Cross-Domain Dynamics and the Effect on Aggression, Escalation, and Deterrence in a Nuclear Environment

Hector Velasco
Naval Postgraduate School
hector.velasco.ctr@nps.edu

I. INTRODUCTION

Cross-domain dynamics (CDD) refers to the interaction of military operations across traditional and emerging domains, such as land, sea, air, space, and cyberspace. It is a relatively new concept, as it has emerged in response to the increasing interconnectedness of these domains and the development of new military capabilities that can operate across multiple domains.

CDD has the potential to significantly impact aggression, escalation, and deterrence in a nuclear environment. For example, an adversary could use cyberattacks to disable or disrupt nuclear command and control systems or launch disinformation campaigns to undermine public confidence in nuclear deterrence. Also, an adversary could use space-based capabilities to degrade nuclear early warning systems, conduct anti-satellite attacks, or even target ground segment infrastructure.

The following are examples of how CDD could affect aggression, escalation, and deterrence:

- *Aggregation of effects*: Adversaries could use cross-domain attacks to aggregate effects across multiple domains, making it difficult for defenders to attribute the attacks and to respond effectively. For example, an adversary could launch a simultaneous cyberattack on nuclear command and control systems and a kinetic attack on conventional forces, in an attempt to overwhelm the defender.
- *Miscalculation*: CDD can make it difficult for adversaries to assess each other's intentions and capabilities. This can lead to miscalculation and the unintended escalation of conflict. For example, a defender might misinterpret a limited cross-domain attack as a prelude to a nuclear attack, and launch a preemptive nuclear strike in response.
- *Deterrence erosion*: Attacks that go beyond traditional warfare, like hacking into a country's nuclear control system, can make that country less likely to use its nuclear weapons. For example, if an enemy country could disable or disrupt a nuclear command and control system, the country being attacked might not be sure it could strike back. This could make the enemy country more likely to act with more confidence and aggressively.

CDD and its effects in a nuclear environment are of paramount importance for several reasons. Due to it being a new concept, there is still much that we do not understand about its implications for nuclear deterrence. Second, the increasing interconnectedness of the traditional and emerging domains of warfare makes CDD increasingly relevant to nuclear deterrence. Third, the development of new military capabilities that can operate across multiple domains makes it possible for adversaries to carry out cross-domain attacks that could undermine nuclear deterrence.

II. CROSS-DOMAIN DYNAMICS

Cross-domain dynamics is a term used to describe the interplay of military operations across traditional and emerging domains of warfare. Traditional domains include land, sea, and air, while emerging domains include space and cyberspace. [6]

CDD differs from traditional warfare in several ways. First, it involves the integration of military operations across the traditional domains. This can be achieved through the use of new technologies, such as hypersonic missiles and artificial intelligence, which can operate across domains. Second, CDD is characterized by the increasing blurring of

the lines between war and peace. This is because adversaries can use non-military means, such as cyberattacks and disinformation campaigns, to achieve their objectives in the cross-domain environment.

Several instances of CDD illustrate the potential challenges and impacts in various strategic scenarios:

In one scenario, an adversary could leverage a sophisticated cyberattack to cripple a defender's satellite navigation system. This act of digital aggression would effectively disable the defender's ability to precisely navigate its air and sea forces, jeopardizing critical nuclear deterrence missions. With compromised navigational capabilities, the defender's air and naval units could experience significant delays, navigate inaccurate routes, or even become completely disoriented, potentially impeding their ability to respond swiftly and effectively in the event of a nuclear attack. This scenario underscores the escalating role of cyberwarfare in modern nuclear dynamics and the need for robust cyber defenses to protect critical infrastructure upon which the effectiveness of nuclear deterrents centers.

In a different context, an adversary could initiate a disinformation campaign aimed at fostering division within a defender's populace. This strategic move has the potential to erode public support for the overall war effort.

Also, the deployment of missiles by an adversary could be leveraged to target the critical infrastructure of a defender. This could encompass vital components such as power grids and telecommunication networks, thereby incapacitating the defender's operational capabilities significantly.

CDD poses several challenges for deterrence. For example, it can make it difficult for defenders to attribute attacks and respond effectively. It can also make it difficult for defenders to assess an adversary's intentions and capabilities, which can lead to miscalculation and the inadvertent escalation of conflict.

‘CDD can thus be likened to a game of “rock, paper, scissors” where different capabilities have different relative strengths and weaknesses depending on the context of their use’ [4]. Overall, it is a complex and challenging phenomenon that has significant implications for warfare and deterrence in the 21st century.

