BODHI SPECTRUM
Global Journal of Multidisciplinary Research

From Deterrence to Forward Deterrence: Changing Dynamics of Iran–Israel–US Wargaming

Dr. Gayathri Pramod Panamoottil

Assistant Professor, School of Law, Karnavati University, Gujarat

ABSTRACT

The topic titled from deterrence to forward deterrence examine the evolution and practice of classical deterrence to forward deterrence and its implications for security wargaming between Iran, Israel and the USA are examined in detail. This paper primarily focuses on the geopolitical significance of, classical deterrence theory and its implications in the war front. The paper is divided into four thematic stages: First, it incorporates an inquiry on the theory of deterrence and forward deterrence, and its lineage as well as its application to the strategic triangle of Iran – Israel – US are mapped. Second, it embeds wargaming in the deterrence enterprise, and illustrates how simulation-based exercises serve as tools for strategic signalling, doctrine-evolution and managing escalation. Third, by performing a thorough comparative study of the various kinds of military, cyber, and economics and proxy warfare used by Iran, Israel, and the United States in their strategic competition, it reveals specific strategic aspects of Iran's policy making regarding these tools and methods. Finally, it integrates all the aspects and extrapolates possible trends of trilateral confrontation. The ultimate argument of the paper is that the operational logic of all three was fixed as one of forward deterrence, which now essentially defines the wargaming practice and the fundamental nature of regional stability.

Introduction

The strategic landscape of West Asia has been reshaped fundamentally over the past four decades by the triangular competition among Iran, Israel, and the United States. What began as a predominantly bilateral Cold War rivalry between Washington and Tehran, mediated through proxies and sanctions, has matured into a complex, multi-domain contest involving sophisticated military doctrines, hybrid warfare tools, and continuous wargaming exercises. At the conceptual heart of this transformation lies the evolution from classical deterrence—a defensive posture designed to convince an adversary that the costs of aggression will outweigh the benefits—to a more proactive and expansive concept of forward deterrence, which seeks to impose costs deep within the adversary's strategic depth before conflict ever reaches one's own borders (Posen, 1984; Quackenbush, 2011)[1].

1 Posen, B. (1984). The sources of military doctrine: France, Britain, and Germany between the world wars. Cornell University Press; Quackenbush, S. L. (2011). Deterrence theory: Where do we stand? Review of International Studies, 37(2), 741–762.

The Islamic Revolution of 1979 changed Iran's strategic posture from pro-western to extreme anti-Americanism and hostility towards the existence of Israel. After the splitting, the three actors have been waging an unrelenting contest of wills across the nuclear arena and the proxy, cyber, drone and escalation rounds. This contest has been heavily skewed by incredible disparities between the United States' unmatched military power and global reach, Israel's military hedging and an extensive—although not revealed, and therefore not technically state—arsenal of nuclear weapons, and its exceptional intelligence capabilities, on one side, and Iran's in some ways offsetting resources in the form of ideological unity, strategic patience, and a broad and elaborate arsenal of missiles, as well as an intricate network of non-state supporters known as the "Axis of Resistance" (Byman, 2019; Cronin, 2019)[2].

In this context, wargaming is proving to be an invaluable tool for strategic planning. Each actor is able to test his assumptions and sweeten his doctrines and predict enemy response using simulations, table-top exercises and computer-assisted war games. The nature of these exercises – including use of cyber space, space technology, information operations and scenarios from multiple fronts – illustrates the rising complexity of the strategic environment. The paper therefore contends that an analysis of the transformation of classical deterrence to 'forward deterrence' and the incorporation of this concept in 'wargaming' is absolutely necessary to understand the current and future dynamics of the strategic triangle Iran–Israel–US (Davis & Arquilla, 1991; Shlapak & Johnson, 2016)[3].

The paper is organised as follows. This is done in Section Two by setting out and examining the theoretical framework, which introduces an examination of the intellectual history of deterrence theory, and which further develops the concept of forward deterrence in a theoretical manner. The operationalization of deterrence logic in Section Three looks at wargaming. In Section Four, a detailed comparative analysis is made of the strategic tools and techniques that are used by each of these actors. Section Five provides a summary and a look ahead. The paper is concluded with a complete list of references.

Theory of Deterrence and Forward Deterrence: Intellectual Foundations and Strategic Implications.

Deterrence theory constitutes one of the most elaborate and consequential bodies of strategic thought produced in the twentieth century. It's a modern intellectual framework is rooted back during the Cold War era—marking an intellectual corridor because of the introduction of nuclear weapons—which forced strategists and scholars to fundamentally rethink the point of having military power. In its simplest terms, the basic principle of deterrence theory is that an actor will decline an undesirable action if he or she estimates that the costs of the action, via the deterring party, will be greater than any potential benefit of the action (Brodie, 1959 and Schelling, 1960)[4]. The deterrent effect works by plausibly threatening and calculating consequences—and assumes both parties are essentially rational utility-maximising actors that can process information and revise preferences as needed.

The basic quandary of nuclear deterrence was expressed by Bernard Brodie (1946)[5], considered the father for nuclear strategy: the role of armed forces has gone from war-winning to war-prevention. This insight was further developed by Thomas Schelling who was the first to calculate in his brilliant books The Strategy of Conflict (1960)[6] and Arms and Influence (1966)[7] the conceptual vocabulary with which deterrence theory would be operationalised. Schelling classified two ways of deterring an adversary: deterrence by denial (whereby the attacker is convinced that they cannot or will not be able to reach their goal no matter the action taken) and deterrence by punishment (whereby the attacker is convinced that whatever is done it costs him more than what he could gain). This binary taxonomy was key to the subsequent deterrence literature, and was a central tenet of both superpowers' strategic doctrines during the Cold War.

Herman Kahn furthered the concept of deterrence by formulating the idea of escalation dominance, which called for the ability to win at each step of the escalation, from a small blood-or waterfight to "all-out nuclear exchange"

2 Byman, D. (2019). Iranian foreign policy and the sponsorship of terrorism. The Brookings Institution Press; Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

3 Davis, P. K., & Arquilla, J. (1991). Deterring or coercing opponents in crisis: Lessons from the war with Saddam Hussein. RAND Corporation; Shlapak, D. A., & Johnson, M. (2016). Reinforcing deterrence on NATO's eastern flank: Wargaming the defence of the Baltics. RAND Corporation.

4 Brodie, B. (1959). Strategy in the missile age. Princeton University Press; Schelling, T. C. (1960). The strategy of conflict. Harvard University Press.

