocean Region." *Global Strategic & Security Studies Review* IX (I):1-15. doi: 10.31703/gsssr.2024(IX-I).01.						
	HARVARD	JILANI, S. G. 2024. Cross Domain Deterrence in Asia Pacific and Indian Ocean Region. *Global Strategic & Security Studies Review,* IX, 1-15.						
	MHRA	Jilani, Sheikh Ghulam. 2024. 'Cross Domain Deterrence in Asia Pacific and Indian Ocean Region', *Global Strategic & Security Studies Review*, IX: 1-15.						
	MLA	Jilani, Sheikh Ghulam. "Cross Domain Deterrence in Asia Pacific and Indian Ocean Region." *Global Strategic & Security Studies Review* IX.I (2024): 1-15. Print.						
	OXFORD	Jilani, Sheikh Ghulam (2024), 'Cross Domain Deterrence in Asia Pacific and Indian Ocean Region', *Global Strategic & Security Studies Review,* IX (I), 1-15.						
	TURABIAN	Jilani, Sheikh Ghulam. "Cross Domain Deterrence in Asia Pacific and Indian Ocean Region." *Global Strategic & Security Studies Review* IX, no. I (2024): 1-15. https://dx.doi.org/10.31703/gsssr.2024(IX-I).01.						

e-ISSN:2708-3616 Volume: IX (2024) Issue: I-Winter (March-2024) p-ISSN:2708-2121

Global Strategic & Security Studies Review
www.gprjournal.com
DOI: http://dx.doi.org/10.31703/glsr

Pages:1-15 URL:https://doi.org/10.31703/gsssr.2024(IX-I).01 Doi: 10.31703/gsssr.2024(IX-I).01

Cite Us

Title

Cross Domain Deterrence in Asia Pacific and Indian Ocean Region

Contents

Abstract

Deterrence as a concept is deeply rooted in human nature and for a considerable time it was contested and jilted, yet it resurfaced in one way or the other. Nuclear weapons became the backbone of the concept of Deterrence. Due to the inherent dynamism of Revolution in Military Affairs, the supremacy of Nuclear is being challenged with the advent of the latest technologies which are acting as enablers and disruptors. The concept of Cross Domain Deterrence emerged a decade ago, took shape, and entered the strategic lexicon. It has enablers and drivers, while a gradual shift in this direction is visible. While remaining within the ambit of complex interdependence theory given by Robert O Keohane and Joseph S Nye. This article examines the applicability of Cross-Domain Deterrence in the Asia Pacific and Indian Ocean Region focusing on the US, China, India, and Pak to identify the need to look beyond the horizon and embrace the change.

Authors:

Sheikh Ghulam Jilani:(Corresponding Author)

PhD Scholar, Department of Strategic Studies, National Defence University, Islamabad, Pakistan.

(Email: jilani1971@ndu.edu.pk)

Keywords: Deterrence, Cross Domain Deterrence, US, China, India, Pakistan and Strategic Stability

Introduction

Deterrence an old concept is in fact very central to human nature. It has many facets and paradigms which have evolved over a period of time. Deterrence is a natural, instinctive, and recurring phenomenon (Freedman, 2004) with origins deep into history in various forms and manifestations. Deterrence ever since its origin has been used as a concept in almost all aspects of life. In the context of strategy and statecraft, it has a more military character based on the interaction of political aspirations, economic capacity, and military equipment. Deterrence in the distant military history is found embedded with the naval arms where the concept of 'fleet in being' (Hauser, 2010) was used which then shifted to the airpower in 1930. After 1945 the same concepts of deterrence were used by Great Britain, the United States of America, and even Europe. Deterrence predicated on nuclear weapons was initially a concept alien to NATO member states, however, after the Second World War, deterrence became synonymous with nuclear capability and is still playing an important role in strategic stability (Cox, 2020). It was widely used in the Cold War and after the nuclearization of India and Pakistan in 1988, it started taking root in South Asia as well.

Deterrence is a coercive strategy, however, with the evolution of warfare, it too has evolved. Until recently, it was solely being used predicated on nuclear capabilities but with the advent of other technologies and weapon systems gradually the entire gamut of warfare has also morphed itself. Advancements and dependencies of warfare and national-level security strategies in other aspects of cyber, space, logistics, artificial intelligence, automated weapon systems, and other disruptive technologies have added to the complexities of the strategists – hence the new term of Cross Domain Deterrence (CDD) emerged. It implies the use or threat to use of one type or different types and or even in combination (the capabilities, weapons systems, or technologies) to deter a target from taking or attempting to take actions to change the status quo(Lindsay and Gartzke, 2019).

The nature of war is constant (Clausewitz, 1984) yet the character has changed manifolds from Napoleonic Total War to Hybrid War. Concepts of *Phalanxes* and *Strategic Corporal*(Liddy, 2004) are poles apart in application yet they aim for the same – victory in the battle. Another conceptual adaptation is multi-domain operations which in yester years was also intrinsically present. Hybrid war, grey hybrid, multi-domain operations, and CDD are all new spikes implying an unabated search for strategic stability. Politics and Economics are intertwined while other aspects of hard power, soft power, smart power, and sharp power are causing pulls and pushes to strategic stability. In the Asia Pacific context, the strategic equation has changed to a great extent. International Liberal Order which was singularly steered by the US is being contested (Patrick, 2017) by a more broad-based world order with China and various other nations. The strategic stability in the Indian Ocean Region (IOR) is not anymore between two nuclear states i.e., India and Pakistan (as discussed in Deterrence Instability by Krepon, 2015)but it has more players – the US the resident power, China the emerging power, Russia the resurgent power, Japan the nascent old imperial power, India the desirous regional power and even North Korea the retaliatory power. Traditional domains of deterrence have been accentuated from the asymmetry of forces to nuclear, from nuclear to cyber, and from cyber to AI alongside the advancement in economics, diplomacy, politics, security, and information-related realms of power projection. Supremacy in the *net national power potential* is the game of deterrence as of today.