III. AGGRESSION, ESCALATION AND DETERRENCE

In the context of a nuclear environment, aggression means any action by an opponent that could be seen as a threat to use nuclear weapons or that accidentally leads to their use. Aggression can happen in different ways, equivalent to building up military forces near a country with nuclear weapons, launching cyberattacks on systems controlling nuclear commands, spreading false information to shake public trust in nuclear deterrence, or making explicit or implicit threats to use nuclear weapons.

Escalation is when a conflict between countries with nuclear weapons becomes more intense and causes more harm. This can happen because of various reasons, such as not understanding the other side's intentions, feeling pressure from citizens to react strongly to an attack, or wanting to win in a conflict even if it means taking the conflict to a higher level.[2]

Deterrence refers to the ability of a nuclear-armed adversary to prevent the other side from using nuclear weapons against them. Deterrence is based on the principle of mutually assured destruction (MAD), which holds that if either side uses nuclear weapons, both sides will be destroyed. [5]

The relationship between aggression, escalation, and deterrence in a nuclear context is complex and interdependent. Aggression can lead to escalation, which can in turn lead to the use of nuclear weapons. Deterrence can help to prevent aggression and escalation, but it is not a perfect method that guarantees it.

For example, if an adversary believes that they can use nuclear weapons to achieve a decisive victory in a conflict, they may be more likely to use those weapons, even if they know that they will be destroyed in retaliation. This is known as the "use-it-or-lose-it" dilemma. [4]

Another challenge to deterrence is the risk of miscalculation. If an adversary misinterprets a defender's actions as aggression, they may launch a preemptive nuclear strike. This is known as the "stability-instability paradox." [10]

Despite these challenges, deterrence remains an essential element of nuclear security. It helps to prevent nuclear-armed adversaries from using nuclear weapons against each other, and it supports to maintain a stable and peaceful international order.

IV. RELEVANCE TO CURRENT EVENTS

Recognizing how military operations interact across domains, CDD is crucial for tackling modern security challenges. This increasing significance results from various factors, such as the blurring of boundaries in traditional domains, the rise of new military capabilities, and the appearance of non-government actors.

In light of these developments, CDD has become a critical consideration for policymakers and military strategists. Understanding the complex interactions between the different domains is essential for developing effective defense strategies and deterring potential adversaries.

The following are examples of how CDD is taking place in current events, even when not in a nuclear context:

- *Russia's invasion of Ukraine*: Russia has employed a range of cross-domain tactics in its invasion of Ukraine, including cyberattacks, airstrikes, and ground maneuvers. This highlights the need for Ukraine and its allies to develop integrated defense capabilities that can effectively address threats across multiple domains.[7]
- *China's growing military capabilities:* China has made significant investments in developing advanced military technologies, including intercontinental ballistic missiles, hypersonic missiles, and anti-satellite weapons. China has more than 500 operational nuclear warheads as of May 2023. This poses a challenge to the continental United States, Hawaii, and Alaska, which must adapt its defense posture to counter these threats. [8]
- *Iran's use of drones and cyberattacks*: Iran has used drones and cyberattacks to target its adversaries, including Saudi Arabia and Israel. These attacks have demonstrated Iran's ability to conduct cross-domain operations.[1]
- *The rise of cybercrime*: Cyberattacks have become increasingly sophisticated and widespread, targeting critical infrastructure, financial institutions, and government systems. This underscores the importance of cross-domain collaboration between defense and civilian agencies to address cyber threats. [1]

Understanding how CDD are used in military conflicts is key for devising effective strategies to counter these emerging threats. In a world that is becoming more interconnected and technologically advanced, the capability to operate and comprehend complexities across various domains is essential for safeguarding national security.

Measuring aggression across domains that influence nuclear deterrence and escalation management is a complex challenge. There is no single metric that can accurately capture the full range of aggressive actions that can be taken in the cross-domain environment. However, there are a number of indicators that can be used to assess the level of aggression across domains.

Some of these indicators include but not limited to:

- *Military deployments and exercises*: The deployment of military forces near a nuclear-armed adversary's borders or the conduct of military exercises that simulate an attack on a nuclear-armed adversary can be seen as indicators of aggression.
- *Cyberattacks*: Cyberattacks on critical infrastructure, such as power grids and telecommunications networks, or nuclear command and control systems can also be seen as indicators of aggression.
- *Disinformation campaigns*: Disinformation campaigns aimed at undermining public confidence in nuclear deterrence or at sowing discord among a nuclear-armed adversary's population can also be seen as indicators of aggression.