5 Brodie, B. (1946). The absolute weapon: Atomic power and world order. Harcourt, Brace and Company.

6 Schelling, T. C. (1960). The strategy of conflict. Harvard University Press.

7 Schelling, T. C. (1966). Arms and influence. Yale University Press.

(Kahn, 1965)[8]. But soon thereafter Robert Jervis complicated this picture, by noting that there were many reasons why even rational actors could still fall into a war that were not an intentional choice to go to war, but rather a miscalculation (Jervis, 1976)[9]. These two scholars built up an extensive system of thought which for decades would influence military planning and wargaming.

The concept of classical deterrence is based on three pillars: capability, credibility and communication. Capability is the military instrument itself that is used to inflict costs on an opponent. Threats must be credible, authentic and not "a bluff. Communication is to signal clearly intentions and capacities through expressed policy, military posture and diplomacy (Morgan, 2003)[10]. But as any of these pillars are undermined – when capabilities are called into question, threats are discounted, or signals are misunderstood – then deterrence is undermined and the chances of conflict increase. While this approach has been utilized in the Iran-Israel-US context to a degree, several points need to be carefully adjusted since the competition in the region is multi-actor and asymmetric.

Deterrence theory is based on a realist approach to international relations theory. In terms of how deterrence fits into his own model, Kenneth Waltz's neo-realist theory (1979)[11] locates deterrence in a systemic logic of self-help within a world of states in an international state of anarchy, balancing threats and deterrence posture as a means of survival. This line of thinking helps clarify—and justifies—why Iran is so willing to risk so much economically for deterrence against both existential threats—from the United States and Israel. The neo-realist perspective also is useful in explaining why Israel perseveres in maintaining its qualitative military edge and forward deterrence posture despite the diplomatic consequences: first of all to ensure its survival in an anarchical system, and first to deter that survival.

Constructivist perspectives add important nuance to purely rationalist accounts of deterrence by highlighting the role of identity, norms, and strategic culture in shaping deterrence behaviour. Iran's strategic culture, deeply shaped by the experience of the Iran–Iraq War (1980–1988) in which the international community largely supported Iraq's use of chemical weapons against Iranian forces, has produced a profound sense of strategic isolation and self-reliance that informs its deterrence calculations (Eisenstadt, 2011)[12]. The revolutionary ideology of the Islamic Republic, which frames resistance to American and Israeli power as a religious and civilizational imperative, shapes Iranian deterrence posture in ways that purely rationalist models may underestimate. Similarly, Israel's Holocaust memory and the existential framing of its security challenges create strategic cultural dispositions toward worst-case planning and pre-emptive action that influence its deterrence behaviour in ways that exceed purely material calculations.

Beyond the dyadic deterrence relationship, classical theory also developed the concept of extended deterrence, in which one state extends its deterrence umbrella to protect allies against attack. The United States refined this concept extensively during the Cold War, committing to the defence of Western Europe and Japan through explicit security guarantees backed by the threat of nuclear retaliation (Huth,1988)[13]. In the contemporary West Asian context, U.S. extended deterrence commitments to Israel, Saudi Arabia, and Gulf States play an analogous role, though complicated by the absence of formal defence treaties and the ambiguous status of Israel's nuclear capabilities (Inbar & Shamir, 2014)[14].

The new equation of nuclear deterrence is complicated by Israel's nuclear stance. Israel, whose status on whether it has nuclear weapons or not has been carefully left ambiguous, would have tried to deter existential threats without any explicit nuclearisation while not incurring political costs (Cohen, 1998)[15]. This posture has influenced wargaming situations to date: analysts and planners have to now deal with the implications of a nuclear capable Israel that decides never to admit she has one. The biggest deterrence dilemma in the region is Iran's own nuclear programme, and the international reaction in the form of sanctions and diplomacy, which have been ramped up over the last 20 years with escalating intent, both at play (Litwak, 2012)[16].

8 Kahn, H. (1965). On escalation: Metaphors and scenarios. Frederick A. Praeger.
9 Jervis, R. (1976). Perception and misperception in international politics. Princeton University Press.
10 Morgan, P. M. (2003). Deterrence now. Cambridge University Press.
11 Waltz, K. N. (1979). Theory of international politics. Addison-Wesley.
12 Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.
13 Huth, P. K. (1988). Extended deterrence and the prevention of war. Yale University Press.
14 Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century. Routledge.
15 Cohen, A. (1998). Israel and the bomb. Columbia University Press.
16 Litwak, R. S. (2012). Deterring nuclear Iran: A guide to evaluating policy options. Wilson Center.

If the Iranians do develop nuclear weapons, the United States faces a special problem of extended deterrence. A nuclear Iran would shift dramatically the power balance in the region, spurring a proliferation all but inevitable, with Saudi Arabia, Turkey and Egypt mulling on their own nuclear programmes. U.S. extended deterrent guarantees for the region would start to become very burdensome if Iran had nuclear weapons, since it too would have a deterrent and this capability would limit Washington's use of force to defend partners in the region. It is these dynamic aspects that have been examined in detail in a range of wargaming sessions, invariably demonstrating that averting the prospect of Iranian nuclearisation is much more desirable than deterring a nuclear Iran, and thus justifying the long Beijing-based campaign of coercion against Iran's nuclear ambitions (Cordesman, 2014; Litwak, 2012)[17].

The notion of forward deterrence is a step forward from the classical concept of deterrence. While classical deterrence is primarily retrospective, it's trying to induce the adversary to not aggression because of the threat of direct retaliation that will be unacceptable to them, forward deterrence refers to something that seeks to impose costs and constraints upon a foreign power's strategic options even before it attacks. Strategically, this shift in concept is inadequate in an era of hybrid warfare, proxy wars and grey-zone operations, as it means waiting for a proxy-US ally to cross a bright-bottom line before reacting (Freedman, 2004; Gray, 1999)[18].

There are several interrelated practices that are considered as forward deterrence. The principle of 'pre-emptive strike' aims to take out enemy capability first before they can be used. Deploying carrier strike groups (CSGs); forward basing aircraft; and missile defence installations are all indications of capability and resolve, as well as limitations on adversary options. Carrier strike groups (CSGs); forward basing of aircraft; and missile defence installations are all signs of both capability and resolve and adviser options constrained. Economic measures, such as restrictive sanctions and financial measures, erode an opponent's ability to raise funds for military initiatives or to maintain political support. The effects of cybers can cause paralysis or degradation of adversary infrastructure while not being included under a traditional military response. A proxy support is a capability that can harass, surveilled, or attack enemies from a distance (Rid, 2013; Lindsay, 2013)[19]. Collectively these instruments form a forward deterrence architecture siloed throughout the spectrum of statecraft.

Forward deterrence is most evident in Israel's strategic doctrine. Former Prime Minister Menachem Begin's Begin Doctrine set the precedent to Israel's wage preemptive wars to destroy existential threats before they became a reality (Cohen & Frankel, 1990)[20]. This doctrine was invoked again last year, when Israeli planes attacked a suspected nuclear plant in Syria. As for Iran, Israeli forward deterrence has taken a "proactive" form, in the sense of repeated targeted assassinations of Iranian nuclear scientists, covert sabotage attempts against Iranian nuclear sites (particularly the Stuxnet cyberattack, which was reportedly developed by joint US-Israeli efforts) and repeated airstrikes operations against Iranian military equipment sites in Syria (Sanger, 2012)[21].

Iran's own specificity constitutes the forward strategy of deterrence: they follow their own rationale, yet around the same magnitude of ambition. Interestingly, instead of aggressively asserting its military power, Iran adopts what strategic analysts refer to as a Forward Defence doctrine, which suggests that Iran's security is not contained within its boundaries but extends to Lebanon, Syria, Iraq, Yemen and Gaza thanks to support for and integration with non-state armed groups (Eisenstadt, 2011; Saab, 2018)[22]. This forward posture has multiple deterrent effects: it adds a layer of complexity to any local attempt at an invasion of Iran; it offers bases for retaliatory strikes at Israel and U.S. presence in the region; and it lets potential opponents know that any attack on Iran will unleash a conflict on multiple fronts. The strategic idea is to deter opponents with threat escalation, that is, to make them believe that the price of war would be limitless in terms of geography and time.

The United States, on the other hand, has developed a forward deterrence strategy based on the 3-Ds: denial, degradation, and deterrence (Cronin, 2019)[23]. Denial: Block Iran from getting nuclear weapons through diplomacy,

17 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies; Litwak, R. S. (2012). Deterring nuclear Iran: A guide to evaluating policy options. Wilson Center.

18 Freedman, L. (2004). Deterrence. Polity Press; Gray, C. S. (1999). Modern strategy. Oxford University Press.

19 Rid, T. (2013). Cyber war will not take place. Oxford University Press; Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.

20 Cohen, A., & Frankel, B. (1990). Opaque nuclear proliferation. Journal of Strategic Studies, 13(3), 14–44.

21 Sanger, D. E. (2012). Confront and conceal: Obama's secret wars and surprising use of American power. Crown Publishers.

22 Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy; Saab, B. Y. (2018). The coming Gulf war: Iran, the United States and their proxies. Foreign Affairs, 97(4), 10–17.

23 Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

sanctions, and covert action. Deals with Iran's military forces, proxy networks and financial infrastructure. Deterrence helps keep threats of military action in the face of Iranian aggression credible. These capabilities have rendered U.S. forward deterrence more flexible and granular, with the ability to use a variety of cyber, precision-strike, and expanded regional partnership tools to cost Iran heavy prices for its strategic conduct without resulting in open war.

Deterrence Stability and Escalation Risks in the Trilateral Context

The trilateral deterrence relationship among Iran, Israel, and the United States presents unique challenges to deterrence stability. The trilateral relationship is not a bilateral one, as during the Cold War between the United States and the Soviet Union, but is characterized by overlapping deterrence commitments, an asymmetric force structure, and multiple actors, each with different strategic cultures and levels of deterrence risk tolerance. A complicating factor is the role of Israel, which may sometimes be a deterrent for the United States but also a potential catalyst to U.S. military engagement, since Israel may not always make decisions in accord with U.S. preferred strategic roles (Indyk, Lieberthal & O'Hanlon, 2012)[24].

Escalation is especially in danger in view of the uncertainties of Iran's nuclear programme. With Iran making progress on its enrichment, Israeli and U.S. deterrence becomes increasingly challenged between the need to prevent priority Iranian nuclearisation and the potential incitement of a regional war. Time and time again, the wargaming drills have emphasized the challenge of achieving strategic goals while trying to calibrate coercive pressure against Iran in ways that do not cross the escalatory thresholds that saddle decision makers with unwanted conflict (Cordesman, 2014)[25]. In 2020, the killing of General Qasem Soleimani revealed the destructive threat forward deterrence operations can have on Iran and the difficult escalation/decision-making of the Iranian side, who retaliated with ballistic missile attacks on

U.S. bases in Iraq but nonetheless managed to act consistently in a way that did not escalate into a wider conflict.

The addition of the cyber and space dimensions aggravates the deterrence stability. Then, in 2010, with the discovery of the attack on Iranian nuclear centrifuges using the Stuxnet malware, a new type of offensive action entered the scene, one below acceptable military thresholds that nevertheless resulted in significant strategic costs (Lindsay, 2013)26. Iran's investment in offensive cyber capabilities, combined with the attacks against Saudi Aramco and U.S.

financial institutions, all indicate a tit-for-tat in the cyber arena, in line with the logic of deterrence, but in a space where the notions of attribution, proportionality, and red lines have yet to be fully established. The use of cyber deterrence as a forward deterrent introduces, then, one more layer of complexity to an already dense and unstable strategic competition.

Particular attention, in the trilateral context, should be given to the issue of communicating red lines. Classical deterrence theory tells us that in order to have deterrence, an adversary must have a clear conception of what is being deterred, by whom and the conditions that result in retaliation. With relation to Iran, Israel, and the USA, there are several "red lines" which overlap and are not always the same among the three parties. The United States has been clear in saying it won't tolerate Iran's acquisition of nuclear arms but has not defined exactly what it considers a line it dare not cross. Israel has its own red lines with respect to both military deployments in Syria and Hezbollah weapons buying that have led to Israeli military responses, not all of which are openly U.S. sanctioned. Iran has its own "red lines," as far as striking its nuclear sites and territory is concerned, and those will lead to escalatory reactions. A crux in deterrability stability in deterrence in the region, is the management of these multiple, overlapping and sometimes conflicting red lines, especially those between Armenia and Azerbaijan.

Wargaming as an Instrument for Forward Deterrence: Theory, Practice, and Strategic Signalling

Wargaming, in its broadest definition, encompasses any structured simulation of conflict designed to test strategic concepts, refine operational plans, and assess the likely behaviour of adversaries under varying conditions (Perla, 1990)[27]. Its intellectual roots extend to the Prussian Kriegsspiel of the early nineteenth century, which introduced rigorous rule-based simulation to military planning and demonstrated that structured play could generate genuine strategic insight. The subsequent diffusion of wargaming across military establishments globally, and its eventual

24 Indyk, M., Lieberthal, K., & O'Hanlon, M. (2012). Bending history: Barack Obama's foreign policy. Brookings Institution Press.
25 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.
26 Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.
27 Perla, P. P. (1990). The art of wargaming: A guide for professionals and hobbyists. Naval Institute Press.

adoption by civilian strategic analysts and policy planners, transformed it from a narrow military tool into a broader instrument of strategic analysis and communication.

Today wargaming is much more sophisticated and complex than ever has been before and involves "wargaming with computer-assisted simulations, multi-agency participation, AI-assisted adversary modelling, and classified intelligence inputs. Wargames can vary from purely conceptual table-top games by senior decision makers to those that are very elaborate with thousands of variables and real-time data feeds ("Davis & Arquilla, 1991")[28]. Widespread wargaming programmes have been built up by the RAND Corporation, the U.S. Naval War College and many of the defence ministries around the world as a regular source of strategic planning and policy development. Wargaming has emerged as an essential instrument in the Iran–Israel–US competition to consider scenarios for escalation, to examine deterrence assumptions and to estimate the capabilities of various coercive instruments.

The typology of wargaming is applicable to the Iran/Saudi Arabia/US context in several different, but related categories. In the strategic-level political-military games, participants explore decision-making at the highest levels of government in the situation of Iran's provocations, Israel's military operations or a failure to deter on the part of the U.S. The ' games are usually led by senior decision makers or experienced practitioner's and typically subject the players to realistic crisis scenarios in the context of political constraints, alliance management, escalating issues and situations etc which govern the high level decision making. Operational-level military war-games focus on a more detailed look at the aspects pertaining to the conduct of military war and are used to study the feasibility and impacts of given military options such as to strike Iranian nuclear facilities or to implement naval engagements to retard Iranian actions on the Strait of Hormuz (Perla, 1990)[29].

Another key aspect of Iran wargaming is the use of red team analysis to make informed guesses at, and attempt to duplicate, adversary decision-making and strategy. Whereas effective deterrence depends on the quality of models of adversary behaviour, red team exercises help to challenge conventional models of responses to pressures being applied by Iran, particularly. The arguments that will be presented provide a basis for the practice of red team modeling by examining how the Iranians behave in crisis situations, such as the Incidents over their tankers in the 1980s, negotiations on JCPOA, and repeating actions and reactions after the assassination of Solimani in 2020. The findings resulting from careful red teaming efforts can also be surprising: Iran has repeatedly been able to show significantly more strategic maturity and self-restraint than presumed in previous assessments of deterrence that relied on stereotypical images of irrational and rash Iranian leadership (Eisenstadt, 2011)[30].

Wargaming is not just an analytical tool; it is also a means of signalling deterrence and communication. The public announcement of wargaming exercises, especially the large-scale, joint military wargaming activities of more than one allied country, provide clear indications of capabilities, resolve, and inter-alliance cohesion. Joint Israel-Gulf exercise have been used by the United States many times to demonstrate regional security consideration and their willingness to respond to Iranian provocations (Cronin, 2019)[31]. Likewise, the Iranians have been regularly conducting exercises themselves, such as drills on attacking carrier strike groups, large-scale missile drills and naval blockade even in the Strait of Hormuz, acts that are deterrence communication both against the United States and Israel.

In a sense of 'forward deterrence' the importance of the signalling function of wargaming is highlighted: to influence adversary calculations in the run-up to war, rather than after. In doing so, the United States tells Iran through its actions that if it attempts to block the Strait of Hormuz, to attack U.S. bases in the region or to assist a proxy strike on Israel, anything it does will result in massive and coordinated U.S. military response. The same message of deterrence in the forward direction is expressed in Israel's air force exercises that practice long-range strike missions – there is no Iranian military development, no matter how hard it is to find and how well it is protected, beyond Israeli strike reach (Cohen & Frankel, 1990: Inbar & Shamir, 2014)[32].

Combined Israeli-American-allied air defence response to the April 2024 range beating Iranian missile and drone attack on Israel, gave America and Israel a compelling application of forward deterrence signalling. The simultaneous

28 Davis, P. K., & Arquilla, J. (1991). Deterring or coercing opponents in crisis: Lessons from the war with Saddam Hussein. RAND Corporation.

29 Perla, P. P. (1990). The art of wargaming: A guide for professionals and hobbyists. Naval Institute Press.

30 Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

31 Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

32 Cohen, A., & Frankel, B. (1990). Opaque nuclear proliferation. Journal of Strategic Studies, 13(3), 14–44; Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century. Routledge.

shooting down of Iranian projectiles by Israeli, American, British, French and Jordanian actors meant it was only too clear that any future direct Iranian attack on Israel would be met by a multi-nation, tightly knitted defence network, significantly boosting the cost to Tehran of options should it decide to opt for retaliatory action. This 'show' part of the demonstration effect is a 'wargaming in reverse,' through a real world event, to impart a sense of deterrence capability that a simulated exercise cannot convey as effectively.

The Role of Technology in Contemporary Warfare

Technology, particularly involving simulation, data analysis, and artificial intelligence, has revolutionized modern wargaming in the Iran–Israel–US arena. Recent high resolution computer simulations have been able to simulate the physical results of kinetic strikes against hardened targets to a fairly high degree of accuracy, allowing planners to make more confident assessments of the likely effects of strike packages against Iran's nuclear facilities than they could previously make using other means (Davis & Arquilla, 1991)[33]. Using AI to create a simulated opponent that mimics an adversary's doctrine and historical patterns can produce a more realistic opponent that adapts to the player's choices.

Cyber and information domains have been introduced into wargaming, bringing new complexity that is testing traditional simulation methods. Cyber operations are conducted in different landscapes than kinetic operations, technical landscapes in cyber operations change quickly, there is significant uncertainty over attribution in cyber operations, and escalatory dynamics in cyber operations are not well represented in traditional military simulation models (Rid, 2013)34. An area of methodological innovation emerging is the development of integrated wargaming frameworks that integrate kinetic, cyber, information, and economic aspects, given the understanding that the Iran–Israel–US competition is a competition across all these domains. Creating a realistic and practical multi-domain simulation environment is still a difficult task, and a joint effort will be needed between the military planners and the technical and social science experts.Another key aspect of technological progress in wargaming is integration of intelligence. Classified intelligence on Iran's military capabilities, strategic intentions and leadership dynamics can provide the basis for a war game to be based on realistic representations of adversary capabilities and behaviour. Satellite, signals and human intelligence inputs can be fed into scenarios for the purposes of wargaming to produce more realistic scenarios. Handling classified information in a war game is not a trivial task that involves adequate information management systems and security measures to capture and share it, while at the same time protecting sources and methods.

Iranian Strategic Tools: Asymmetric Power Projection and the Axis of Resistance

Iran's strategic tool kit is an elaborated adaption to material limitations. The technological capability of the conventional military forces of the United States and Israel, plus the qualitative advantage of the latter, is something that Iran cannot match, and it attempts to make up for these shortcomings by creating a multi-layered strategy for power projection based on its geographical location, ideology, and organisational strength. This approach of Iranian strategists, dubbed strategic patience and managed deterrence, is an integrated strategic posture, which unites long-range missile power, proxy networks, information warfare, cyber warfare and economic warfare in a single strategy (Saab, 2018; Eisenstadt, 2011)[35].