IOR and Asia Pacific house a number of nuclear states; China, US, and Russia; India (Prestige driven) and Pakistan (Security Driven); North Korea (Coercer); while Iran (Aspirant) and Japan (Nascent) – all have a significant role in this strategic equilibrium. Amidst this congregation of nuclear states, there is an interplay of other domains which has started the debate on the efficacy of concepts of nuclear deterrence. Specifically focusing on the Asia Pacific and IOR, the applicability of CDD has been tested to ascertain whether CDD is a distortion in the existing concept of deterrence (Jaffery, 2020) or is an amplification of the same.

Framework

The article is primarily based on C*omplex Interdependence as given by* Keohane and Nye, (2012). The current discussion of nuclear deterrence and CDD is about the power struggle and the role of politics, economics, and geography in it. 'Complex Interdependence' as explained by Robert O Keohane and Joseph Nye has three main characteristics; (1) multiple channels exist that connect societies formally and informally, (2) multiple issues exist without any hierarchy or order or agenda and there is a lack of coordination yet there is a lot of interconnectivities, (3) absence of use of military force towards other governments in the same region. This gives birth to a distinctive political process through which power is used to control and deter. The explanation that 'globalization' has brought the world closer to complexities on various issues of climate, financial market, and terrorism is also recognized as complex interdependence. With a similar analogy, the idea of connectivity, relevance, and interdependence in the application of the same in the construct of CDD seems to amplify the aspects in a much better manner.

Importance of Asia

Asia has always been the center stage for power contestation, surfing on high tides of stability and instability paradox where the quest for the supremacy of domains is juxtaposed with the inherent national intent and interests. This competition is constantly spiraling into multi-

domains i.e., conventional, nuclear, political, economic, diplomatic, and lately hybrid. China-US strategic contestation has brought in the aspects of cyber, AI, and space thus affecting the stability equilibrium. A security dilemma exists in the Asia Pacific and IOR. Competing changes in the international order due to the rise of other powers (China and Russia) viz the traditional supremacy of the US amidst the 'Asian Century (Overholt, 2012), started an intense debate regarding the competing strategies, security dilemma models, and theories, and trade war. On the other hand, the concept of deterrence with its traditional legacy of World War II and the Cold War is also under discussion. Ideas of Hard Power, Soft Power, Smart Power (Nye Jr, 2009), and Sharp Power (Walker & Ludwig, 2017) are casting shadows onto the conceptual edifices of deterrence – Nuclear Weapons. The advent of other disruptive technologies and weapons also added to this discussion. The idea of CDD has been discussed in the US for the last 10 years, Russia also focuses on it where we see 'Strategic Deterrence' (Bruusgaard, 2016) in action and Japan which is a highly sophisticated nascent military power also issued its defense paper in 2019 discussing the issues of cyber, space and AI. China is running bounds and leaps in such technologies hence domain effects are significant (Westerheide, 2020)While remains true for extremely developed nations like the US, China, and Russia where other domains (Cyber and Space) are inextricably linked to their security sectors yet in the context of India, Pakistan, North Korea, and Iran, this aspect is yet to attain some solid grounds and currency in the military lexicons and statecraft.

The Debate of Cross-Domain Deterrence

Freedman identifies that deterrence is an instinctive act that is basically to alter or control the behavior of another person or entity. He also identifies that it can either be based on a capability or even a bluff yet it is a deliberate effort to control the other. The concept of deterrence is natural, instinctive, focused, and deliberate. Deterrence is a state of mind, it can also be a technique and a doctrine. Deterrence can be marginal, tangential, or speculative. It intrinsically defends the interest and also demonstrates how it will function even if challenged and still defending the interest. Freedman also laid emphasis on the principles of Credibility, Capability, and Communication. This entire spectrum of deterrence in the context of emerging technologies and CDD, remains valid and adaptable; and is fully applicable without any linkage to any deciding factor as such.

Jon R Lindsay and Eric Gartzkehad explicitly documented the concept of CDD, while the Pentagon recognizes *land, air, sea, (traditional), space, and cyberspace* as new domains. Interestingly, the entire gamut of conflict is spread from disaster relief to counter-terrorism and from conventional combat to nuclear war, with this diversity, the military power and state power success depends intimately upon cross-domain operations. The Chinese concept of 'integrated strategic deterrence' and the Russian concept of 'strategic deterrence' integrates and synchronizes non-nuclear, informational, and nuclear means to tackle hybrid warfare. Merging various emerging technologies has created contradictions and expectations. Weaker states and Non-State Actors may manipulate the technological advantages and undermine bigger powers while bigger powers may augment their existing potential. CDD poses challenges and problems, especially in 21st-century warfare. For the US and other developed nations, CDD has more implications in cyberspace. The mere vulnerability of the cyber domain has led to the concern for US and China alike once we see operations being conducted. Deterrence has been a political problem that is predicated on interests, power, information, and resolve. The concept of CDD arose in particular contexts and amidst the diversity of technologies after the Cold War. In order to tackle the complexities of modern deterrence one may have to relax the traditional focus on nuclear weapons and improve mutual undertakings while controlling proliferation. Addressing the challenges in the domains of space, and cyberspace besides other traditional aspects of land, air, and sea will also enhance the thresholds. The primary concern is that these domains differ from each other yet their effects and problems are interlinked, intertwined and complexities are manifold. There are different implications at strategic levels for various military domains and the sole idea of technology relating to CCD is also at times contestable. For CDD to be effective, just like the traditional requirements of deterrence, the aspects of credibility and communication are very valid and applicable. CDD has become acute in 21st-century globalization, is very much valid, and needs

further deliberation. It is in this context, that once we mount the template on the Asia-Pacific and IOR, its manifestation is vivid and is impacting the strategic stability.

Revolutionary transformation in the concept of 'Deterrence' to the concept of 'Cross Domain Deterrence' is actually a leap of faith and is indeed a long journey yet it is still rooted in the original concept. The concept is deceptive apparently where it seems that traditionally deterrence was being practiced in all three domains of land, air, and sea – militarily. In the context of the Cold War, fear and possibility of an attack either conventional or nuclear, in any domain i.e., air, land, or sea, formed the basis of the concept of deterrence (Mallory, 2018). The current strategy of politico-military or politico-economic and even a combination of both is a cross-domain deterrence once we call it politico-military-diplomatic-economic coercion – it is cutting through a lot of places that can deter and hurt. However, there are various definitions which are available in the literature but all of them converge on the point that CDD engages the threat in one domain to deter and counter the activities in another domain (Sweijs&Zilincik, 2019). It is also noticeable that most of the definitions focus on the military domains of land, air, and sea and add cyber and space. However, once we focus on the contemporary definitions of CDD, it extends the notion of basic deterrence in a classical fashion, thereby exploring and investigating how the threat(s) in a particular domain can be countered by different capabilities in a different domain. CDD can also be explained as posing a threat in a domain or combination of threats and domains so as to prevent the activities in other domain(s) which can potentially alter the status quo or it could also be using different means to gain political dividends of deterrence. CDD also can be explained that it is the ability of a weapon or tool, the use of which can stop the use of a weapon by an adversary in another domain (Dawkins, 2019). The use of cyber technology to affect the guidance of missile systems is one of the examples that can explain the usage. In a more precise and broad fashion CDD can also be explained as the use of economic sanctions, and diplomatic and political tools (*non-military domains*) to preclude or thwart an action in land, sea, air, space, or cyber domains (*military domains*) (Vince, 2015). There is also a realization that with new generations, types, and manifestations of warfare the concept of CDD is also getting more dynamic and all-encompassing. The CDD can engulf military and non-military domains in unison once it is defined by Mallory as a state "*when an opponent has no incentive to initiate or escalate conflict at any given intervention or escalation threshold in any given domain of warfare - both vertically and horizontally within that domain and laterally into one or more additional domains of warfare*" (Mallory, 2018).

For achieving CDD, there is a need for a very elaborate cross-domain integration. With the emergence of new domains, new technologies, and new doctrines – synergized application is becoming ever more quintessential in this regard. The traditional concept of definite boundaries in various domains is greatly altered in the evolving concept of CDD. For achieving a response to multi-domain threats, there is a need to study them in the multi-domain context and their increasing complexities should be addressed using both military and political processes.

Applicability Parameters for Cross-Domain Deterrence

A successful CDD can be claimed to be effective once an actor is not in a position to escalate or has been disincentivized in any domain, while there are no additional opportunities available both horizontally or vertically within the same domain or moving into any another domain laterally. In the discussion and explanation of the CDD, the important aspect of 'domain' and its intricacies are of utmost importance. It can refer to an area (geographical or cognitive), or even it can be an environment and it can also denote a certain sphere of activity or knowledge (Lehman, 2019). A domain may also refer to places where activities are taking place, main activities, or the associated activities. Traditionally, strategic weapons especially nuclear weapons have cross-domain effects due to their lethality and strategic effects, hence, they are considered multi-domain instruments. Delineation of the military and non-military domains is a continuous process and it continues to morph as per the requirements and perceptions of human beings (Lehman, 2019). Traditionally warfare and deterrence were a subject restricted to the military alone and it has various dimensions as per the development of warfare.

Today we speak of additional capabilities and related domains like space, and cyber besides land, sea, and air as primary domains. At times unconventional warfare, special operations, undersea operations, underground operations, and even hybrid war are also discussed as domains for warfare and deterrence. (Lehman, 2019) In the highly interconnected and globalized world, it is no longer the economy that is linked but the states, nations, and governments including the population living in them are interconnected and interdependent. This interconnectivity and interdependency give birth to cross-domain manipulation or CDD and exploitation as well. Political, Social, Economic, Virtual, and Physical domains are some of the areas that are exploitable and interconnected (Greenhill, 2019).

Like classical forms of deterrence, CDD is prone to challenges, and overcoming those and their interplay identifies the applicability parameters. CDD is situational and is to be seen in the overall context of the effects desired. Contingency planning, forward-looking effects cutting into other domains, and requisite infrastructure both physical and cognitive are essential for its application. It is fluid, evolving, and dynamic – the applicability environment needs to embrace it by keeping pace with its fast-moving, cross-cutting, domain-hopping characteristics. CDD can be proactive or reactive, hence the application of CDD is predicated on the corresponding capabilities and applicability parameters. CDD is complex, with both overt and covert means, therefore, it is dependent on the policies and capabilities of the state.

Applicability of Cross-Domain Deterrence

In order to quantify the applicability of CDD, there are some enablers, trends, and drivers relevant to each domain, the interplay and the bargain of these domains help in understanding the CDD. Lindsay and Gartzke, while summarizing the interplay of various domains in their book have created a chart (Table 1) (Lindsay and Gartzke, 2019), which is of immense value to understand the interplay of various domains. The table exhibits how the interplay of different aspects (vertical column) in each domain (horizontal column) creates the effect.

Table 1

(Lindsay and Gartzke, 2019)

Bargaining Characteristics of Various Domains							
	Nuclear	**Land**	**Sea**	**Air**	**Space**	**Cyber**	**Migration**
Barriers to Entry	Higher	Mixed	Higher	Higher	Higher	Lower	Lower
Credible Communication	Higher	Higher	Mixed	Mixed	Mixed	Lower	Higher
Plausible Deniability	Lower	Mixed	Mixed	Mixed	Mixed	Higher	Mixed
Warfighting Potential	Lower	Mixed	Higher	Higher	Higher	Mixed	Negligible
Counterforce Potential	Lower	Mixed	Mixed	Mixed	Lower	Mixed	Lower
Punishment Costs	Extreme	Mixed	Higher	Higher	Lower	Mixed	Higher

In light of the table above, while discussing the barriers to entry in different domains due to economy, technology, and other drivers it would be difficult to initiate a war in different domains. In the second row, credible communication regarding threats and assurances has its own unique characteristics as per the domains and has different standards for different weapons and technologies used in each domain. This can have positive or negative effects on the overall deterrence paradigm. While highlighting the plausible deniability the table identifies that it also differs as per the domains and at times it assists in covert actions or propaganda aspects. As regards war-fighting potential which is purely a military potency largely dependent on the eco-military complex and

strength of states, the effects desired show themselves differently in different domains. In contrast, the aspects needed to counter the effectiveness of the adversary's warfighting potentials i.e., counter force potential also present themselves in a variety. This, however, may not be the same as developing matching capabilities, yet the indirect effects of raising the cost of war are at play. Similarly, the means to raise the cost of war by enhancing or thwarting the punishment costs is also important to note. Hence, it is evident from the interplay of different factors in different domains, that the concept of diversity and a departure from the traditional fixed idea of deterrence is generated which is termed CDD and is radiating plausible acceptance. Its correct understanding would assist in national strategies and international relations.

This concept of CDD is also summarized in another paradigm in a study under the auspices of the Research and Development Corporation United States, where the CDD is identified as an inability to contain the war within the boundaries of a single geographical theater or domain (Mallory, 2017). It is influencing domains of land, air, sea, space, and cyberspace, while it is also transcending into the hybrid warfare and strategies of non-state actors, once it is studied in the context of the US, its allies, and adversaries primarily the strategic competitors i.e., China and Russia. The study ascertained that the conflict would be initiated by a trolling campaign in the cyber domain and it would also be laterally and vertically moving through the hybrid war domain thereby suggesting a terrorist attack, and then it would aim to affect the cyber and space domain targeting the US capabilities of early warning and information. This would then lead to the outbreak of hostilities in the conventional domain while cyber-attacks on critical nerve centers and infrastructure and also the destruction of US satellites are visualized. Then it would be a pre-emptive counterforce attack against US weapons and capabilities and lastly, it would be the nuclear weapon employment (Mallory, 2018).

Suggested Applicability Methodology for CDD

To quantify the capabilities and deterrence in the context of CDD and its applicability in Asia Pacific (US-China and US-North Korea) and IOR comprising (India-China and India-Pakistan) a method has been devised keeping in view certain factors and then grading them accordingly. The grading criteria given below in Table 2 have been devised based on the capabilities and perceived effects as deterrence is a perceptive exercise in itself (Jervis, 1982).

Table 2

Grading Criteria

Grade	Status	Explanation
10	Fully Functional	Fully functional and is the best in the world
8	Optimally Functional	Functional as per the optimal requirements of the user
6	Partially Functional	Functional at the minimum level and is partially effective
4	Acquisition Based	Functional at the minimum level, acquisition-dependent dependent, and partially effective
3	Developmental Stage	It is being developed and radiating effects at the conceptual level, however, no physical effects
2	Conceptual Only	Only conceptual effect can affect future projections
0	Not Existing	Not existing at any levels

In the next step, various factors have been identified primarily affecting deterrence, based on the capabilities, and accordingly the nations would be graded and the net effect calculated which has been used as analysis subsequently. The factors that have been chosen are appended below. The first three aspects are the famous 3Cs used in nuclear deterrence while the other three denote the politico-eco-military interplay. (Peters, Anderson, and Menke, 2018).

- *Capability*. Reflective of how much hardware a nation possesses that can be effective in deterring the adversary.

- *Credibility*. How credible is the capability and how credible is the will to use it (political will of the leadership)?
- *Communication*. Strategic communication on a particular capability in terms of policies, doctrines, and political aims.
- *Research & Development*. Standing in research and development indigenous, collaborative, dependent, or borrowed.
- *Economy*. The economic strength, GDP, and defense spending.
- *National Aims, Aspirations*. The national ideology is reflective of the deterrence potential. Hegemon, net security provider, superpower, global power, regional power, and economic power are a few national aspirations that lead to competition, collaboration, cooperation and even induce severe security dilemmas.

Applicability in Asia Pacific

Asia Pacific houses a variety of nations where the classic strategic competition exists due to a security dilemma, morphing world order, the advent of new technologies, and the effects of nuclear weapons. Important nations engaged in the scope of deterrence are the US-China and US-North Korea. In the Pacific, the US is grappling with eroding deterrence, and a new 'Peace Deterrence Initiative' is also in the offing (Rimland and Buchan, 2020). China with its modernization is inducing a fear that with an increasingly assertive role in the Asia-Pacific, it can dominate the region, can deter and if needed defeat the US (Maizland, 2020). North Korea with its evolving deterrent strategy based on nuclear weapons and Inter Continental Ballistic Missiles (ICBM) is alarming for the US (Bandow, 2020). Japan, Indonesia, and Australia are also important, but the study has focused on the US, China, and North Korea.