- *Threats to use nuclear weapons*: Any threat to use nuclear weapons, either explicit or implicit, can be seen as an indicator of aggression.

It is important to note that not all of these indicators will be present in every case of aggression. Additionally, the significance of each indicator will vary depending on the context. For example, a military deployment near a nuclear-armed adversary's borders may be more significant if it is accompanied by other indicators of aggression, such as cyberattacks or disinformation campaigns.

Another challenge to measuring aggression across domains is that it can be difficult to attribute attacks to specific factors. This is especially true in the cyber domain, where adversaries can use sophisticated methods to disguise their identities.

Even in light of these difficulties, there are several efforts underway to develop tools and methods for measuring aggression across domains. These efforts are essential for developing effective strategies to deter aggression and manage escalation in the cross-domain environment.

We need to note that no single indicator can provide a complete picture of aggression across domains. It is necessary to consider all of the indicators together, as well as the context in which they occur, to make an accurate assessment of the level of aggression and therefore for retaliation.

Additionally, it is critical to distinguish between aggression and deterrence to develop effective strategies for deterrence and escalation management. Deterrence is a legitimate and necessary tool for preventing war and maintaining peace and security. However, aggression is a hostile act that can lead to escalation and conflict. It warrants serious consideration to be able to distinguish between these two different types of behavior.

In a cross-domain context, a variety of strategies may be employed to effectively manage escalation and enhance deterrence. These strategies encompass the following:

- *Clarity of Communication*: Antagonistic parties must possess a lucid comprehension of each other's delineated thresholds for escalation and red lines. This objective can be attained through the consistent and unambiguous exchange of information, both in public and through private channels.

- *Transparency:* The divulgence of pertinent information about military capabilities and intentions serves to mitigate distrust and the potential for misinterpretation amongst adversarial entities. This objective can be realized through the implementation of measures such as confidence-building initiatives and initiatives promoting defense openness.[3]

- *Crisis Management*: The establishment of effective mechanisms for crisis management is pivotal in averting the transformation of minor incidents into larger-scale conflicts. This entails the delineation of clear communication channels and the formulation of protocols facilitating de-escalation.[3]

- *Resilience:* The fortification of defenses against cross-domain incursions serves to dissuade acts of aggression and complicates the realization of adversaries' objectives. This goal is pursued through the implementation of measures including redundancy, fortification, and deceptive tactics.

- *Deterrent Capabilities:* The maintenance of a credible deterrent posture assumes paramount importance in forestalling acts of aggression and overseeing escalation dynamics. This encompasses the possession of a diversified array of capabilities, capable of imposing costs deemed intolerable upon any potential aggressor contemplating an attack.[3]

In addition to these general strategies, several measures can be taken to manage escalation and improve deterrence in specific domains. For example:

Cyber domain: In the cyber domain, countries can cooperate to develop norms and rules of behavior, and to establish mechanisms for responding to cyberattacks. Countries can also invest in cyber defenses to protect their critical infrastructure and military systems.

Space domain: In the space domain, countries can cooperate to develop norms and rules of behavior for space operations. Countries can also invest in space situational awareness and space defenses to protect their space assets.

Nuclear domain: In the nuclear domain, countries can cooperate to reduce the risk of nuclear war. This can be done through measures such as arms control treaties, confidence-building measures, and crisis management mechanisms.

To date, there is no single solution to managing escalation and improving deterrence in a cross-domain environment. A combination of different strategies and measures will be needed to address the complex challenges posed by this new era of warfare. [11]

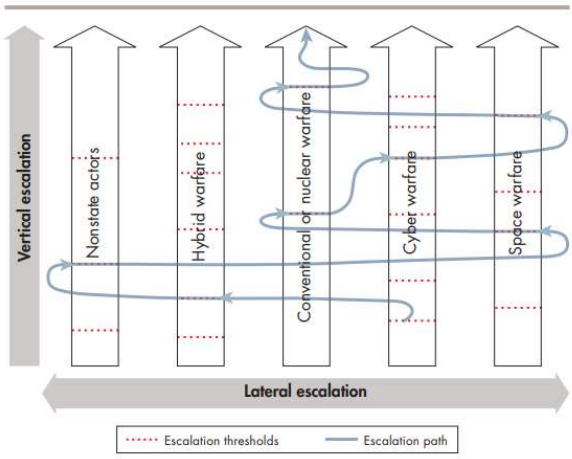

Figure 1 Cross-Domain Escalation Path (New Challenges in Cross-Domain Deterrence, RAND Corp)

V. THE NUCLEAR ENVIRONMENT

The nuclear realm presents a series of distinctive challenges about deterrence and stability, encompassing the following aspects:

The unparalleled destructive potential of nuclear armaments renders them the most formidable weapons ever devised. A singular nuclear weapon can inflict mass casualties, decimate entire urban centers, and unleash unparalleled devastation. This potency imbues nuclear deterrence with a high degree of inherent risk, as a breakdown in deterrence could yield catastrophic consequences of unprecedented magnitude

Next, the compressed timeframes associated with nuclear decision-making engender a profound challenge. Decision-makers in the nuclear sphere may find themselves confronted with mere minutes or even seconds to discern the appropriate course of action in response to a perceived threat. This abbreviated temporal window complicates endeavors to forestall misjudgments and inadvertent escalations, heightening the complexity of navigating nuclear contingencies.

Additionally, ascertaining the true intentions of nuclear-armed adversaries presents a formidable challenge, predominantly in the cyber domain. Adversaries can employ sophisticated tactics to cloud their identities and motives, rendering it arduous to establish a foundation of trust and foster conditions beneficial to stability. The resultant lack of transparency exacerbates the intricacies associated with maintaining a balanced and secure nuclear environment.

Lastly, there's a worry about accidental nuclear conflicts, even when countries don't intend to use nuclear weapons. Things like technical problems, mistakes by people, and wrong calculations can make the chance of accidental nuclear fights higher. This provides a compelling case for the criticality of this matter and works diligently to reduce risks in the context of nuclear deterrence and stability.

In addition to these challenges, the nuclear environment is also becoming increasingly complex and dynamic. The emergence of new military technologies, such as hypersonic missiles and artificial intelligence, is making it more difficult to maintain deterrence and stability.

The introduction of hypersonic weapons raises concerns about the potential for destabilizing the nuclear balance. The speed and maneuverability of these weapons could make it possible for one side to launch a disarming first strike that would neutralize the other side's nuclear arsenal before it could retaliate. This could lead to a situation where both sides feel compelled to launch a preemptive strike in a crisis, increasing the risk of accidental nuclear war.

Examining the challenges outlined earlier reveals specific instances of how they might impact deterrence and stability in the nuclear environment. The powerful destructive capacity of nuclear weapons, while potentially fostering caution in their use, also introduces the possibility of a preemptive nuclear strike if a party perceives losing a conventional war. The compressed timeframes for nuclear decision-making elevate the likelihood of miscalculations and escalation, such as misinterpreting a nuclear exercise as preparations for an attack, prompting a preemptive nuclear response.

Also, the intricate task of verifying nuclear intentions poses difficulties in building trust and maintaining stability among nuclear-armed adversaries, potentially heightening tensions and the risk of conflict. The perpetual concern of accidental nuclear war is exemplified by scenarios like technical failures in nuclear early warning systems, which could generate false alarms triggering unintended nuclear launches. These examples underscore the intricate web of challenges impacting the delicate balance of deterrence and stability in the nuclear realm.

It is important to note that these are just some of the challenges posed by the nuclear environment to deterrence and stability. The nuclear environment is complex and dynamic, and many other factors could impact deterrence and stability.

VI. IMPLICATIONS FOR POLICYMAKERS

Policymakers should consider the following recommendations for mitigating the risks associated with CDD in the nuclear environment:

Firstly, emphasis should be placed on enhancing communication and transparency between adversaries. This involves the establishment of clear and consistent communication channels to diminish the likelihood of miscalculation and inadvertent escalation. Additionally, efforts should be made to augment transparency regarding military capabilities and intentions. This objective can be pursued through the implementation of confidence-building measures and initiatives promoting defense openness.

Secondly, countries must collaborate in formulating norms and rules of behavior governing cross-domain operations. Such cooperative endeavors are integral in diminishing the likelihood of conflict and escalation. For instance, countries could collectively commit to refraining from employing cyberattacks to target nuclear command and control systems.

Additionally, countries are urged to allocate resources towards bolstering capabilities geared towards deterring cross-domain attacks and ensuring an effective response in the event of an attack. This includes investments in cyber defenses, the enhancement of space situational awareness, and the development of hypersonic weaponry.

Lastly, a robust focus should be placed on reinforcing crisis management mechanisms. Countries should have in place effective protocols and communication channels designed to prevent minor incidents from escalating into larger-scale conflicts, thereby facilitating timely and controlled de-escalation.

In addition to general recommendations, policymakers have specific actions they can take to lessen the risks from CDD in the nuclear environment. For instance, to lower the chances of cyberattacks on nuclear command and control systems, policymakers can invest in cybersecurity, reinforce critical infrastructure, and create plans for unexpected situations. In addressing space-based attacks, strategies can be developed by investing in space situational awareness, establishing defenses in space, and collaborating with allies for coordinated responses.

Regarding the risks associated with hypersonic weapons, policymakers can handle them by creating defenses against hypersonic attacks, coordinating responses with allies, and having discussions with adversaries to lower the chance of misunderstandings and escalations.

By taking these and other measures, policymakers can help to mitigate the risks posed by these dynamics in the nuclear environment and to maintain peace and security.

It is important to note that there is no single solution to mitigate the risks presented by CDD in the nuclear environment. Policymakers will need to adopt a comprehensive approach that includes a combination of different measures.

VII. CONCLUSIONS

In the contemporary landscape of warfare and deterrence, the intricate phenomenon of CDD presents a formidable challenge with far-reaching implications. For 21st-century policymakers and military strategists, comprehending the intricacies and nuances of this multifaceted concept is of paramount importance. It is imperative to devise comprehensive strategies aimed at alleviating the associated risks.

One instrumental approach to mitigating the inherent risks of CDD entails the enhancement of communication and transparency among nuclear-armed adversaries. This strategic initiative serves to diminish the probability of critical errors in judgment and inadvertent escalation. By fostering a climate of clear and consistent dialogue, the potential for misinterpretation and miscalculation is substantially reduced.

A parallel avenue towards risk mitigation in the realm of CDD lies in the strategic investment in cross-domain deterrence capabilities. This encompasses a range of endeavors, including fortifying cyber defenses, augmenting space situational awareness, and developing cutting-edge hypersonic weaponry. Such initiatives strengthen a nation's ability to deter and respond effectively to cross-domain threats, thereby contributing to the maintenance of stability and security in an evolving global context.

In addition, it is also important to consider that cross-domain dynamics is not just a challenge for nuclear-armed countries. It is also a challenge for non-nuclear-armed states. This is because non-nuclear-armed states can also be targeted by cross-domain attacks, and they may not have the same capabilities to deter or respond to these attacks as nuclear-armed states.

As a result, it is important for all states to work together to develop norms and rules of behavior for cross-domain operations. This is essential for reducing the risk of conflict and escalation in the cross-domain environment.

VIII. REFERENCES:

[1] Director of National Intelligence. Annual Threat Assessment of the U.S. Intelligence Community. DNI, 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

[2] RAND Corporation. Dangerous Thresholds: Managing Escalation in the 21st Century. RAND Corporation, 2008. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf

[3] Fruhlin, Stephan and O'Neil, Andrew. *Alliances, Nuclear Weapons and Escalation: Managing Deterrence in the 21st Century*. Australian National University, 2021.

[4] Lindsay, Jon and Gartzke, Erik. *Cross Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press, 2019

[5] Drewien, Celeste. *Cross-Domain Deterrence*. Sandia National Laboratories, 2019. https://www.osti.gov/servlets/purl/1644932
[6] Institute for National Strategic Studies. *Deterrence and Escalation in Cross-Domain Operations Where do Space and Cyberspace fit?* INSS, 2011. https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf
[7] RAND Corporation. *Anticipating Adversary Military Interventions*. RAND Corporation, 2021 https://www.rand.org/content/dam/rand/pubs/research_reports/RRA400/RRA444-1/RAND_RRA444-1.pdf
[8] US Department of Defense. *DOD Report Details Chinese Efforts to Build Military Power*. DOD News, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3562442/dod-report-details-chinese-efforts-to-build militarypower/
[9] Scott D. Sagan. *The Nuclear Necessity Principle*. Ethics Matter Interview series, 2017. https://www.carnegiecouncil.org/media/series/gt/20170804-scott-sagan-nuclear-necessity-principle
[10] The SAGE Encyclopedia of Political Behavior. *Stability-Instability Paradox*. NPS, 2017 https://nps.edu/documents/105858948 /106279825/Kapur_Sage+Encyclopedia_Stability-Instability_OCt17/c7952c37-2f5d-4462-9630-5bff04f6cd8f
[11] RAND Corporation. *New Challenges in Cross-Domain Deterrence*. RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf.