A New Interpretation of Integrated Deterrence: Physical and Virtual Strategies

Jim Q. Chen
U.S. Department of Defense National Defense University, Washington, DC. USA

jim.chen@ndu.edu

Abstract: The integrated deterrence strategy, backstopped by nuclear deterrent, calls for seamless collaboration in deterrence across warfighting domains, using all instruments of national power, and with allies and partners. Being a warfighting domain and being closely related to the information instrument of national power, the cyber domain should certainly be included, and cyber deterrence should play a significant role in the integrated deterrence strategy. Nevertheless, as cyber deterrence seems not to be as effective as it is expected at least currently, some scholars and practitioners doubt its mere existence, not mentioning the role that it can play in the integrated deterrence strategy. This paper argues that not having deterrence in cyberspace leaves a blank spot in the strategy since some critical functionality of deterrence in cyberspace cannot easily be replaced. By recognizing the unique strategic context of cyberspace, the paper maintains that deterrent effect can actually be achieved in unique ways in this space. To further explore the unique role that deterrence in cyberspace plays within the integrated deterrence strategy, this paper proposes a multi-level and multi-aspect architecture for integrated deterrence strategy. This novel architecture is able to cover varied levels of strategic environments both below and above the threshold of armed conflict. It is also able to correlate varied deterrent measures with varied strategic environments categorized via various aspects, such as diplomacy, information, military, economy, etc. This paper shows that the inclusion of deterrence in cyberspace can empower the strategy by making the strategy flexible enough in tackling various challenges. Eventually, the strategy can make its contribution in preventing war and maintaining peace.

Keywords: Strategies, integrated deterrence, deterrence in cyberspace, multi-level and multi-aspect architecture, strategic contexts

1. Introduction

Deterrence is used to prevent war and maintain stability. It is an important means in the military instrument of national power. In the Joint Publication 3-0, *Joint Operations*, it is defined as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/belief that the cost of action outweighs the perceived benefits." (The Joint Staff, 2011).

Kahn (1960), Schelling (1960), and Schelling (1966) are the pioneers of the deterrence theory. Kahn's work lays the foundation for deterrence-by-denial strategy, while Schelling's work lays the foundation for deterrence-by-punishment strategy. These two strategies, focused on nuclear deterrence, have shaped the current strategies regarding strategic stability. Payne (2008) provides a good explanation of these two strategies. In the cyber era, cyberspace has been created based on the physical sphere. One may certainly wonder whether deterrence can also be applied in cyberspace. If it does, to what degree it can be applied. If it does not, what other measures can be used in cyberspace.

Since it is very hard to create a virtual impact that can reach the level of nuclear deterrence, some scholars and practitioners question the mere existence of deterrence in cyberspace, not mentioning the role that it can play in the integrated deterrence strategy. One example is Harknett and Smeets (2020), in which they discuss the reasons for the failure of cyber deterrence as well as other measures that can be used in supporting some functionalities needed for cyber operations. Smeets (2020) further discusses the use of the replacement strategies such as persistent engagement and defend forward. Nevertheless, other scholars and practitioners insist on the pursuit of deterrence in cyberspace, as the crucial role of deterrence is not replaceable in their view. Healey (2019) points out the challenges in defend forward. Libicki (2009), Nye (2017), Chen (2017), Chen (2018a), Libicki (2021), and others argue for deterrence in cyberspace as well as its role in supporting national security. For instance, Libicki (2021; 2009) argues for cyber deterrence. He discusses the difference among cyber deterrence, nuclear deterrence, and criminal deterrence.

It needs to be pointed out that both schools of thoughts have some valid points in their arguments. Nonetheless, a solution that can be accepted by both sides is hardly to be reached, especially when the discussion is only focused on cyberspace.

To address this challenge, it is worthwhile to have a better understanding of the goal and the essential components of deterrence. The goal of deterrence is to force deterrent targets to give up their current aggressive commitment or at least restrain their behavior. In other words, it is to change the decision-making

calculus of deterrent targets. This is likely to happen when the following conditions are met: (1) The deterrent targets see no significant gains but only high costs in their commitment. (2) They are overwhelmed with fear and anxiety after they see no chance of changing the upcoming results and after they realize that the unavoidable consequences will threaten their survival and/or reputation. Art and Greenhill (2018) describe how coercion can lead to the change of an opponent's behavior. Brodie (1946) holds that atomic weapons are not made for use but to keep the opponents from using them. It is in this sense that it can be argued that deterrence works in the human minds.

One may wonder how such a psychological state can be created. To do so, the following essential components should be called upon. They are capabilities, willingness to use capabilities, demonstration of capabilities, and credible consequences. Successful deterrence relies entirely upon these components. Among these components, the component of capabilities is the most critical one. Without it, the other three components cannot play any role in deterrence.

One may then wonder what capabilities can be used to make deterrence work. For a long time, the strongest physical forces with technological superiority serve as the capabilities that create such a psychological state, because the potential physical punishment can fully convince deterrent targets that they have no chance of achieving their goal and their fate is doomed if they do not stop their commitment. In the physical world, nuclear weapons serve as a last resort in deterrence. This is because they, as weapons of mass destruction, can cause tremendous casualty and destruction to adversaries. The intimidating consequences of being attacked via these weapons are totally beyond what adversaries can bear in any circumstances. The destruction is absolute. The use of these weapons can have a destructive impact. When both sides possess these weapons and neither side ventures to use them first, a balance is thus created.

Currently, the notion of deterrence is heavily influenced by nuclear deterrence strategies, as nuclear weapons possess a paramount threatening capability. Nevertheless, the notion of deterrence itself does not exclude other ways of generating deterrent effects, at least theoretically. If there is a capability that can push deterrent targets into an extreme psychological state to stop or change their behavior, this capability can certainly serve as a capability for deterrence. It does not matter whether this capability is physical, digital, or the combination of the two. If it can help to achieve the deterrence outcome, it is worth to be explored.

To develop a novel solution in this paper, other aspects and instruments of national power should be considered. Extending the scope will generate insights that otherwise may not have. This paper is structured as follows: Here in Section 1, an overview of both deterrence and the major approaches in deterrence theories is provided. In Section 2, the issues of the current deterrence approach, especially the one in cyberspace, are examined. In Section 3, an innovative multi-level and multi-aspect architecture for the integrated deterrence strategy is proposed to address the issues discussed in the previous section. This architecture, incorporating deterrence in cyberspace, points out a new way of effectively implementing the integrated deterrence strategy and ultimately achieving the goal of the strategy. It contains the levels of severity both below and above the threshold of armed conflict as well as the aspects of varied instruments of national power, such as diplomacy, information, military, economy, law enforcement, allies, and partnership. In Section 4, the benefits of the multi-level and multi-aspect architecture for the integrated deterrence strategy are discussed. In Section 5, a conclusion is drawn.

2. Issues of Implementing Deterrence in Cyberspace

It should be pointed out that deterrent capabilities will be effective only when they are employed in the contexts they are designed for. Hence, it is critical to understand the relationship between a deterrent strategy and a strategic context, since one capability that works in one context is not as effective as it should be in another context.

Deterrence in the physical world possesses the following characteristics:

- The purpose of deterrence strategies is to prevent further escalation of conflict and avoid war.
- The deterrent capabilities designed, developed, and employed are for armed conflict. Hence, they are used above the threshold of armed conflict.
- The display of capabilities and the demonstration of willingness to use the capabilities are transparent and unambiguous.
- The entry level is high because tremendous investment is needed for the education of the professionals as well as the design and development of weapons with technological superiority.

- The main deterrent sources are physical, the potential destructive impacts indicated are physical and psychological, and the actual deterrent consequences are psychological and physical.

However, this is not exactly the same in cyberspace. As Chen (2019) points out, cyberspace possesses the following critical factors: speed, accuracy, precision, dynamics, stealth, ambiguity, and individual operators. In most cases, capabilities used for a deterrence purpose in cyberspace are seldom made known publicly. The impact is felt. The capabilities as well as the willingness to use capabilities are demonstrated, but the source codes and algorithms are always kept secret. Besides, as pointed out by General Paul Nakasone, USA, in Nakasone (2019a), "the locus of struggle for power has shifted towards cyberspace, and from open conflict to competitions below the level of armed attack". In addition, the entry level in cyberspace is low (Nakasone, 2019b).

Deterrence in the virtual world possesses the following characteristics:

- The purpose of deterrence strategies is to stop aggressive cyber operations from deterrent targets and prevent cyber conflict from further escalating into armed conflict.
- The deterrent capabilities designed, developed, and employed are for both non-armed and armed conflict. Hence, they are used both below and above the threshold of armed conflict.
- The display of capabilities is opaque and ambiguous, while the demonstration of willingness to use the capabilities is transparent and unambiguous.
- The entry level is relatively low because the cost of design and development of cyber weapons with technological superiority is relatively low compared with the cost of design and development of nuclear weapons (even though tremendous investment is needed for the education of professionals).
- The main deterrent sources are virtual; the potential destructive impacts indicated are virtual, physical, and psychological; and the actual deterrent consequences are psychological, virtual, and physical.

Comparing the characteristics in the virtual world with those in the physical world, one can quickly see that there are differences in the purpose of deterrence, the requirement for deterrent capabilities, the requirement for the display of capabilities, the requirement for the demonstration of willingness to use the capabilities, the requirement for the investment of human resources as well as research and development, deterrent resources, the potential destruction impacts indicated, and the actual deterrent consequences.

Given these differences, it is hard to imagine that the deterrence strategies designed solely for the physical world could be effective in cyberspace. The strategy of deterrence by denial and the strategy of deterrence by punishment are two examples.

The strategy of deterrence by punishment is hard to be employed in cyberspace because proportional punishment, immediate responses, and jurisdiction are usual challenges. In almost all cases, the chances of using nuclear responses to cyber breach operations are slim, since they are not at the same level of severity. Such responses are not proportional. In some cases, economic sanctions and diplomatic protests are introduced, but the responses are frequently delayed. In other cases, retaliatory cyber operations are launched. Due to the anonymous and hidden nature of some cyber operations and the amount of time needed for attribution, immediate responses are hard to be guaranteed.

The strategy of deterrence by denial requires strong defense in cyberspace. However, due to the complexity of systems (namely, having hidden layers that users do not have access to and/or having codes hard to be comprehended by users without technical knowledge) and the opaque nature of cyber supply chain, vulnerabilities within systems have been constantly exploited, thus defeating layers of defense. Restricted by the amount of time needed for attribution and accurate targeting, prompt retaliation in cyberspace is either delayed or is left aside. As a result, this deterrence strategy does not work in some cases.

Kello (2022) examines the two approaches in which deterrence is not sufficiently used in cyberspace as well as the consequences that these approaches may bring about. In one approach, nothing is done after being attacked in cyberspace. Kello (2022) calls this approach "appeasement", and considers it being "inherently escalatory". According to him, "nations that pursue it again teach opponents the lesson of 1938: further gains from aggression lie in wait". In the other approach, persistent engagement is employed while deterrence in cyberspace is not used. This approach "has a proactive element: it takes the fight to the other side's computer terrain". However, it is mainly for defensive purpose, not "a policy of attacking forward". Besides, it "commits unknown national resources to wherever the opponent brings the fight or is preparing it". Hence, following what is discussed in Kello (2017), Kello (2022) argues for punctuated deterrence, which punishes "a series of actions

and their cumulative effects". In Kello's view, punctuated deterrence "gives the victims the option to retaliate wherever and whenever fits their interests and capacities".

Kello's approach shows the significance of having deterrence in cyberspace as well as the difference between deterrence in cyberspace and persistent engagement in cyberspace. Nevertheless, this approach is primarily used for dealing with challenges in cyberspace. Its position in integrated deterrence is not investigated. Hence, this needs to be explored in the next section of this paper.

As discussed, deterrence in cyberspace is undoubtedly needed. However, in cyberspace, the strategy of deterrence by punishment is hard to execute, while the strategy of deterrence by denial may not be successful in all cases because these deterrence strategies are specifically designed for conflict in the physical world, and they are not specifically designed for cyberspace. Hence, they may or may not be effective in the cyber contexts.

As shown above, deterrent capabilities are effective only when they are employed in the strategic contexts they are designed for. So are the deterrence strategies that employ deterrent capabilities.

It needs to be pointed out that having problems in implementing these deterrence strategies in cyberspace does not mean that deterrence will never work in cyberspace. It instead means that appropriate deterrence strategies have not been employed in cyberspace as they have not been figured out and their corresponding deterrent measures have not been built yet. One of the urgent tasks that we have is to design context-based and appropriate deterrence strategies for cyberspace, building corresponding deterrent measures, and relating these strategies to the overall integrated deterrence strategy. This is what is going to be explored in the next section.

3. An Innovative Proposal

Varied deterrent capabilities not only are bound by varied contexts designed for but also can be tied together to achieve deterrence effects. When they are organized in a holistic way, a new version of integrated deterrence is brought into being.

In the 2022 U.S. National Security Strategy (NSS), integrated deterrence is defined as "the seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits". It entails integration across domains, regions, the spectrum of conflict, the U.S. Government, and with allies and partners. In the 2022 U.S. National Defense Strategy (NDS) Fact Sheet, three primary ways of advancing the Department of Defense goals are mentioned. They are integrated deterrence, campaigning, and building enduring advantages.

In these national strategies, clearly listed are the key components of integrated deterrence, namely, the role of nuclear deterrent, cross-domain and cross-aspect interagency efforts, and cooperation with alliances and partners. In a sense, the integrated deterrence strategy, backstopped by nuclear deterrent, mobilizes all the parties and resources available, both internally and externally, to build enduring advantages in deterring adversaries.

Starling, Wetzel, and Trotti (2021) describe the integrated deterrence concept as an expansion from traditional deterrence to strategic deterrence by promoting whole-of-government deterrence plus whole-of-alliance deterrence. Within whole-of-government deterrence, instruments of national power are used.

To capture the essence of these strategies, this paper, following the model of deterrence levels recommended in Chen (2018a), proposes a multi-level and multi-aspect architecture, which is shown in Figure 1 below. This architecture consists of the levels that capture the escalation and de-escalation of conflict as well as the width that covers multiple instruments of national power and alliances.

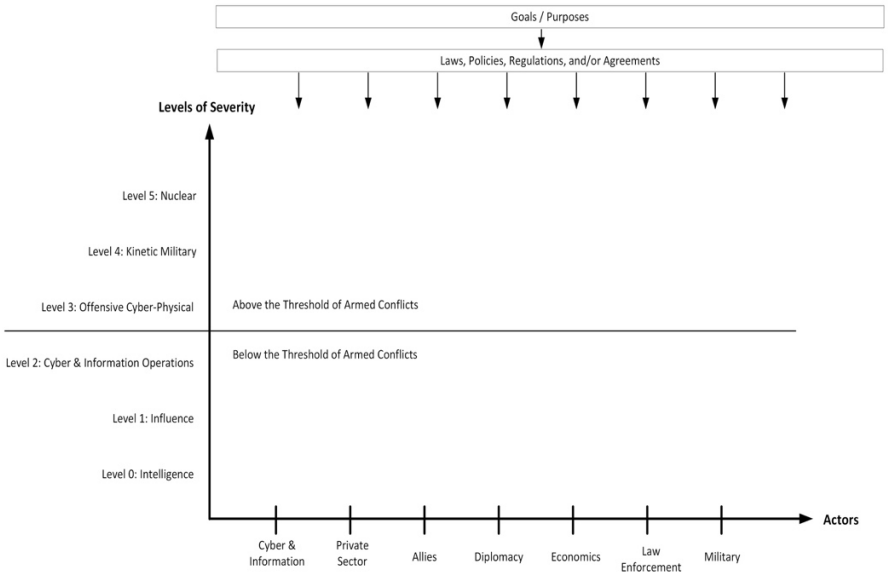

Figure 1: The Multi-level and Multi-Aspect Architecture for Integrated Deterrence Strategy

This architecture captures various levels of competition and conflict based on severity. These levels are either below or above the threshold of armed conflict. The following levels are below the threshold of armed conflict:

- Level 0 is the level of intelligence collection and analysis operations.
- Level 1 is the level of influence campaigns.
- Level 2 is the level of cyber operations and cyber-enabled information operations.

The following levels are above the threshold of armed conflict:

- Level 3 is the level of offensive cyber-physical operations and campaigns.
- Level 4 is the level of kinetic and conventional military campaigns.
- Level 5 is the level of nuclear warfare.

Going from a lower level to a higher lever indicates an escalation of a conflict and an increase in deterrence intensity, while going from a higher level to a lower level designates a de-escalation of a conflict and a decrease in deterrence intensity.

This architecture also captures the varied aspects that can be involved in deterrence endeavors. They consist of the following aspects: information, private sector, allies, diplomacy, economics, law enforcement, and military. Each aspect has a focus on a certain level or certain levels. Only the military aspect has the access to all levels. Besides having more aspects involved in the execution of deterrence means widening the scope of deterrence, while having fewer aspects involved in the execution of deterrence means narrowing the scope of deterrence.

Being dynamic and flexible, this architecture makes it possible to have different levels of deterrence in different strategic contexts. This means that there is no need to execute nuclear deterrence at Level 2, namely, the level of cyber operations and cyber-enabled information operations. However, as the situation escalates, the level of severity may get up to Level 5, namely, the level of nuclear warfare. Nuclear deterrence can be proportionally executed in an appropriate context. It is in this way that the nuclear deterrent is positioned in the integrated deterrence strategy, namely, supporting all lower level deterrent measures and serving as the ultimate deterrent measure. This satisfies the requirement of the 2022 NSS, which states that “nuclear deterrence remains a top priority for the Nation and foundational to integrated deterrence.”

Being dynamic and flexible, this architecture also makes it possible to widen the scope of deterrence. Instead of only resorting to the military force of one country, allied forces may be asked to get involved. By increasing the number of aspects involved, the weight of deterrence becomes amplified. Similarly, by engaging the private sector at the levels below the threshold of armed conflict, more capabilities can be assembled in executing deterrence in cyberspace.

In this architecture, Level 5 is focused on total physical destruction, while Level 2 is focused on cyber operations, especially surprise and signalling from the virtual world.

To summarize, this multi-level and multi-aspect architecture for the integrated deterrence strategy can satisfy the requirements of the 2022 NSS and the 2022 NDS by successfully bringing varied deterrent capabilities and varied strategic contexts together in a holistic way, thus achieving proportional and effective deterrence effects.

Given this architecture, deterrence must be proportional and effective at every level. Should there be little or no deterrent capabilities at one level, the integrated deterrence strategy will not be effective overall. Therefore, deterrence in cyberspace is required to support the overall integrated deterrence. Should cyber conflict at Level 2 escalate to cyber-physical conflict at Level 3, human casualty and property damage can be expected via attacks against critical infrastructure.

In Fischerkeller and Harknett (2018), two strategic spaces are mentioned. One is the strategic competitive space short of armed conflict, and the other is the strategic space of militarized crises and armed conflict. The first space contains a competitive interaction dynamic. It is in this space where the persistent engagement strategy and the defend forward strategy are executed. The second space encompasses escalation dynamics. It is in this space where compellence measures, including conventional weapons and nuclear weapons, are used. Deterrence lies in the space between these spaces. However, little is talked about the deterrence space. This approach is thus limited. Leaving a blank spot on the continuum is not a good idea, because one line of defense is left unused. Hence, ways of creating deterrence in cyberspace should be included for strategic reasons. The multi-level and multi-aspect architecture for integrated deterrence strategy elegantly bridges this gap, as it, sitting in the deterrence space, provides a link between the strategic competitive space short of armed conflict and the strategic space of militarized crises and armed conflict. With the introduction of this continuum, the role of deterrence prior to armed conflict can be explicitly captured and efficiently emphasized.

Within the deterrence space, one level of deterrent is simply not enough since the deterrent will be either too strong or too weak in a non-associated strategic context. For instance, if the nuclear deterrent is chosen as an option for deterrence in cyberspace, it will not be executed as a response for cyber breach attacks in almost all cases because it is too strong and not proportional. Likewise, if kinetic military campaigns are chosen as an option for deterrence in a nuclear war, it will not work because it is too weak and not proportional. Hence, it is important to employ context-based deterrent in a specific context.

Fischerkeller, Goldman, and Harknett (2022) also mention four important variables in the cyber strategic environment. These variables are “accessibility, availability, speed, and affordability.” They hold that persistent engagement, which is “able to effectively anticipate and persistently set the conditions of security” in one’s favour “in and through cyberspace”, is the key for success in cyberspace since it perfectly fits in the cyber strategic environment, which is “the product of interconnectedness, constant contact, and inherently reconfigurable terrain and capacity to act across and through that domain”. In other words, the persistent engagement strategy should be executed in the strategic competitive space short of armed conflict. Even though their analysis is not for deterrence in cyberspace, it is still applicable regarding the strategic context in cyberspace.

Which deterrent then fits in the cyber strategic context? Strategic surprise is one of them. This is because it can make deterrent targets overwhelmed with shock, confusion, and fear, at least for a period, and it can help to achieve the goal of stopping aggressive cyber operations from deterrent targets and preventing cyber conflict from further escalating into armed conflict. Strategic surprise can affect the minds of deterrent targets, making them lose the will to continue their commitment. This certainly offers deterrent initiators superiority during that period.

Kam (1988) points out that “surprise is a basic and recurring event in human life. Still, neither the repeated occurrence of surprises nor our assumption that life has surprises in store for us makes us any less vulnerable to its impact.” Following Kam (1988), strategic surprise can be created in the minds of adversaries when an act or development goes against the expectations of adversaries; catches them unprepared; and provokes shock, confusion, and fear in their minds. To satisfy these conditions, the state of uncertainty is needed. This state of mind, in turn, relies on ambiguity, anonymity, speed, and unique capabilities such as intelligence collection and analysis, precision, accuracy, and stealth maneuver. Chen (2017) and Chen (2018b) provide some detailed discussion about these capabilities. These are also the critical factors in cyberspace. Hence, in the virtual world, they can be naturally employed to create deterrent effects.

Therefore, in the strategic context of cyberspace, strategic surprise supported by stealth operations can be employed as a deterrent. This is one of the components in the strategy of deterrence by engagement and surprise, proposed in Chen (2017). For instance, this deterrent can perform the following functions to

overwhelm deterrent targets with fear and anxiety. First, various types of surprised warming messages can be sent to deterrent targets via unexpected means, to unexpected devices, and at unexpected times, indirectly indicating that the deterrent targets are being closely monitored and their identities are known. The frequency, target locations, message delivery methods, and message transmission time can be changed dynamically. Second, various direct and indirect but surprise cyber operations can be launched specifically against deterrent targets on varied hardware, software, and firmware without prior notice. Third, cyber-enabled information operations can be launched against deterrent targets without warning via unexpected means, to unexpected devices, and at unexpected times. Such operations are launched to damage deterrent targets' reputation via social media. All these surprised operations, which catch deterrent targets unprepared, can create uncertainty that will provoke shock, confusion, and fear. Overwhelmed by fear supported by uncertainty, deterrent targets can be deterred. Besides, varies operations send out varied signals to deterrent targets. Note that all these occur at Level 2 of the architecture proposed. These operations are below the threshold of armed conflict. It should be pointed out that the deterrence at this level is not as powerful as the deterrence at the level of nuclear weapons; however, it is proportional and serves its purpose. Besides, the signalling function is provided.

Deterrence at the offensive cyber-physical level is above the threshold of armed conflict. Here, cyber means are used for military purpose. Critical infrastructure is held hostage in deterrence. Nevertheless, the state of uncertainty can be generated with the help of ambiguity, anonymity, speed, and unique capabilities. This type of kinetic military operations or campaigns can also overwhelm deterrent targets with shock, confusion, and fear. Consequently, deterrent effect is created, and deterrent targets can be deterred. Likewise, extremely strong signals are sent out to deterrent targets.

As shown above, deterrent capabilities in cyberspace can be used either below or above the threshold of armed conflict. They are applicable not only in cyberspace but also in the physical world. With the multi-level and multi-aspect architecture for integrated deterrence, the differences in deterrent purposes, capabilities, and applications can be explicitly and successfully captured.

4. Benefits of the Multi-level and Multi-Aspect Architecture for the Integrated Deterrence Strategy

The multi-level and multi-aspect architecture for the integrated deterrence strategy holistically captures the essence of the 2022 NDS. It successfully reveals the relationship among different components, especially the dependency relationship. This makes it possible to execute deterrence proportionally and effectively within a certain strategic context, increasing its chance of being successful. This holistic approach also makes deterrence dynamic and flexible by resorting to varied deterrents based on varied strategic contexts. This architecture for integrated deterrence differentiates varied strategic contexts either below or above the threshold of armed conflict. Recognition of different strategic contexts helps to design and develop context-based deterrent capabilities, as well as dynamic tactics, techniques, procedures (TTP), and mechanisms. This approach makes deterrent capabilities efficient and effective within their relevant strategic contexts.

With the introduction of the multi-level and multi-aspect architecture for the integrated deterrence strategy, some challenging questions can be successfully addressed. In this new approach, a deterrent is no longer treated as something that can be executed anywhere. Instead, it must be executed within a relevant strategic context should it be effective. In this sense, they are context-based deterrent capabilities.

This holistic approach not only makes deterrence in cyberspace a part of the overall integrated deterrence but also provides national security decision-makers and strategists with ways of executing proportional and effective deterrence at different levels and within different aspects/scopes, thus successfully achieving national security goals. Ultimately, the research shows that deterrence in cyberspace is an essential component of integrated deterrence.

This innovative approach can certainly enrich integrated deterrence, since more domains, dimensions, and facets are added into this strategy, thus making the strategy more powerful and more flexible.

5. Conclusion

This paper examines the issues of the current deterrence approaches, especially the one in cyberspace. It argues that deterrent capabilities will be effective only when they are employed in the contexts in which they are designed for. Based on this argument and the requirements of the 2022 NSS and the 2022 NDS, an innovative multi-level and multi-aspect architecture for the integrated deterrence strategy is proposed. The need for

deterrence in cyberspace is discussed. So are various ways of conducting deterrence in cyberspace, especially ways that resort to strategic surprise. Besides, the benefits of the multi-level and multi-aspect architecture for the integrated deterrence strategy are discussed.

Given the proposed multi-level and multi-aspect architecture for integrated deterrence, varied deterrent capabilities and varied strategic contexts can be holistically tied together in a structured way; deterrence in cyberspace can be accounted for as an essential component in integrated deterrence; varied novel deterrent capabilities at different levels and within different aspects can be created, and ways of effectively using all deterrent capabilities at different levels can be provided to national security decision-makers and strategists in helping them to execute proportional and effective deterrence at various levels and within various aspects based on the requirements of strategic contexts, thus maintaining strategic advantage. As a result, the integrated deterrence strategy can eventually prevent war and maintain peace.

References

Art, R. and Greenhill, K. (2018) "Coercion: An Analytical Overview", *Coercion: The Power to Hurt in International Politics*, K. Greenhill & P. Krause (eds.), pp. 3–32, Oxford University Press, Oxford, UK.

Brodie, B. (1946) (ed.) *The Absolute Weapon: Atomic Power and World Order*, Harcourt Brace, New York.

Chen, J. (2019) "AI-Based Deterrence in the Cyber Domain", *Proceedings of the 14th International Conference on Cyber Warfare and Security*, pp.38–45.

Chen, J. (2018a) "On Levels of Deterrence in the Cyber Domain", *Journal of Information Warfare*, Vol.17,.2, pp.32-41.

Chen, J. and Dinerman, A. (2018b) "Cyber Capabilities in Modern Warfare", *Cyber Security: Power and Technology*, M. Lehto and P. Neittaanmäki (eds.), pp. 21–30. Springer.

Chen, J. (2017) "Cyber Deterrence by Engagement and Surprise", *PRISM*, Vol.7, No.2, pp.101-107.

Fischerkeller, M., Goldman, E., and Harknett, R. (2022) *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Oxford University Press, New York, New York.

Fischerkeller, M. and Harknett, R. (2018) "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation", Institute for Defense Analyses.

Harknett, R. and Smeets, M. (2020) "Cyber Campaigns and Strategic Outcomes: The Other Means", *Journal of Strategic Studies*, Spring 2020 Issue, pp.1–34.

Healey, J. (2019) "The Implications of Persistent (and Permanent) Engagement in Cyberspace, *Journal of Cybersecurity*, 2019, pp.1-15.

Kahn, H. (1960) *The Nature and Feasibility of War and Deterrence*, P-1888-RC, RAND Corporation, Santa Monica, California.

Kam, E. (1988) *Surprise Attack: The Victim's Perspective*, Harvard University Press, Cambridge, Massachusetts.

Kello, L. (2022) *Striking Back: The End of Peace in Cyberspace – And How to Restore It*, Yale University Press, New Haven, CT.

Kello, L. (2017) *The Virtual Weapon and International Order*, Yale University Press, New Haven, CT.

Libicki, M. (2021) *Cyberspace in Peace and War*, (2nd Edition), Naval Institute Press, Annapolis, Maryland.

Libicki, M. (2009) *Cyberdeterrence and Cyberwar*, Project Air Force. RAND Corporation, Santa Monica, California.

Nakasone, P. (2019a) "A Cyber Force for Persistent Operations", *Joint Force Quarterly*, Vol.92, 1st Quarter 2019, pp.10–14.

Nakasone, P. (2019b) "An Interview with Paul M. Nakasone", *Joint Force Quarterly*, Vol.92, 1st Quarter 2019, pp.4–9.

Nye, J. (2017) "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol.41, No.3, pp.44-71.

Payne, K. (2008). *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century*, National Institute Press.

Schelling, T. (1960) *The Strategy of Conflict*, Harvard University Press, Cambridge, Massachusetts.

Schelling, T. (1966) *Arms and Influence*, Yale University Press, New Haven, Connecticut.

Smeets, M. (2020) "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection", *Intelligence and National Security*, Vol.35, No.3, pp.444-453.

Starling, C., Wetzel, T., and Trotti, C. (2021) "Seizing the Advantage: A Vision for the Next US National Defense Strategy", Atlantic Council Strategic Paper, Atlantic Council Scowcroft Center for Strategy and Security, Washington DC.

The Joint Staff. (2011) *Joint Publication 3-0: Joint Operations*, Washington DC.

The United States Office of the Secretary of Defense (OSD). (2022) *Fact Sheet: 2022 National Defense Strategy*, Washington DC.

The White House. (2022) *National Security Strategy*, Washington DC.