United States

As of now US is struggling hard to regain the credibility of its deterrence on a simple principle of 'making China believe that it cannot win'. The element of CDD is visible where having accepted that the US may not be able to deter and defeat China militarily, the US needs to find other solutions (Mattis, 2020). The US is spending more, increasing its budgetary allocations, and focusing on key military capabilities in order to deter China. The US is reorienting towards Asia-Pacific through its Pacific Deterrence Initiative (Inhofe and Jack Reed, 2020)also giving reassurances to its allies. The US is going for a CDD approach where it is investing to make China believe that the US is undefeatable. As of now, the US has a $ 766.6 Bn defense budget, the largest in the world.

Table 3

Assessment for US - Open Source

Domains	Capability (Hardware)	Credibility (Political Will)	Communication (Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
	a	b	C	d	e	F	Sum(a:f)/6
Nuclear	10	10	10	10	10	10	10
Conventional (Land, Air, Sea)	10	10	10	10	10	10	10
Un-Conventional (NSA, Hybrid)	6	3	6	6	10	10	6.8
Cyberspace	10	10	10	10	10	10	10
Space	8	10	8	8	10	10	9
AI	6	8	8	10	10	10	8.6
Information	8	10	8	10	10	10	9

Note: *Data created based on the Analysis Model*

China

China is rapidly modernizing under the banner of the 'China Dream', where reforms have been undertaken regarding defense structures and the integration of modern military equipment (Hein, 2028). China is focusing on developing its arsenal, infrastructure, and information base (Military Balance, 2020) which clearly reflects the concept of multi-domains to win the war. Defense Paper 2019 of China is also reflective of a mindset to take advantage of the situation and develop in all domains. China identifies itself as the competitor of the US, but at no place it is seeking any conflict, it is competing and looking for cooperation and a win-win situation. As per Military Balance 2023, it has the 2nd largest defense budget in the world at $ 242.4 Bn.

Table 4

Assessment for China – Open Source

Domains	Capability (Hardware)	Credibility (Political Will)	Communication (Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
	a	b	c	d	e	f	Sum(a:f)/6
Nuclear	10	10	10	10	10	10	10
Conventional (Land, Air, Sea)	10	10	8	10	10	10	9.6
Un-Conventional (NSA, Hybrid)	6	2	2	2	10	10	5.3
Cyberspace	10	10	10	10	10	10	10
Space	8	10	8	10	10	10	9.3
AI	10	10	10	10	10	10	10
Information	8	10	8	10	10	10	9

Note: *Data created based on the Analysis Model*

North Korea

North Korea after its covert nuclearization and with a strong-willed national leader, has opted to use nuclear and missile deterrence, which till now has been able to play its part to some extent. It is investing in asymmetric capabilities, further diversifying its shorter-range delivery systems, quasi-ballistic missiles, hypersonic glide vehicles, and land-attack cruise missiles (Military Balance, 2023) US termed North Korea as a rogue state as it continues the pursuit of nuclear weapons, missile capabilities, is conducting sophisticated nuclear and Intercontinental Ballistic Missiles tests, thus posing a threat to the US and its allies. In the realm of deterrence, both nuclear states have mutual vulnerabilities and it is not possible to achieve victory either in terms of military or nuclear warfighting (Khan, 2020), hence the concept of CDD is also emerging, while its true defense spending is not known.

Table 5

Assessment for North Korea - Open Source

Domains	Capability (Hardware)	Credibility (Political Will)	Communication(Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
	a	b	c	d	e	F	Sum(a:f)/6
Nuclear	6	10	10	3	4	10	7.1

Domains	Capability (Hardware)	Credibility (Political Will)	Communication(Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
Conventional (Land, Air, Sea)	4	6	6	3	4	8	5.1
Un-Conventional (NSA, Hybrid)	3	3	2	2	4	3	2.8
Cyberspace	4	6	6	4	4	8	5.3
Space	6	8	6	6	4	8	6.3
AI	0	0	0	0	0	0	0
Information	4	8	4	2	4	4	4.3

Note: *Data created based on the Analysis Model*

Quantitative Comparison

Based on the above data, a comparison in Tables 6 and 7 is drawn which identifies the applicability of CDD. Adjoining graphs identify that the US and China are ensuring deterrence in all domains almost equally, hence the concept of CDD is emerging explicitly and no singular capability is predominant from either side. However, once the comparison of the US and North Korea is studied, it is identified that in this dyad, nuclear weapons and asymmetric capabilities are the prime basis for deterrence, especially by North Korea against the US for any unwanted actions, while the US is trying to compel North Korea with its state-of-the-art capabilities in conventional, space and AI as well.

Table 6

US - China Strategic Comparison

	US	China
Nuclear	10	10
Conventional (Land, Air, Sea)	10	9.6
Un-Conventional (NSA, Hybrid)	6.8	5.3
Cyberspace	10	10
Space	9	9.3
AI	8.6	10
Information	9	9

Figure 1

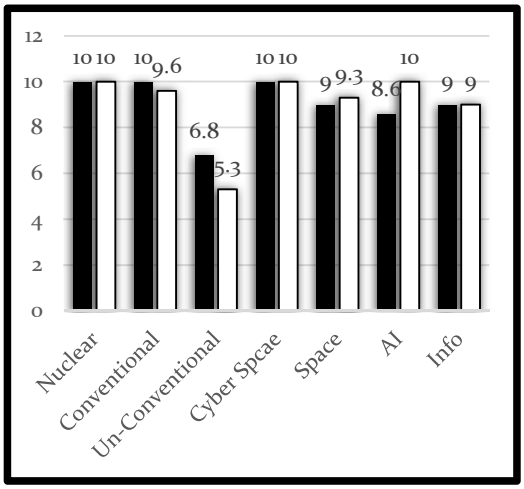
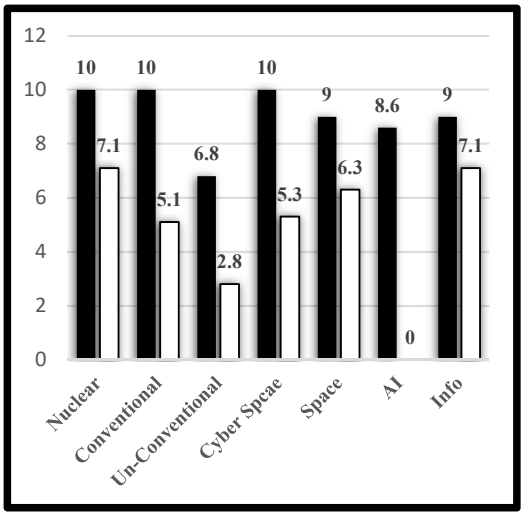


Table 7

US - North Korea Strategic Comparison

	US	NK
Nuclear	10	7.1
Conventional (Land, Air, Sea)	10	5.1
Un-Conventional (NSA, Hybrid)	6.8	2.8
Cyberspace	10	5.3
Space	9	6.3
AI	8.6	0
Information	9	7.1

Figure 2



Applicability of CDD in the Indian Ocean Region

In IOR, the prevailing security environment is a typical security dilemma, in which a state is increasing its own security and reducing the security of the other (Glaser, 2020). IOR typically witnesses the contestation between three nuclear states i.e., Pakistan, India, and China. There are two separate yet intrinsically interconnected power contestations in the region, one, India-China, where India has bilateral differences, regional and global aspirations and is a party to the great power competition (US-China), this dyad of India-China is formed; two, India-Pakistan historical contestation based on geographical issues, morphed due to Indian hegemonism and Pakistan's resilience thus another dyad India-Pakistan emerged in the region. These three nations are nuclear-capable, have highly developed militaries, are amongst the largest defense spenders and two of them are the top economies of the world. Strategic competition in the Asia Pacific has a direct linkage to IOR because the players have common interests in both the oceans and have the potential to entrap others in this as well (Abbassi and Khan, 2020).

China and India are deeply engaged in competing strategies in the Asia Pacific and its effects are reaching the IOR. Both India and China are large growing economies and their interdependence and competitiveness can assist in avoiding the conflict and at the same time could induce a conflict. Sino-U.S. competition and the Indian role in acting as a frontline state for the US or hedging China in the process is exacerbating the situation.

India due to its economic strength and geographical location has been able to become a

frontline state to contain the rise of China, hence, a strategic relationship between India and the US has emerged. Geographically, India shares the contested waters with China, is economically integrated into the world economy, and has become a major US ally benefitting militarily and politically from the US. It has gradually achieved an important position in the strategic equation of the region. India is focusing on building a nuclear triad while it is also creating another triad based on space, cyber, and special operations. Overall, India with a defense budget of $ 66.6 Bn is using all domains to deter adversaries (Military Balance, 2023).

Table 8

Assessment for India - Open Source

Domains	Capability (Hardware)	Credibility (Political Will)	Communication (Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
	a	b	c	d	e	F	Sum(a:f)/6
Nuclear	10	10	8	6	8	8	8.3
Conventional (Land, Air, Sea)	8	8	8	6	8	8	7.6
Un-Conventional (NSA, Hybrid)	8	10	8	8	8	8	8.3
Cyberspace	4	6	6	4	6	6	5.3
Space	8	8	6	8	8	8	7.6
AI	6	6	3	4	6	8	5.5
Information	8	10	10	8	8	8	8.6

Note: Data created based on the Analysis Model

Pakistan struggles for its national security and upkeep of its national aims and aspirations. Conflict between India and Pakistan is deeply rooted based on the territory of Kashmir (Lamb, 1991), and subsequently it has also transformed due to the ongoing contestation(s) and competition(s) in political, diplomatic, and military spheres. The strategic competition in the IOR between China and the US has its linkages and impact on the strategic stability and deterrence in the IOR. Pakistan is an important player in the region and possesses a strong conventional military capability backed by nuclear and strategic arsenal (missiles) with a defense budget of $ 9.8 Bn. (Military Balance, 2023). The table below is the quantitative assessment for Pakistan from the opensource data which is reflective of its capabilities in various domains.

Table 9

Assessment for Pakistan - Open Source

Domains	Capability (Hardware)	Credibility (Political Will)	Communication (Doctrines, Policies)	Research and Development (Indigenous)	Economy (GDP Strength)	National Aims / Aspiration (Strategic Competition)	Net Effects (Sum Total of all aspects)
	a	b	C	d	e	F	Sum(a:f)/6
Nuclear	8	8	10	8	4	10	8

Conventional (Land, Air, Sea)	4	10	10	4	4	8	6.6
Un-Conventional (NSA, Hybrid)	6	6	6	4	6	6	5.6
Cyberspace	4	4	4	3	3	6	4
Space	3	6	6	3	6	8	5.3
AI	2	4	2	2	4	4	3
Information	6	6	6	6	6	8	5.3

Note: *Data created based on the Analysis Model*

Based on the data, a comparison in Tables 10 and 11 is drawn to ascertain applicability of CDD. India and China have matching capabilities and a semblance of CDD is emerging, however, in the context of Pakistan and India, the classical application of CDD has yet not fully emerged.

Figure 2

Table 11
Pakistan -India Strategic Comparison

	Pak	India
Nuclear	8	8.3
Conventional (Land, Air, Sea)	6.6	7.6
Un-Conventional (NSA, Hybrid)	5.6	8.3
Cyberspace	4	5.3
Space	5.3	7.6
AI	3	5.5
Information	5.3	8.6

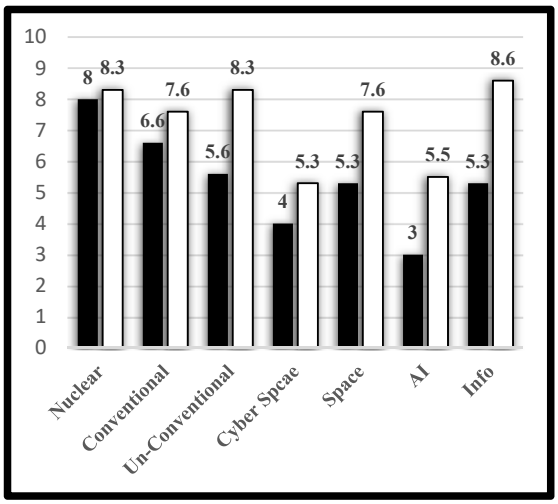
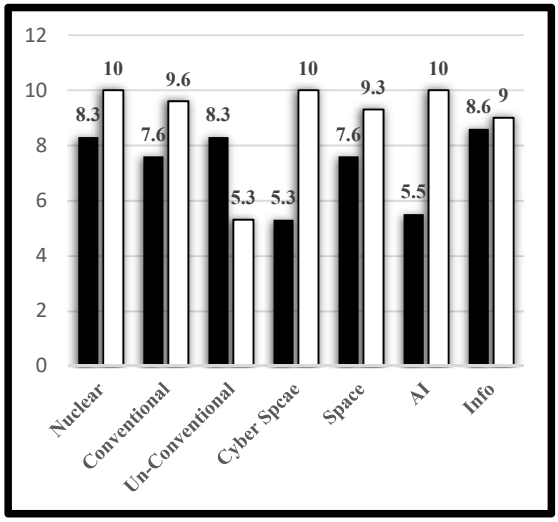


Table 10
India -China Strategic Comparison

	India	China
Nuclear	8.3	10
Conventional (Land, Air, Sea)	7.6	9.6
Un-Conventional (NSA, Hybrid)	8.3	5.3
Cyberspace	5.3	10
Space	7.6	9.3
AI	5.5	10
Information	8.6	9



Conclusion

The nature of the times old concept of deterrence remains unaltered even today. CDD is an emerging and evolving phenomenon. It existed in various forms previously, however, its improved expression in the broader military domain was observed in the last decade. The complexities of emerging technologies, the advancement in the concept of domains, interconnectivity, and interdependence of domains and technologies make CDD a reality. The desire of nations to acquire, modernize, and complete the nuclear triad underlines the importance that nuclear weapons enjoy. The lethality and effects of nuclear weapons in terms of destruction are far superior to any other arsenal. Conversely, it is this lethality and effects that preclude the use of nuclear weapons and avoidance of nuclear warfighting – hence giving precedence to other technologies to coerce an opponent (with more possibility of its use as compared to nuclear) thus yielding space to CDD.

All the latest technologies are in a very strong position to affect the strategic stability equation. It is because of the dependency, unavoidable connectivity, and linkages that new technologies have disruptive potential on the erstwhile sole owner of deterrence –nuclear power. Space, cyberspace, Artificial Intelligence, and hypersonic weapons (in various combinations) have the potential to alter strategic stability. CDD is rapidly becoming the new face of deterrence especially in the military domain. Disruptive potential needs to be harnessed and can be used by developed states to answer the asymmetric responses of underdeveloped states and vice versa. The speedy development(s) in the latest technologies and their disruptive nature merits attention by strategists, academia, and practitioners to review the existing policies and doctrines in line with the emerging realities.

References

Abbassi, R & Khan, Z., (2020). *Nuclear Deterrence in South Asia: New Technologies and Challenges to Sustainable Peace.* Routledge,
Google Scholar Worldcat Fulltext

Bandow, D., (2020). Why North Korea Needs its Nukes. *Foreign Policy*
Google Scholar Worldcat Fulltext

Bruusgaard, K. V., (2016). Russian Strategic Deterrence. *Survival* 58 (4), 7-26.
Google Scholar Worldcat Fulltext

Clausewitz, C. V., (1984) *On War*, Princeton University Press.
Google Scholar Worldcat Fulltext

Cox, Jessica. (2020), Nuclear Deterrence Today. *NATO Review*
Google Scholar Worldcat Fulltext

Dawkins, J. C., (2019). *Rising Dragon: Deterring China in 2035*. US Air University Montgomery.
Google Scholar Worldcat Fulltext

Defense of Japan (2019), Ministry of Defence Japan.

Freedman, L. (2004). *Deterrence*. Polity Press.
Google Scholar Worldcat Fulltext

Glaser, C. (2011). Will China's Rise Lead to a War? Why Realism does not mean Pessimism. *Foreign Affairs90* (2), 82. https://www.jstor.org/stable/25800459
Google Scholar Worldcat Fulltext

Greenhill, K. M., (2019). Weaponizing People as Nonmilitary Instruments of Cross-Domain Coercion. In Lindsay J. R. & Erik Gartzke (Eds) *Cross Domain Deterrence: Strategy in Era of Complexity*. Oxford University Press.https://doi.org/10.1093/oso/9780190908645.003.0012
Google Scholar Worldcat Fulltext

Hauser, B. (2010). *The Evolution of Strategy: Thinking War from Antiquity to the Present*. Cambridge University Press.
Google Scholar Worldcat Fulltext

Hein, M. V. (2018). Xi Jinping and the Chinese Dream. *DW*. https://www.dw.com/en/xi-jinping-and-the-chinese-dream/a-43685630.
Google Scholar Worldcat Fulltext

Inhofe, J. & Reed, J., (2020). The Pacific Deterrence Initiative: Peace through Strength in the Indo-Pacific. *War on the Rocks*. https://warontherocks.com/2020/05/the-pacific-deterrence-initiative-peace-through-strength-in-the-indo-pacific.
Google Scholar Worldcat Fulltext

Jaffery, S. A. Z., (2020), *Enhancing Deterrence Stability on the Subcontinent: The Case for Conventional Deterrence*. Stimson.
Google Scholar Worldcat Fulltext

Jervis R., (1982). Deterrence and Perception. *International Security7* (3), 3-30.https://doi.org/10.2307/2538549
Google Scholar Worldcat Fulltext

Keohane, R. O. & Nye, J.S., (2012), *Power and Interdependence.* Longman.
Google Scholar Worldcat Fulltext

Khan, Z., (2020). North Korean Nuclear Learning under the Essentials of Nuclear Revolution: Cooperative Mechanics for Stabilizing the Korean Peninsula. *East Asia*. https://doi.org/org/10.1007/s12140-020-09338-7
Google Scholar Worldcat Fulltext

Krepon, M., (2015) et al (eds.), *Deterrence Instability and Nuclear Weapons in South Asia* Stimson Center.
Google Scholar Worldcat Fulltext

Lamb, A. (1991). *Kashmir: A Disputed Legacy 1846-1990*. Oxford University Press.
Google Scholar Worldcat Fulltext

Lehman, R.(2019). Simplicity and Complexity in the Nth Nuclear Era. In Lindsay J. R. & Erik Gartzke (Eds) *Cross-Domain Deterrence: Strategy in Era of Complexity*. Oxford University Press.https://www.jstor.org/stable/26271621
Google Scholar Worldcat Fulltext

Liddy, L., (2004).The Strategic Corporal. *Australian Army Journal* 11 (2), 139-148.
Google Scholar Worldcat Fulltext

Lindsay, J. R., &Gartzke, E. (2019) *Cross-Domain Deterrence: Strategy in an Era of Complexity.* Oxford University Press.
Google Scholar Worldcat Fulltext

MaizlandL., (2020). China's Modernizing Military. *Council on Foreign Relations*. https://www.cfr.org/backgrounder/chinas-modernizing-military.
Google Scholar Worldcat Fulltext

Mallory, K., (2018). *New Challenges in Cross-Domain Deterrence.* RAND Corporation.
Google Scholar Worldcat Fulltext

Nye Jr, J. S. (2009). Get Smart, Combining Hard and Soft Power. *Foreign Affairs* 88 (4), 160-163. https://doi.org/10.1007/978-981-99-0714-4_8
Google Scholar Worldcat Fulltext

Overholt, W.H., (2012). *Asia, America and the Transformation of Geo-politics* .Cambridge University Press.
Google Scholar Worldcat Fulltext

Patrick, S. M., An Open World Is in the Balance. What Might Replace the Liberal Order? *Worlds Politics Review,*https://www.worldpoliticsreview.com/articles/20868/an-open-world-is-in-the-balance-what-might-replace-the-liberal-order.
Google Scholar Worldcat Fulltext

Peters R, Anderson J, &Manke H., (2018). Deterrence in the 21st Century: Integrating Nuclear and Conventional Force. *Strategic Studies Quarterly* 12 (4), 15-43.
Google Scholar Worldcat Fulltext

Rimland, B. & Buchan, P., (2020). Getting the Pacific Deterrence Initiative Right. *The Diplomat*, https://thediplomat.com/2020/05/getting-the-pacific-deterrence-initiative-right.
Google Scholar Worldcat Fulltext

Sweijs&Zilincik, (2019). *Cross Domain Deterrence and Hybrid Conflict*. The Hague Centre for Strategic Studies.
Google Scholar Worldcat Fulltext

US Department of Defence, (2020). *Nuclear Deterrence: America's Foundation and Backstop for National Defense*. Pentagon Press.
Google Scholar Worldcat Fulltext

US Department of Defence, (2018). *Remarks by Secretary Mattis on National Defense Strategy*. https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1702965/remarks-by-secretary-mattis-on-national-defense-strategy.
Google Scholar Worldcat Fulltext

Vince, R. J., (2015). *Cross-Domain Deterrence Seminar Summary Notes*, https://www.slideshare.net/LivermoreLab/summary-notes-47797997.
Google Scholar Worldcat Fulltext

Walker, C. & Ludwig, J., (2017). The Meaning of Sharp Power. *Foreign Affairs.*https://doi.org/10.4467/20801335PBW.21.032.14309
Google Scholar Worldcat Fulltext

Westerheide, F. J. G., (2020). China the First Intelligence Super Power. *Forbes*.
Google Scholar Worldcat Fulltext