The Islamic Revolutionary Guard Corps (IRGC) is Iran's foremost forward deterrence institution. The IRGC has organised, trained, equipped, and advised non-state armed groups, creating and developing an Axis of Resistance that includes Shia militia groups in Iraq under the banner of the Popular Mobilisation Forces, the Syrian government forces, and the Houthis (Ansarallah) in Yemen, and Hamas and Palestinian Islamic Jihad in the Gaza Strip and the West Bank, and Hezbollah in Lebanon (Byman, 2019)[36]. This network, with geographically distributed forward deterrence assets that can threaten Israel and U.S. regional interests at the same time from multiple angles, will dramatically complicate military planning by the adversary and increase the costs of any direct attack on Iranian territory.

The ballistic and cruise missile programme is perhaps the most important conventional military development for Iran in terms of strategic importance. Iran possesses a missile force estimated at more than 3,000 ballistic missiles of

33 Davis, P. K., & Arquilla, J. (1991). Deterring or coercing opponents in crisis: Lessons from the war with Saddam Hussein. RAND Corporation.

34 Rid, T. (2013). Cyber war will not take place. Oxford University Press.

35 Saab, B. Y. (2018). The coming Gulf war: Iran, the United States and their proxies. Foreign Affairs, 97(4), 10–17; Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

36 Byman, D. (2019). Iranian foreign policy and the sponsorship of terrorism. The Brookings Institution Press.

various ranges, giving it the ability to strike anywhere in the Middle East and throughout Israel, and all U.S. bases in the Middle East (Cordesman, 2014)[37]. Key systems include the Shahab-3 medium-range ballistic missile (MRBM) that has a range of around 2,000 km, Khorramshahr and Emad series precision-guided missiles and Fateh-110 short-range ballistic missile (SRBM) with proven accuracy. The first direct attack on Israel from Iran in history was on April 2024, when more than 300 projectiles were fired, including ballistic missiles, cruise missiles and drones, and gave real-life data on Iranian missile capabilities, as well as the effectiveness of multi-layered Israeli and allied air defenses.

Drone programs have proven to be an especially cost efficient and flexible device for Iran's forward deterrence. The Shahed-136 loitering munition has proven that use of a relatively simple and low-cost weapon system can be sufficient to outnumber and outgun more sophisticated air defence systems, especially when fired in large numbers, as Russia has now done in Ukraine and has done for Houthi and Iraqi proxy forces. Iranian drone technology includes tactical reconnaissance drones, long-range drones that can reach targets far into enemy territory, and other advancements. Combined arms strikes with drones and missiles as seen in the April 2024 attack on Israel is a big leap forward in Iranian offensive capability and a big challenge to those who plan deterrence (Cronin, 2019)[38].

Since the 2010 revelation of Stuxnet, which showed the vulnerability of Iranian critical infrastructure to sophisticated cyberattack, the cyber capabilities of Iran have seen a significant improvement. Iran reacted to the impact of Stuxnet by heavily investing in its offensive cyber capabilities, creating the IRGC Cyber Command and other organisations tasked with offensive operations against opponent networks. Iranian cyber operations have included distributed denial-of-service attacks against U.S. financial institutions, cyber attacks against Saudi Aramco and the Shamoon malware, and extensive espionage against Israeli government and military systems (Rid, 2013)[39]. These cyber operations are for forward deterrents to show off the capacity to inflict asymmetric costs on a host of adversaries without going over the threshold of conventional military action, in order to broaden the deterrence envelope beyond conventional military actions.

Economic tools and sanctions countermeasures also are components of Iran's strategic tool kit. With the massive U.S.-led sanctions, Iran has devised ways to evade financial limitations by engaging in barter deals, cryptocurrency trading, and trade deals with China, Russia, and other regional countries who are in its camp. Iran also has made efforts to make use of its status as a significant oil and gas producer to develop connections with energy importing countries that are willing to keep maintaining business relations despite the pressure from the United States. Iran has substantial economic leverage, provided by the risk of disrupting oil flows through the Strait of Hormuz, through which some 20 percent of the world's oil trade travels, as a deterrence against escalatory U.S. action (Cordesman, 2014)[40].

One of the areas that Iranian information operations and narrative management have introduced is an aspect that is underestimated in the arsenal of its strategic capabilities. The Islamic Republic is able to project itself with sophisticated skills using Arabic satellite TV (Al-Alam, Al-Manar), social media and pro-IRI media outlets in the region. Such capabilities can help Iran to challenge the information landscape, to spin conflicts in ways that suit its own agenda (such as highlighting Palestinian rights, opposition to America's imperialism, and regional unity) and perhaps to sway public opinion in opposition countries and beyond. Wargaming also makes use of information operations, as the increasing dimensions of the information environment in simulations consider how competing narratives might affect the political environment in which military operations take place.

Israel being small, strategically isolated nation facing hostile neighbours, needing to be both quality militarily superior and intelligence superior to its adversaries to compensate for its numerical weakness (Cohen, 1998)41. Since the mass armour and infantry battles of the Yom Kippur War in 1973, Israel's strategic toolkit has grown significantly, alongside its increased focus on precision strike capabilities, advanced air defence systems, the integration of intelligence, and what Israeli military doctrine calls the Campaign Between the Wars (Mabam in Hebrew): a sustained series of covert and semi-covert operations carried out to ensure that Iran does not allow Hezbollah and other proxy forces to build up their weapons stockpiles in Syria and Lebanon (Eisenstadt, 2011)[42].

37 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.

38 Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

39 Rid, T. (2013). Cyber war will not take place. Oxford University Press.

40 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.

41 Cohen, A. (1998). Israel and the bomb. Columbia University Press.

42 Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

The Israel Defence Forces is widely considered to have the most capable air force in the Middle East, with advanced variants of the F-15 and F-16 in service and the fifth-generation F-35I (known as Adir) the first operational air force anywhere outside the USA to deploy it. Israeli air strike capabilities are complemented by long-range standoff munitions such as the Rampage missile (which is launched from an aircraft and can carry a warhead to a range of up to 600 km) and a number of precision-guided bombs, which give the IAF the ability to strike targets at distance of up to Iran with in-flight refuelling (Inbar & Shamir, 2014)[43]. Strike packages are normally developed in Israel to eliminate or neutralize an enemy air defense system before launching precision weapons on high-value targets, a tactic that Israel has used on many occasions during the Campaign between the Wars over Syria.

Another strategic weapon is Israel's multi-layered air-defence system. Israel's combination of short-range rockets and artillery defence – the Iron Dome – together with Trophy active protection system for armoured vehicles, David's medium-range air defence system, and ballistic missile defence – Arrow 2 and Arrow 3 – forms a layered defence against short-range rockets and medium- to long-range ballistic missiles (Inbar & Shamir, 2014)44. The April 2024 Iranian attack proved to be a major operational trial of this architecture, yielding an intercept rate above 99% – a feat achieved by Israel's own systems and those of the U.S., British, French and Jordanian governments. This is proof of interoperability, and it is an important asset in front of Iran now because when they are striking, they have to plan to saturate an interoperable multi-nation system of integrated air defence, not just Israeli systems.

Perhaps Israel's most unique and significant strategic asset is its intelligence capability. The Mossad's record of entering Iran, even to assassinate nuclear scientists, as well as the 2018 operation in which it extracted an entire nuclear archive from a Tehran warehouse, and the killing of IRGC officers within Iran, indicates the extent to which the organization has been able to penetrate into Iranian territory, thereby providing powerful forward deterrence capabilities (Sanger, 2012)[45]. The mere fact that Israeli intelligence is able to identify, locate and strike a high value target anywhere in Iran provides an enormous psychological and operational deterrence to Iranian decision makers and military planners. This intelligence superiority also translates into high accuracy targeting when it comes to wargaming scenarios—the Israeli planners have a high level of knowledge about the Iranian military infrastructure, command networks and hardened facility locations.

Israel's cyber capabilities are a premier offensive capability in the world, and they are developed in close cooperation with the United States and are mostly housed under the umbrella of Unit 8200 of the IDF Intelligence Corps. The Stuxnet operation, believed to have destroyed around 1,000 Iranian centrifuges and hindered Iran's nuclear program by about two years, showed the potential of sophisticated cyber-attack to reach strategic goals previously thought to be kinetic military attacks (Sanger, 2012; Lindsay, 2013)[46]. Other Israeli cyber operations have specifically targeted Iran's nuclear control systems, industrial infrastructure and transportation systems. The use of cyber means in Israeli forward deterrence strategy is indicative of the understanding that cyber action can be employed to exact significant costs on Iran, while keeping the risk of escalation to a minimum, and while being possible to deny to the adversary.

The Campaign between the Wars (Mabam) is a unique Israeli foray into the theory and practice of forward deterrence and is worthy of special analysis. This ongoing series of military attacks has targeted the transfer of advanced weapons to Hezbollah through Syria, interference in Iranian military networks in Syria and the killing of Hezbollah and Iranian leaders involved in arms transfers. The campaign, which has taken place over a decade in hundreds of strikes, is an application of the forward deterrence logic: to move one step ahead of the enemy and prevent him from concentrating and deploying against Israel, thus leaving things favourable for the IDF (Inbar & Shamir, 2014; Eisenstadt, 2011)[47].

A key element of Israel's strategic arsenal is its diplomatic apparatus, such as the Abraham Accords normalisation process and the establishment of security cooperation agreements with the Gulf States. Israel's military and intelligence ties with the United Arab Emirates, Bahrain, and Saudi Arabia have been strengthened, adding to the multi-lateral nature of Israel's deterrence and providing the countries with new avenues to coordinate strategy against a common

43 Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century. Routledge.
44 Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century. Routledge.
45 Sanger, D. E. (2012). Confront and conceal: Obama's secret wars and surprising use of American power. Crown Publishers.
46 Sanger, D. E. (2012). Confront and conceal: Obama's secret wars and surprising use of American power. Crown Publishers; Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.
47 Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century. Routledge; Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

enemy, Iran. CENTCOM (U.S. Central Command) authority over Israel in 2021—an area it previously did not have jurisdiction over—has helped to increase operational cooperation between Israel's military command and the U.S. regionals, including the CENTCOM command, and played a role in the coordinated response to the Iranian April, 2024 attack.)

Along with Israel the unique defence posturing and hard power capabilities of America in today's world make it even more unpredictable in the current geo-strategic competition with Iran accompanied with Israel: the most interconnected terrestrial military force with a presence in all physical domains and surrounded by an integrated cyber domain, the most extensive military alliance network — covering most of the world's economic and military power — and the most high-tech military industry, capable of producing advanced military technology at scale. U.S. strategic options in the context of deterring Iran and aiding Israel include forward-deployed troops, high-end strike capabilities, missile defence integration, comprehensive alliance management, economic sanctions, support to Israeli intelligence, and counterintelligence (CI) and cyber capabilities (Cronin, 2019; Indyk, Lieberthal & O'Hanlon, 2012)48.

Presence of U.S. troops in the area is the base from which credible deterrence works against Iran. The U.S. Fifth Fleet is permanently deployed to Bahrain to keep a military naval presence in the Persian Gulf and surrounding waters. The region is supported by air superiority, precision strike and intelligence collection capabilities that are based at Al Udeid Air Base in Qatar, Al Dhafra in the UAE and Incirlik in Turkey. Special Operations Forces are deployed across the area to deliver training, advising and direct action operations in order to increase the capabilities of partner nations and offer immediate strike assets. The total of these forward deployed forces, in turn, represents a deterrent presence – both in terms of capability and will – for regional security guarantees (Cordesman, 2014)49.

The unique flexibility and scalability of a deterrence tool in the Iran context is the capability of U.S. naval power projection in the form of carrier strike groups (CSGs) centred around nuclear-powered aircraft carriers. A carrier strike group that deployed to the Gulf area indicated the presence of some 70 to 80 combat aircraft, as well as surface combatants and submarines capable of launching Tomahawk cruise missiles, and full air defence capability. Since the October 2023 Hamas attack on Israel, two carrier strike groups have been deployed to the Eastern Mediterranean, showcasing U.S. conventional military force projection capability to send a deterrence signal quickly once more. Such deployments are typical forward deterrence measures, designed to tell Iran and Hezbollah that upsetting Israelis, if they genuinely decide to do so, will incur the wrath of both Israel and America.

Targeted sanctions, an instrument of economic coercion, is one of the favorite instruments that the United States has used in its strategic competition with Iran. In addition to the Comprehensive Sanctions that would be reimposed after the U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA) in 2018, the sanctions would also target Iranian oil exports, access to the banking system, which has been done via exclusion from the SWIFT banking system, Iranian arms transfers, and Iranian official personal finance. (Litwak, 2012)50 Much has been written about the effectiveness of sanctions in effecting a change in Iranian strategic behaviour (Iran's uranium enrichment has continued despite sanctions, and its proxy network has expanded), but the fact that sanctions have taken place for a few years, in all, has slowed down Iranian defence expenditure, reduced its ability to acquire new technology, and put some strain on the Iranian leadership, even domestically.

America has also made a major effort to create and sustain the regional alliance structure that supports forward deterrence. That was the case with the Abraham Accords of 2020, according to which Israel signed a normalisation deal with the United Arab Emirates, Bahrain, Sudan and Morocco, creating a major realignment of regional politics in favor of the anti-Iranian unity, and allowing for unprecedented Israeli-Arab military cooperation. Israel has, and continues to, extensively expand intelligence-sharing capacities with Gulf states and the U.S. in a distributed surveillance network that can improve situational awareness throughout the region. Weapons sales to the regional coalition make military deterrence more potent and need for U.S. forces less direct, such as sale of advanced fighter aircraft, missile defence systems and precision-guided munitions.

The forward deterrence narrative with Iran has been couples with a massive yet mostly underground U.S. cyber capability — built and wielded by the Cyber Command and National Security Agency elements. In addition to this publicly disclosed and politically significant Stuxnet' operation, U.S. cyber operations have been used to disrupt Iranian military communications, jam air defence systems, and to 'cost' the IRGC financial networks. Persistent

48 Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press; Indyk, M., Lieberthal, K., & O'Hanlon, M. (2012). Bending history: Barack Obama's foreign policy. Brookings Institution Press.

49 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.

50 Litwak, R. S. (2012). Deterring nuclear Iran: A guide to evaluating policy options. Wilson Center.

engagement doctrine, as developed by U.S. Cyber Command, which argues that the constant presence of U.S. cyber operations in adversary networks is fundamental to deterrence signalling and intelligence collection is an example of how cyber operations are being incorporated into the forward deterrence architecture (Rid, 2013)[51].

The institutional aspect of the U.S. strategic tools should be called to attention. The International Atomic Energy Agency (IAEA) system of inspections, bolstered by the diplomatically-based pressure applied by the United States, offers leverage for pressure and a monitoring mechanism to increase transparency regarding Iran's nuclear program. Sanctions and other measures for achieving the goal of coercion provide multilateral legitimating framework at the UN Security Council where United States possesses a veto power. The Financial Action Task Force (FATF), which is dominated by U.S. interests, has established a framework of regulations which limits Iranian access to foreign financial institutions. The institutional tools together with the military and cyber tools provide a multi-layered coercive architecture which is simultaneously used on the diplomatic, financial and informational dimensions.)

Comparative Assessment: Strategic Tools in Interaction

A comparative analysis of the strategic tools deployed by Iran, Israel, and the United States reveals a dynamic of asymmetric competition in which each actor's strengths are matched against the others' vulnerabilities in ways that produce complex and potentially unstable deterrence equilibria. The United States possesses overwhelming conventional superiority but is constrained by domestic political limits on military engagement, alliance management obligations, and the risk of triggering Iranian proxy responses that could destabilise the region. Israel possesses exceptional qualitative military capabilities and intelligence dominance but is geographically small and vulnerable to missile attacks from multiple directions. Iran is militarily outmatched in conventional terms but has constructed an asymmetric deterrence architecture—combining long-range missiles, forward-deployed proxies, cyber capabilities, and economic leverage—that imposes significant costs and constraints on adversary strategic planning (Byman, 2019; Eisenstadt, 2011)[52].

The interaction of these tool sets in practice creates a complex deterrence dynamic characterised by continuous competitive adaptation. Iranian investments in missile accuracy and payload drive Israeli and U.S. investments in more capable missile defence. Israeli and U.S. cyber operations against Iran's nuclear programme drive Iranian investments in offensive cyber and physical security of nuclear infrastructure. U.S. sanctions designed to constrain Iran's defence budget drive Iranian development of low-cost asymmetric tools—drones and proxy forces—that can be produced domestically without access to international markets. This action-reaction dynamic has produced a competitive environment of remarkable intensity and sophistication, in which each actor continuously learns from and adapts to the others' strategies and capabilities. Wargaming serves as a critical tool for tracking and anticipating these competitive dynamics, enabling planners to explore the second and third-order consequences of strategic choices before they are implemented in the real world.

One particularly significant interaction pattern involves the relationship between Iranian proxy activation and U.S. deterrence credibility. When Iranian proxy forces attack U.S. assets—as Iraqi militias did repeatedly following the October 2023 Hamas attack—the United States faces a dilemma between responding forcefully enough to restore deterrence credibility and restraining its response enough to avoid escalation to direct conflict with Iran. U.S. responses that are perceived as insufficient by regional partners may undermine extended deterrence commitments, while responses that are too forceful risk triggering Iranian counter-escalation. Managing this dilemma has become a central challenge for U.S. forward deterrence strategy and a recurring theme in wargaming exercises focused on the Iran–Israel–US competition.

The foregoing analysis demonstrates that forward deterrence has become the dominant operational logic governing strategic competition among Iran, Israel, and the United States. All three actors have moved beyond purely defensive deterrence postures toward active strategies of shaping the adversary's strategic environment before conflict begins. This convergence toward forward deterrence reflects shared recognition that in a world of hybrid warfare, where grey-zone operations, proxy conflicts, and cyber-attacks are the primary instruments of strategic competition, passive deterrence is insufficient to protect core interests. The challenge going forward is to manage the escalatory risks inherent in a strategic environment where all major actors are simultaneously pursuing forward deterrence strategies that push continuously against one another's red lines (Freedman, 2004; Gray, 1999)[53].

51 Rid, T. (2013). Cyber war will not take place. Oxford University Press.

52 Byman, D. (2019). Iranian foreign policy and the sponsorship of terrorism. The Brookings Institution Press; Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

53 Freedman, L. (2004). Deterrence. Polity Press; Gray, C. S. (1999). Modern strategy. Oxford University Press.

The October 2023 Hamas attack and its aftermath—involving the most extensive direct Iranian attack on Israel in history in April 2024, Houthi attacks on Red Sea shipping affecting global commerce, and Iraqi militia strikes on U.S. bases that killed American service members—demonstrated the real-world costs and risks of the current forward deterrence dynamic. Each of these events had been anticipated in various wargaming scenarios, yet the specific combinations and sequencing of events exceeded most planners' expectations, highlighting the inherent unpredictability of complex strategic systems. The period also demonstrated the resilience of the multi-layered Israeli-allied air defence architecture and the limits of Iranian proxy operations in producing decisive strategic effects, providing important empirical data for updating wargaming models.

The future trajectories of Iran-Israel-US strategic competition will be shaped by several emerging technological and geopolitical dynamics that current wargaming frameworks are only beginning to incorporate. Artificial intelligence applications in military decision-making, particularly AI-assisted targeting, autonomous drone swarms, and AI-enabled information operations, have the potential to fundamentally alter the tempo and character of conflict in ways that challenge established deterrence frameworks (Davis & Arquilla, 1991)54. If AI systems can compress decision-making timelines in ways that outpace human oversight, the risk of inadvertent escalation through automated responses to perceived threats increases significantly. Wargaming frameworks will need to incorporate AI decision agents to explore these dynamics and develop appropriate safeguards.

Hypersonic weapon systems, missiles capable of flying at more than five times the speed of sound with manoeuvrable trajectories that defeat traditional ballistic missile defence systems, represent another emerging challenge. Iran has announced development of hypersonic missile systems, and while independent verification of claimed capabilities is difficult, the trajectory of Iranian missile technology development suggests that hypersonic delivery systems will eventually enter the Iranian arsenal (Cordesman, 2014)55. The implications for Israeli missile defence architecture, which currently relies heavily on kinematic intercept systems calibrated for ballistic trajectories, are significant. Wargaming exercises will need to explore the implications of hypersonic threats for Israeli, U.S., and allied defence planning, and potentially for the entire logic of deterrence by denial that underpins current missile defence investment.

The militarisation of space and the growing dependence of all three actors on space-based assets for intelligence, navigation, communication, and missile guidance introduce another dimension of strategic competition that wargaming frameworks are increasingly incorporating. Israel's Ofeq reconnaissance satellite series, U.S. military space assets, and the growing Iranian space programme, whose ostensibly civilian launchers provide relevant ballistic missile technology, all represent investments in space-based capabilities with direct military applications. The vulnerability of these assets to anti-satellite weapons and the cascading effects of space asset degradation on terrestrial military operations represent important scenarios for future wargaming exploration (Shlapak & Johnson, 2016)56.

Conclusion

This paper has traced the intellectual and strategic evolution from classical deterrence theory to forward deterrence, and has situated this evolution within the specific context of the Iran–Israel–US strategic triangle and its wargaming practices. The central argument has been that forward deterrence—proactive, multi-domain, and continuously adaptive—has become the dominant strategic logic governing the competition among these three actors, reshaping military doctrines, strategic tools, and simulation methodologies in profound ways.

Classical deterrence theory provided the essential conceptual vocabulary—capability, credibility, communication—but proved insufficient for capturing the complexity of a strategic environment characterised by hybrid warfare, proxy conflicts, and continuous grey-zone competition. Forward deterrence extended this vocabulary to encompass pre-emptive strike doctrines, coercive military posturing, proxy warfare, economic coercion, cyber operations, and information campaigns, integrating them into coherent strategic architectures that operate across the full spectrum from covert action to overt military confrontation. Each of the three actors has developed a distinctive forward deterrence posture that reflects its specific capabilities, constraints, and strategic objectives: the United States leverages multi-domain conventional superiority and alliance architecture; Israel leverages intelligence dominance, cyber capabilities, and precision strike; Iran leverages asymmetric proxy networks, long-range missiles, and economic leverage over energy flows.

54 Davis, P. K., & Arquilla, J. (1991). Deterring or coercing opponents in crisis: Lessons from the war with Saddam Hussein. RAND Corporation.

55 Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.

56 Shlapak, D. A., & Johnson, M. (2016). Reinforcing deterrence on NATO's eastern flank: Wargaming the defence of the Baltics. RAND Corporation.

Wargaming has evolved correspondingly, expanding from traditional kinetic military simulations to multi-domain exercises that incorporate cyber, information, and economic dimensions. Wargaming serves not only as an analytical tool for testing strategic assumptions and refining operational plans but also as an instrument of strategic communication and deterrence signalling. The increasing sophistication of wargaming methodologies—incorporating artificial intelligence, high-resolution physical simulation, and multi-agency participation—reflects the growing complexity of the strategic environment and the corresponding demand for more realistic and comprehensive analytical frameworks.

The period ahead will be defined by the interaction of intensifying forward deterrence competition with emerging technological disruptions—artificial intelligence, hypersonic weapons, space competition—that threaten to destabilise existing deterrence equilibria. Managing these dynamics will require continued investment in sophisticated wargaming capabilities, sustained diplomatic engagement, and the development of shared norms for managing competition in emerging domains. The stakes are high: miscalculation in this strategically dense and technologically dynamic environment could trigger conflicts with catastrophic regional and potentially global consequences. Understanding the evolution from deterrence to forward deterrence, and embedding that understanding in rigorous wargaming practice, is not merely an academic exercise but an urgent strategic necessity.

Bibliography.

Brodie, B. (1946). The absolute weapon: Atomic power and world order. Harcourt, Brace and Company.

Brodie, B. (1959). Strategy in the missile age. Princeton University Press.

Byman, D. (2019). Iranian foreign policy and the sponsorship of terrorism. The Brookings Institution Press.

Cohen, A. (1998). Israel and the bomb. Columbia University Press.

Cohen, A., & Frankel, B. (1990). Opaque nuclear proliferation. Journal of Strategic Studies, 13(3), 14–44.

Cordesman, A. H. (2014). Iran and the Gulf military balance. Center for Strategic and International Studies.

Cronin, A. K. (2019). Power to the people: How open technological innovation is arming tomorrow's terrorists. Oxford University Press.

Davis, P. K., & Arquilla, J. (1991). Deterring or coercing opponents in crisis: Lessons from the war with Saddam Hussein. RAND Corporation.

Eisenstadt, M. (2011). Iran's Islamic Revolutionary Guard Corps: A study of organizational change. Washington Institute for Near East Policy.

Freedman, L. (2004). Deterrence. Polity Press.

Gray, C. S. (1999). Modern strategy. Oxford University Press.

Huth, P. K. (1988). Extended deterrence and the prevention of war. Yale University Press.

Inbar, E., & Shamir, E. (Eds.). (2014). Israel's national security challenges in the 21st century.

Routledge.

Indyk, M., Lieberthal, K., & O'Hanlon, M. (2012). Bending history: Barack Obama's foreign policy. Brookings Institution Press.

Jervis, R. (1976). Perception and misperception in international politics. Princeton University Press.

Kahn, H. (1965). On escalation: Metaphors and scenarios. Frederick A. Praeger.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404.

Litwak, R. S. (2012). Deterring nuclear Iran: A guide to evaluating policy options. Wilson Center.

Morgan, P. M. (2003). Deterrence now. Cambridge University Press.

Perla, P. P. (1990). The art of wargaming: A guide for professionals and hobbyists. Naval Institute Press.

Posen, B. (1984). The sources of military doctrine: France, Britain, and Germany between the world wars. Cornell University Press.

Quackenbush, S. L. (2011). Deterrence theory: Where do we stand? Review of International Studies, 37(2), 741–762.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Saab, B. Y. (2018). The coming Gulf war: Iran, the United States and their proxies. Foreign Affairs, 97(4), 10–17.

Sanger, D. E. (2012). Confront and conceal: Obama's secret wars and surprising use of American power. Crown Publishers.

Schelling, T. C. (1960). The strategy of conflict. Harvard University Press.

Schelling, T. C. (1966). Arms and influence. Yale University Press.

Shlapak, D. A., & Johnson, M. (2016). Reinforcing deterrence on NATO's eastern flank: Wargaming the defence of the Baltics. RAND Corporation.

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley.