

# Is Indian Deterrence Effective Against Potential Aggressors?

Lieutenant General PR Kumar, PVSM, AVSM, VSM (Retd)<sup>\*</sup>

## Abstract

*The concept of deterrence is undergoing transformation in the emerging multi polar and multi nuclear world. The democratic world order and international institutions are being challenged, leading to a dynamic international security environment, where strategic balancing by even the global powers has become the norm. This has resulted in 24 X 7 Multi Domain Operations (MDO), where the military dimension is but one of the verticals albeit a decisive one. Applied effectively, deterrence discourages an adversary from pursuing an undesirable action. It works by changing the adversary's calculation of costs, benefits and risks.*

*The assumption that 'modern weapon systems are so destructive that no sane leader would risk igniting a war – and so the requirements of deterrence are relatively modest' is profoundly misplaced. Military competition is expanding to several new domains, from space and cyberspace to information and sea bed. New capabilities and disruptive technologies are making it harder to accurately gauge the military balance of power. More vitally, they make identification and attributability of adversary difficult and complicated, changing the landscape of confrontation, conflict and whom to deter. For India, our immediate neighbours, China and Pakistan (strategic partners), with unresolved border disputes are challenging our strategic space. China, an Asian*

---

<sup>\*</sup>This is an edited version of the 17th Major General Samir Sinha Memorial Lecture 2019, delivered by Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd), on 10 Jul 2019 at the USI.

<sup>®</sup>Lieutenant General PR Kumar, PVSM, AVSM, VSM (Retd) was commissioned into the Regiment of Artillery on 15 Dec 1976. He has held the appointment of Director General of Army Aviation. He superannuated, after 39 years of service, as Director General of Military Operations. He keeps abreast with contemporary strategic and security related issues worldwide.

*goliath, will remain an adversary for the distant future. Deterrence by denial is a national imperative.*

*Warfare has already transcended the domains of soldiers and military affairs, and is increasingly becoming a matter for politicians, scientists, bankers and the 'common man'. Adversaries, such as China, have expanded the battlefield in time (a blurred distinction between peace and war), in domains (space, cyberspace and information), and in geography (including the hinterland/homeland) to create strategic, operational and tactical standoff. In a state of continuous competition, all nations exploit the conditions of operational environment to achieve their objectives without resorting to armed conflict by fracturing the adversary's resolve. We must focus on a capability based armed force to script future joint task forces for conducting operations in support of the nation and provide credible deterrence.*

*Warfare itself, and certainly deterrence, is not a numbers game. For India, a two front conflict scenario will prove a big challenge. While India will employ its Comprehensive National Power (CNP), and its entire repertoire of strategic tools, to avoid a two-front war, strategic prudence dictates that we must be prepared to confront and fight such a war and be prepared to prosecute MDO 24X7 along with other instruments of national power. Increase in number of Nuclear Weapon States (NWS), MDO specially in the cognitive and non-kinetic domain, high-technology delivery systems and munitions have made warfare more destructive. Increased transparency, difficulty of attribution for response, nations exploiting below the war threshold line to achieve strategic objectives, expansion and compression of the battle field have contributed to the ambiguity of deterrence.*

*Deterrence requires a national strategy that integrates political, diplomatic, military, and economic powers. We must develop strategies, plans and operations to effectively counter specific adversaries.*

*Deterrence must convince adversaries not to take actions that threaten India's vital interests. Decisive influence is achieved by credibly threatening to deny benefits and impose costs, while encouraging restraint. Deterrence must be planned and executed across all domains in concert with other elements of national and international power.*

*Recent studies regarding psychological dimension of human decision-making raise questions about the very logic of deterrence. Information Influence Operations (IIO) and weaponisation of social media are new game changers. Cyber warfare has further eroded effectiveness of deterrence and its ever increasing potency has alarmed the world. The distinction between online and offline confrontation has become blurred. Diplomacy, and to a large extent even confrontation and conflict, have become less private and policy-oriented. China and Pakistan are already playing this deadly game against us.*

*The article examines the aspect of effectiveness of Indian deterrence against our adversaries. MDO provide India with hitherto unused domains like cyber, IIO and space. A collusive China-Pakistan in our immediate neighbourhood, rising trend of ultra-nationalism infecting our immediate neighbours and contested strategic space of Asia and fluid internal security situation, dictate that India must get its act together, continue building its CNP, militarily transform into MDO capable armed forces and get its multi domain deterrence capabilities in place for specific nations and scenarios. India must rethink its deterrence strategy in changing geo-political and strategic environment, including psychology of decision making. 'Deterrence by Denial' against adversaries, will continue to remain the first priority for India.*

*"Even the Fruits of Victory would be Ashes in our Mouth"*

President John F. Kennedy during  
the Cuban Missile Crisis

## Introduction

The concept of deterrence is undergoing a transformation in the emerging multi polar, multi nuclear world, where the liberal democratic world order and international institutions are being challenged, leading to a dynamic international security environment where strategic balancing by even the global powers has become the norm. This has resulted in 24 X 7 Multi Domain Competition, where the military dimension is but one of the verticals albeit a decisive one.

Dr Atul Gawande, a general and endocrine surgeon of Indian origin practicing in Boston, USA, in the phenomenal bestseller titled “Being Mortal”, to a question by a relative about a terminally ill parent, “Dr, so how long has he got”, answers ‘technically as long as we want’. What he meant was that modern medicine has advanced so far that they can keep humans alive using modern technology. But the issue is the ‘quality of life he will live’. Similarly, when it comes to Indian deterrence against potential aggressors, a quick response is ‘Yes and No or even Not Yet’; Yes on strategic and existential issues, No on tactical actions by adversaries and Not Yet for the remaining. Ironically, it is the same for the superpower and global powers, USA, China or Russia, forget the lesser mortals. Most of us believe that despite the nuclear overhang, India has a window for prosecuting conventional operations against Pakistan. The same logic applies for and against us and our adversaries including China. In fact, when it comes to China, due to the stated nuclear policy of both countries, the conventional space gets formalised. Given the overwhelming and overbearing CNP of USA, increasingly many minor nations such as Iran, North Korea, Venezuela, Philippines, Syria and Pakistan are thumbing their noses at USA with impunity.<sup>1</sup> Naturally, there are geo-political, geo-strategic and technological reasons for that, but it is a pointer to deterrence. In today’s world of realpolitik, strategic balancing and engaging in competition<sup>2</sup> (also cooperation and confrontation when required) by nations is in itself ‘a form of engaging in deterrence operations’. This also validates the popular quote ‘there are no permanent friends or enemies, only permanent interests’.<sup>3</sup>



### **Deterrence and Compellence**

While generically understood, it is wise to benchmark the dictionary definition of deterrence and compellence at the outset. Oxford dictionary defines deterrence as ‘the action of discouraging an action or event through instilling doubt or fear of the consequences’, and compellence as a ‘direct action that persuades an opponent to give up something that is desired’.<sup>4</sup> The Complex Deterrence Theory, General Deterrence Theory,<sup>5</sup> Immediate Deterrence Theory, as applicable between USA and Russia during Cold War period, and a lot of papers have emerged on deterrence in recent years. Applied effectively, deterrence discourages an adversary from pursuing an undesirable action. It works by changing the adversary’s calculation of costs, benefits, and risks. A country can, for instance, convince its adversaries that an attack is so unlikely to succeed that it is not even worth the attempt: deterrence through denial. Or a country may convince its adversaries that defeating it would be so costly as to be a victory in name only: deterrence through punishment. On 04 July 2019, American politician Mike Gallagher argued in The Washington Quarterly that while the US has traditionally relied on the deterrence through punishment, it must now move to deterrence by denial like the Chinese do; indicating a decline in CNP (specially military), growing clout of China, Russia and regional powers, increase in number of NWS and availability of hi-tech domains. In most cases, a rational adversary will decide to stay put.

The assumption that ‘modern weapon systems are so destructive that no sane leader would risk igniting a general war; and so the requirements of deterrence are relatively modest’ is profoundly misplaced. Increase in nuclear weapon holding states, assumption that Tactical Nuclear Weapons (TNWs) specially those which generate electromagnetic pulse (EMP) form part of conventional warfare and technology creating transparency is leading countries to contemplate ‘use it or lose it’ regarding nuclear weapons. Technological advancements, and potency and accuracy of conventional weapons, have coupled conventional and nuclear domains with alarming implications for deterrence. Military competition is expanding to several new domains, from space and cyberspace to information and sea bed (energy pipelines and data cables) and new capabilities and disruptive technologies are making it harder to accurately gauge the military balance of power. More

vitality, they make identification and attributability of adversary difficult and complicated, changing the landscape of confrontation, conflict and whom to deter. Meanwhile, advances in cognitive science are challenging the theoretical underpinnings of deterrence by upending our understanding of how humans behave in high-risk situations – such as facing the possibility of war. Taken together, these developments lead to an inescapable and disturbing trend. The greatest threat is neither multi polar world or great power rivalries nor the spread of advanced weaponry or niche technology available off the shelf, but the decline of deterrence.<sup>6</sup>

### **Overview of International Security Environment**

The liberal democratic world order established by the USA, and her allies, since World War II has not only changed but is also being challenged. The rapidity of change accelerated ever since 9/11 and launch of Global War on Terrorism (GWOT). We are living in paradoxical times and looking down a precipice; while at no point of mankind has the globe been more peaceful, healthier with man living longer, wealthier, better quality of life; concurrently we are looking at instantaneous mutually assured destruction, catastrophic global warming, biological and medical disasters, constant competition and confrontation for strategic space and resources which can any time result in conflict with high probability of turning global. The inevitable diminishing CNP and power projection capabilities of USA started the slide to a multi polar world with emergence of China as a global power and resurgence of Russia under President Putin. State controlled narratives leading to signs of ultra-nationalism; authoritarian governments like Philippines, North Korea, Syria, Turkmenistan; emerging powers with regional aspirations like Iran, Saudi Arabia, South Africa, Nigeria, Turkey, India which are not necessarily aligned with the thought process of a world order established and controlled by USA and her allies; rise of religious Islamic fundamentalism with a twist of occupying territory and establishing a caliphate like the Islamic State of Iraq and the Levant (ISIL); global warming and climate change indicators; transnational Multinational Companies (MNCs) with their own agendas, drug cartels and international crime syndicates have changed the world scape.<sup>7</sup> There is a renewed political, ideological, economic and military competition due to globalisation, which brought many good practices and developmental growth but is a major driver of instability and conflict.

While threat of full-scale conventional wars has gone down, correspondingly the span of conflict, its complexity, unpredictability, lethality, accuracy, reach and manifestation into many domains have emerged. The physical and nonphysical domains, including the cognitive, have expanded. There are no front, rear and flanks and there is no place to hide. Many new types of warfare have also emerged like hybrid, media, cyber, information, network, electromagnetic spectrum (EMS), asymmetric, big data and digital, waged either singularly or cross domain in peace, no war no peace, or war. The environment continues to change in four fundamental and interrelated ways: adversaries challenging established states and practices in all domains; the battlespace becoming more lethal; operational complexity increasing globally; and contextually deterring aggressive acts becoming more challenging. Creating and retaining strategic space within a state's area of interest calls for prosecuting multi domain activities/operations against other state and non-state actors leading to constant competition 24X7. We are in an 'era of persistent, constant engagement'. Ironically, this process is providing some level of stability in an otherwise increasingly incoherent, chaotic and turbulent world order. Nations have their national vision and aspirations and want to find their legitimate place amongst the comity of nations. India, the ancient, proud civilisation with a glorious history, too aspires for the same and we are destined by our geography, size, population, resources and history to be a great power in the world order. Specifically in Asia, 'The Continent of the Century', the US is desperate to assert and implement their vision of a rule-based order, freedom of navigation and overflight in the maritime commons, respect for international law, enhancing connectivity, maritime security, non-proliferation and terrorism. Clearly, these are in response to China's growing assertiveness in the region. India, naturally, must strengthen its deterrence capabilities to ensure a stable security environment to achieve its vision.

### **Theoretical Precepts of Global and Regional Security Zones**

International Relations Theory (IRT) and Regional Security Complex Theory (RSCT)<sup>8</sup> state that territorial pre-eminence (military/kinetic) is more potent and powerful than non-territorial domains in the security calculus. Regional security zones are fairly independent of globalisation and global political trends due to their strong emotional, geographical and historical links (ironically, it rings true

even for our Act East Policy – we need to Act Northeast before we can fructify a robust Act East policy, which addresses vulnerable China's underbelly, and can act as a deterrent). RSCT enables one to understand new alliances and structures to evaluate relative balance of power, and relationship between regionalising and globalising trends. The capabilities of global powers enable them to transcend distance, while lesser powers are satisfied with subsystem level interplay whose main security environment is their local region. The central idea in RSCT is that, since most threats travel easily over short distances, security interdependence is normally patterned into regionally based clusters or security complexes. The hope was that economic liberalisation will eventually generate political liberalisation and a lowering of threat perceptions, especially amongst non-liberal states like China, Russia, Iran and North Korea. In the security chess board, as the international system reaches global scale, room is created in which distinct regional security subsystems can emerge. A handful of states at the top of the power league play a truly global game, treating each other as a special class and projecting their power into far-flung regions. But for the great majority of states, the main game of security is defined by their near neighbours. China dominates the regional security zones of Asia (East, South-East and South Asia). Geography, specially as our disputed borders are in the remote, attrition causing high Himalayas, economics and trade realities, anti-access area denial (A2AD) and cost of intervention discourage physical intervention by any of our allies. India, unfortunately, is caught in the classical power play of global and regional security dynamics as it's not yet a great power. However, these dynamics will prevent or provide opportunities for India to emerge as a unique balancing power and, if we get it right as a prequel to a global power. It remains a truism that 'physical geography has a continuous, powerful, and profound effect on the nature and course of combat'.<sup>9</sup> On the multi-dimensional chessboard, the facts of geography, strategy and the realities of politics and technology all interact.<sup>10</sup> For India, our neighbour with an unresolved border dispute and challenging our strategic space, China as a regional Asian goliath, will remain a truism and adversary for the distant future. Deterrence by denial is a national imperative.

### **Multi Domain Operations (MDO)<sup>11</sup>**

It is ironic that while change is inevitable, it is generally resisted

as it moves nations and individuals out of their comfort zone and is initially chaotic. And if change is at global level, driven by geo-strategic and geo-political considerations, economics, resources and technology, and is multi layered, multi-dimensional, cross-impacting and affecting nations, allies and adversaries, corporates, terrorist organisations, we are looking at a turbulent, insecure international security environment leading to global 'Competition'<sup>12</sup> 24X7'. The commonly held perception of deterrence has changed irrevocably. Warfare has already transcended the domains of military units and military affairs, and is increasingly becoming a matter for politicians, scientists, and even bankers.<sup>13</sup>

Incidentally this was stated as early as 1999 by Qiao Liang and Wang Xiangsui in their famous treatise 'Unrestricted Warfare'. Four interrelated trends are shaping competition and conflict: adversaries are contesting all domains, the EMS, and the information environment and dominance of any country is not assured; smaller armies fight on an expanded battlefield that is increasingly lethal and hyperactive; nation-states have more difficulty in imposing their will within a politically, culturally, technologically, and strategically complex environment; and near-peer states more readily compete below armed conflict making. Adversaries, such as China and Russia, have leveraged these trends to expand the battlefield in time (a blurred distinction between peace and war), in domains (space, cyberspace and information), and in geography (now extended into the Strategic Support Area, including the homeland) to create strategic, operational and tactical standoff. In a state of continuous competition, nations (like China and Russia) exploit the conditions of the operational environment to achieve their objectives without resorting to armed conflict by fracturing the adversary's (US's alliances, South China Sea (SCS) etc.) resolve. They attempt to create stand-off through integration of diplomatic and economic actions, unconventional and information warfare, thus making deterrence more challenging. In future, no one power (including USA) can dominate one or multiple domains forever. Multi-Domain Warfare (MDW) calls for a change of thought process, 'a transformation and not just modernisation'.<sup>14</sup> Visualisation of battle spaces, cross domain operational capabilities and capacity in the military and non-military fields in war and peace, goes beyond the current jointmanship and synchronisation of operations. Multi-domain means creating an effect in one domain that produces an effect in other. Multi domain-specific capabilities



can be leveraged to defeat a capable foe in another domain. The resources must be capable of cross domain operations and must be robust, deployable, low maintenance and manoeuvrable.<sup>15</sup> MDW envisions the military and non-military; everything from fighters to destroyers, space shuttle to submarine, cyber to satellites, tanks to attack helicopters, electromagnetic to electronic, media to information, influence operations, economists to MNCs, politicians to think tanks, munition factory worker to hacks - working together intrinsically as 'one', to overwhelm the enemy with attacks from all domains: land, sea (including sub surface), air, space, cyberspace, information including media and social media, and electronic. The span of operations addressed simultaneously is from the political, national, strategic and operational to the tactical. Traditional turf and domains are shed as it's everybody's domain and whoever is more effective, more lethal and faster, acts and reacts. Both, adapting to and driving change in the operating environment, adversaries continue to alter the battlespace in terms of time, geography, and domains and by blurring the distinctions between peace and war. Battle space has expanded, converged and compressed all at once during competition and actual conflict; tactically, by bringing kinetic and non-kinetic effects to bear from any place in the world and, strategically, by being able to challenge the deployment and echeloning<sup>16</sup> of forces into the fight at all places simultaneously. In fiscally challenging times and amidst ever-increasing diversity throughout the globe, interdependence, interoperability, and integration are vital to inevitable success on the battlefield no matter its form. Are the Indian armed forces ready to fully commit to being an interdependent, interoperable and 'capabilities' based armed force and avoid paradigm paralysis? In order to maintain a ready-force that is able to conduct full-spectrum (military and non-military) operations in its fullest form and at a moment's notice, we must focus on capabilities based armed force to script future joint task forces for conducting operations in support of the nation and provide credible deterrence.

### **Global Power Rankings, Net Assessment and CNP of Nations**

In an adversarial scenario, multi-dimensional power index of nations with special reference to India, China, Pakistan, USA, Russia and Japan has strategic relevance. CNP is relevant when we talk of a nation's standing and its deterrent capability. Most Defence and National Security Think Tanks (there are over 5000 think tanks in



the world and India has around 280<sup>17</sup>), when they collate and put together all ingredients to come up with Overall Nation's Power Index, generally rate US and China 1 and 2 and India between 3 to 5. When you speak individually of specific fields like military, economic, diplomatic, R&D, technological growth etc., generally US and China come within the top 3 and India within the top 6 and lowest 10. This index, being multi-dimensional, is itself an indicator to the question of our deterrent capabilities. The data researched, created and is captured by Lowy Institute, Australia in 2019 Asian Power Index is comprehensive. Warfare itself and certainly deterrence is not a numbers game. We appear very confident that India would not have to fight a two-front war, as our Political, Diplomatic, Information, Military and Economic (PDIME) standing would ensure that. Our armed forces are prepared and confident of responding credibly, and in case of Pakistan punitively, against a one front/one country threat. However, in case of an all-out two front war, while the bean count/arithmetic of human resource numbers may be acceptable, in terms of war waging equipment and armaments as also the high percentage of vintage equipment, and given China's very intense focused modernisation processes (quality over quantity) actually paint a sobering reality, specially when it comes to our army and air force. For the record, China's People's Liberation Army Navy (PLAN) with more fighting vessels 317 vs 283 of USA, 3 carriers, to be built to 5/6, 60 submarines (to be built up to 80), 1200 short-range missiles and up to 300 intermediate range missiles, new destroyers, amphibious vessels, stealth fighters and long-range weapons is quickly increasing its ability to threaten every part of the globe due to its massively expanded expeditionary military operations. In recent years, the Chinese have exponentially increased their foreign presence around the globe, in a transparent effort to rival the US as a global superpower. The Chinese have made large incursions into Africa, and even set up a military base in Djibouti, Africa. Chinese SSBNs are now able to patrol with nuclear-armed JL-2 missiles, able to strike targets more than 4,500 nautical miles. As for People's Liberation Army Air Force (PLAAF), all of China's fighters in 2000, with the potential exception of a few modified Su-27s, were limited to within-visual-range missiles. China over the last 15 years also has acquired a number of sophisticated short and medium-range air-to-air missiles; precision-guided munitions including all-weather, satellite-guided bombs, anti-radiation missiles, and laser-guided

bombs; and long-range, advanced air-launched land-attack cruise missiles and anti-ship cruise missiles. China's acquisition of Russian-built S-400 surface to air missiles will further enhance her A2AD capability. Niche technology like artificial intelligence (AI), robotics, big data, hypervelocity missiles, drone/robotic swarms, and the Chinese creation of 'quantity over quality' has its own impact. In response to US modernisation and expansion of its entire nuclear infrastructure, China is following suit at a much faster pace. The increasing strategic bonhomie between China, Russia and Pakistan also needs factoring in, more in the non-kinetic domain. One very important factor which is being increasingly accepted is the mind of the leader and people and their likely reaction to deterrence.

### **DETERRENCE IN THE INDIAN CONTEXT**

*"The Department of Defence's enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our Nation"*

- National Defence Strategy of the United States of America

As a regional power dominating South Asia, India is forging strategic alliances, trying to ensure neutrality of some and keep adversaries at bay by strategic balancing (internal, external, and soft power balancing) and deterrence. India has bilateral strategic partnerships including Security Agreements with USA, Japan, Bhutan and forged alliances in multi-national alliances/groupings (like Association of Southeast Asian Nations (ASEAN), Shanghai Cooperation Organisation (SCO), Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) etc.). India also needs to prosecute 'Competition' operations in all domains as also develop deterrence tools and capabilities, to act/prohibit/restrain/react to other nations from degrading our CNP. To illustrate, ability to protect our networks and carry out cyber warfare, protect our space assets, our economic and trade pathways, defend and prosecute influence information operations down to the basic essentials of protecting India's sovereignty and integrity in all domains including Indian Ocean Region (IOR). We must be absolutely clear that all countries are in competition with us including our neighbours, strategic partners and our known collusive adversaries China and Pakistan.

Deterrence is enhanced through security cooperation, military integration and interoperability with own security and intelligence

agencies, allied forces and partner nations and building trust and confidence between partners. The deterrent impact of such cooperation and integration is both political and military in nature. The political impacts are primarily derived from the effects that coalition-based responses have on adversary decision-makers' perception of India's and allied political will; the potentially long-lasting, harmful post-conflict political and economic effects of taking on India. Allied and partner contributions to the joint fight are significant. For example, they can provide host nation security, fly additional combat and support sorties, supplement naval presence, provide additional manoeuvre forces, supplement Intelligence, Surveillance and Reconnaissance (ISR) inputs, to name just a few. They could stay short of providing 'kinetic support'. These actions contribute significantly to deterrence, force protection and overall operational success. While military intervention of any of our strategic partners including USA is very tenuous at best, the unique potency of US Global Strike capabilities: their nuclear and armed forces contribute uniquely and fundamentally to deterrence<sup>18</sup>, through their ability to threaten to impose costs and deny benefits to an adversary in an exceedingly rapid and devastating manner (practice of imposing trade sanctions if adversary does not cooperate is a deterrent operation). A mention of US high end Conventional Prompt Global Strike (CPGS) system being developed by America is one such example. CPGS is based on a leading-edge military technology said to make it possible to accurately destroy any target on earth using a non-nuclear warhead that is carried by a strategic missile such as an intercontinental ballistic missile (ICBM) before detaching at a near-space altitude and then accelerating to fly at hypersonic speeds of Mach 5 or faster. While US is planning to only arm conventional weapons, it is rumoured that China will deploy even nuclear warheads on it (on the new Wu 14 missile).<sup>19</sup> It must be noted that China and Russia too possess such strike capabilities and even USA feels threatened and insecure. Knowing our main adversaries, they can and will operate with and through proxies, and attempt to achieve their strategic and operational goals below the threshold of armed conflict. Terrorism, proxy insurgency, information and unconventional warfare (UW) are inherently difficult to attribute and subsequently to punish the originator, and, therefore, difficult to deter. Armed forces do not possess the capabilities to carry out deterrence in all domains, especially non-military.

Deterrence requires a national strategy that integrates political, diplomatic, informational, military, and economic powers. We must develop strategies, plans and operations that are tailored to the perceptions, values, and interests of specific adversaries. Deterrence strategies and actions must span daily operations and must be developed for all phases of competition and conflict planning. Deterrence operations convince adversaries not to take actions that threaten India's vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome. Deterrence operations must, therefore, be planned and executed across all domains in concert with other elements of national and international power in order to achieve strategic objectives. Till we fine-tune our international security alliances and are fairly confident of their direct military and non-military participation, India must plan and prepare to go it alone.

A crucial aspect is that successful deterrence is knowledge-dependent and requires the ability to establish and secure communication access to adversaries in order to generate the desired decision outcomes. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence. For India, to list some of the main military deterrents would be a credible nuclear triad with second strike capability<sup>20</sup> (China has it and Pakistan claims full spectrum capability to justify their tactical nuclear weapons<sup>21, 22</sup>), capabilities of conventional ICBM / intermediate-range ballistic missile (IRBM), missile and rocket artillery; strategic lift; robust command, control, communications, computers, cyber, intelligence and information, reconnaissance and targeting (C5I2SRT); ballistic missile defence (BMD); dominate IOR; strategic offensive capabilities military and multi domain to provide credible deterrence and punitive deterrence against China and Pakistan respectively.

Conventional deterrence is more complicated than nuclear deterrence because it is hard to convince an adversary that you have the capacity to carry out sufficiently severe punishment, a problem that is less severe in nuclear deterrence because of the level of destructiveness associated with nuclear weapons. Moreover, in conventional deterrence efforts, adversaries

repeatedly miscalculate the relative power balance and their capacity to bear punishment. And deterrence of terrorism with threats of conventional retaliation is still more complicated, even when it is state-sponsored. Deterrence, the first option, is challenged because the threat of massive retaliation loses its value if adversaries are achieving their operational and strategic objectives before conflict. Effective deterrence combines military and non-military means. In some cases, military capabilities may not be an effective tool to deter a particular adversary's action, making other instruments of power the primary deterrent. Additionally, coalition support should be integrated to enhance deterrence credibility, but deterrence also must be viable as a unilateral strategy. Our deterrence will obviously be challenged by our adversaries. Military options/actions will always remain the final pivotal option to achieve national objectives, both proactive and reactive.

In relation to Pakistan, we face a peculiar problem of whom to deter? If Pakistan suffers significant conventional losses or loss of territory, she may assess that escalating the conflict by employing weapons of mass destruction or effect or disruption could recapture the initiative or drive policymakers to the negotiation table to end conflict on more favourable terms. Pakistan may also use TNWs, if presented an appropriate target, contributing to the attainment of operational or strategic objectives. This brings us to the strategic nuclear dilemma that India should not risk escalation for Pakistan to reach a perceived "use it or lose it" situation, especially if she perceives backing by USA. If and when India prosecutes offensive operations, we must conduct effective Influence Operations (IO) against Pakistan and to the world too about the dangers of employing Weapon of Mass Destruction (WMD), minimise vulnerabilities and demonstrate the ability to continue operations if attacked. If deterrence fails to preclude a tactical WMD or disruption attack, our IO must ensure isolation of Pakistan, internationally and regionally. The option of exercising our stated nuclear policy is a constant. When it comes to non-state actors and terrorist organisations, it's a different ball game. They differ in their susceptibility to our efforts to credibly threaten cost imposition. They have different goals/objectives, different values, and they employ different means to achieve them. Since India does not believe in using a hammer to kill a fly which is why planning and preparing for deterrence operations against specific targets (nation,



non-state actors like corporates, agencies, terrorist organisations or even individuals) is important. MDO provide India with hitherto unused domains like cyber, Information Influence Operations (IIO), space, psychological operations (psyops) and with the raising of the Special Forces Division our coercive kinetic response can be deeper, stronger with strategic intent, but restricting it locally.

Coming to deterrence against terrorist organisations, we need to hit their assets which they rely on for survival. Attack the organisation's leadership strata and commander; its military capability for carrying out terrorist attacks; its economic and financial support base; and the network of alliances with other organisations and states that provide support in the form of arms and finances. It is possible to achieve deterrence by demonstrating the will to use military force to inflict damage on these assets.<sup>23</sup> We can proudly say that our nation and army has identified the same but been only somewhat successful in following this deterrence concept in entirety, specially hitting their support bases across our borders, unlike Israel where the geo-political/strategic context is entirely different.

As far as China is concerned, the People's Liberation Army (PLA) is undergoing the most comprehensive restructuring in its history to become a force capable of conducting complex joint operations and global power projection. China is a past master and strong advocate of 'unrestricted warfare' in which deterrence forms a key component. Her rapid growth of CNP, with focus on military modernisation (A2/AD), coupled with development at par, if not superior capabilities, in niche technology poses multiple challenges even to USA, and she is currently engaging India in Competition 24X7 to ensure our CNP, strategic growth and space remains confined and restricted. In addition, China is increasingly discarding the rule based international system and conventional defined norms of international behaviour, as prescribed by USA and its allies, and its opaque strategic thinking and decision making make deterrence more difficult. China's military strategy and ongoing PLA reform reflect the abandonment of its historically land-centric mentality. Similarly, doctrinal references to "forward edge defence" that would move potential conflicts far from China's territory suggest PLA strategists envision an increasingly global role.<sup>24</sup> Recently President Xi asked the PLA to prepare for war.<sup>25</sup> Speaking at the US Naval War College, Prof James Holmes quoted Clausewitz,



“it’s wise to pick a fight with a stronger power today if you see the trend lines running against you”, and further elaborated that, “You might get part or all of what you want today, but not tomorrow, next year, or a decade from now. If China sees its rise plateauing or starting to decline, it might strike rather than wait.”<sup>26</sup> These proclamations should be taken very seriously by our leaders, and deterrence measures must be planned and put in place both military and non-military. Recent Chinese publications have increasingly spoken of strategic deterrence.

China’s existential importance of Belt and Road Initiative (BRI) and China–Pakistan Economic Corridor (CPEC), her relationship with Pakistan, her suspicions about Tibet and her desire to maintain levers in relationship with India suggest that a boundary settlement is not a Chinese priority at present. Add to this, China’s dependence on the Indian Ocean and her suspicions about India-US defence cooperation and strategic coordination. Taken together these factors make it likely that China will keep the boundary issue alive as a lever in relationship with India. Settling the boundary will not settle or eliminate strategic competition between India and China in their shared periphery. China’s confrontation with India is not all about the boundary issue but political. It is unlikely that Chinese Communist Party (CCP) leadership, which increasingly relies on nationalism for its legitimacy, will find it easy to make compromises necessary for a boundary settlement. That is one reason why public Chinese rhetoric on the boundary has become stronger in the last few years, even though their posture on the border has changed only marginally.

### **Possible Conflict Scenario**

The confrontation being political, it could be ‘to teach India a lesson and show the world’ her power projection potential of an ‘Arrived Super Power’. The conflict could start as an aggressive competition and confrontation using both kinetic and non-kinetic means but could easily escalate to a broader conflict. Probability of Pakistan jumping into the fray must be factored as it could very well be part of the strategic plan. Similarly, using land and maritime routes through other immediate neighbouring states cannot be ruled out. Getting a little specific, with Pakistan along the western borders (both operated MDO pan India in hinterland), we anticipate his employment of fires across domains (cyber, computer, IO, hybrid,

EMS, space; Diplomatic, Information, Military and Economic (DIME)) during peace (constant competition) and imposition of his will with increasing tempo, focus and lethality just prior to conflict to try and achieve his political and military aims, without fighting. For instance, China's first step is to achieve what the Chinese call 'information dominance' by targeting adversary's data and communications networks.<sup>27</sup> Physical attacks on satellites, including 'blinding' them with lasers, would be combined with cyber-attacks on computer systems. Concurrently jamming air, rail, logistics, banking, financial networks and prosecuting IIO to create panic in local population in the mainland, delay and disrupt our armed forces mobilisation and impact morale. Shifting gears to actual combat, employ their air assets including attack helicopters, ISR capabilities, special forces, rockets, missiles and artillery to degrade our strategic, operational and tactical assets and military forces, isolate the battle field, and then employ offensive forces to defeat our land and air forces in detail. Permanent terminal objectives even in the event of a full scale war are most likely to be Chinese perception of his traditional borders which in Ladakh are close to the current Line of Actual Control (LAC) and in the eastern front include the state of Arunachal Pradesh. Except for the physical land boundary disputes, there is no other territorial or maritime dispute with China. However, terminal objective would be dictated by his political aim translated into military objectives, battle field success in terms of real estate, domains, Chinese casualties and vulnerabilities, India's response, specially military, including resolve and warfighting potential, international reactions and the nuclear dimension. The same is being war gamed on a regular basis at the strategic, operational and tactical levels within our armed forces. The intensity of hard and soft power would be nothing like the nation and our troops would have experienced. We have one of the most battle-hardened troops in the world, but the intangible effect of psyops, isolation, lack of situational awareness, operating in a degraded environment coupled with a 360 degree conflict with no front, rear and flanks will certainly impact them; if we do not train, prepare and have the capacity to counter and negate his design of conflict, China will wage such a war. Just as a stalemate for India is considered a defeat, if we launch pro-active operations against Pakistan, China too will aim to achieve his political and military objectives swiftly against India. While it will be a challenge, we must keep increasing our military capabilities to impose prohibitive costs to deter this adventure.

While focusing on China and Pakistan, we must not ignore other adversaries or conclude that the multi domain lessons learnt can be commonly applied, as every competitor is different. Naturally, India has to address non-state actors on equal priority. We must bear in mind that the traditional escalatory ladder is defunct in MDO, it will more likely look like a web of intersecting paths, where each intersection is a domain be it space, cyber, land and response can be on any one or multiple domains.

‘Know and understand your adversary’ is a pre-requisite for combating MDW and is bedrock of deterrence. This requires enhanced ISR and operational intelligence gathering capacity and capability including hi-tech mechanisms to understand adversary’s perceptions, assets, capabilities, vulnerabilities, his decision making hierarchy, procedure and structure, non-state actors sponsored by him, in short ‘a holistic situational awareness’ of all. We must develop cogent plans to identify and defeat his military and non-military plans during and after ‘Competition’ and create a proper military and non-military target list which we keep reviewing. What cannot be understated for above capability is understanding of our own capabilities including allies, limitations and real time situational awareness. Such understanding is achieved only by total synergy amongst all players involved in deterrence operations. Highly networked forces, which are integrated and interoperable, will increase the Commander’s flexibility to choose from widely varying types of capabilities to achieve the desired deterrence effect.

### **Nuclear Deterrence**

If you type deterrence on the net, the response will overwhelmingly talk of nuclear deterrence. Most experts saw a balance of power as the structural condition necessary for peace to prevail globally. Indeed, at the dawn of the Cold War era, balance of power theory/ balance of terror or Mutual Assured Destruction (MAD) constituted the conventional wisdom of the field. Emergence of more nuclear weapon holding states threw this theory off kilter. With the emergence of MDO and options short of war, nuclear deterrence is increasingly being challenged by smaller states and even amongst nuclear states (China, Pakistan and India). Disruptive technologies like AI, surveillance capabilities, cyber domain and hypersonic weapons have further eroded deterrence potential of big powers (transparency and doubtful second strike

capability). This also creates pressure on less technologically endowed countries to put their nuclear arsenal at a hair-trigger operational status or adopt the 'use it or lose it' concept. It has led to creation and deployment of TNWs, which some nations assume are part of conventional warfare. Russia is talking of 'Escalate to De-escalate' if conventionally out manoeuvred. As an emerging nuclear power which is still striving to attain a robust second-strike capability, India needs to act expeditiously as we are dangerously behind the big three (US, China, Russia) in R&D and application of niche technologies. Our nuclear policy has stood the test of time. There is talk of urgent review which may not be a bad idea for creating ambiguity, but 'there is nothing in the present doctrine that prevents India from responding proportionately to a nuclear attack'.

### **Human and Psychological Dimension**

Recent studies and insights into the nature of human decision-making raise questions about the very logic of deterrence. As a theoretical concept, deterrence rests on assumption that where risk is involved, humans act rationally, in the sense that they base their decisions on a cost-benefit calculus and act only when the expected gains outweigh the anticipated costs. Over the past 40 years, however, research in behavioural economics has cast great doubt on this assumption. Humans, it turns out, cannot be counted on to always maximise their prospective gains. Even when they do, they are remarkably inept at understanding how the other side – the adversary in a conflict – calculates its own costs, benefits and risks. The reference point for leaders and nations impacts risk taking. Security strategies built on deterrence may no longer assure peace as USA has found out to its consternation.

### **IIO and Weaponisation of Social Media**

Through the weaponisation of social media, the internet is changing war and politics, just as war and politics are changing the internet.<sup>28</sup> Terrorists livestream their attacks, 'Twitter wars' produce real-world casualties, and viral disinformation alters not just the flow of battles but the very fate of nations. The result is that war, technology and politics have blurred into a new kind of battlespace that plays out on our smartphones. Today war has gone online and the online world is waging it against each other (ideals, ideas, politics, religion etc.). The occupation of northern Iraq by Islamic State of

Iraq and Syria (ISIS), during the summer of 2014, with hardly a fight is a classic example of social media winning a conflict on ground. The ISIS used the internet as a weapon to carry out a blitzkrieg. There is a lot of talk of 'cyber security and cyberwar' but the ISIS had no real cyber capabilities yet won a victory. It hadn't hacked the network but hacked the information on it. The distinction between online and offline confrontation/operations/conflict has become blurred. With each Trump tweet, US diplomats and foreign embassies alike scramble to figure out whether they should treat these online messages seriously. Meanwhile, Russia, China, Iran, North Korea and most others are playing their own IIO. Who can forget the intervention of Russia in the US Presidential elections in 2016, the probe of which is going on currently. Diplomacy has become less private and policy-oriented and more public and performative. China and Pakistan are already playing this deadly game against us.

### **Ground Realities Regarding Deterrence**

The Cold War deterrence (mainly nuclear) has given way today, leading to a lot of cynicism about the relevance and even effectiveness of deterrence, especially on illiberal nations and terrorist organisations. MDO, especially attributes of ambiguity of cognitive domains, have given power to lesser states, organisations and even individuals to challenge established norms. Deterrence effect finds it difficult to prevent strategic competition which fall beneath the threshold of traditional military force (military dimension less than armed conflict), allowing these adversaries to make operational gains without tripping the 'go-to-war' calculus of the adversary. Russia demonstrated some of these capabilities as part of its operations into Georgia, Crimea and Ukraine. North Korea demonstrated its advanced cyber capabilities in November 2014 when they launched a cyberattack on Sony Pictures and China has built artificial islands in the SCS to advance its sovereignty claims on vital international waterways that are part of the busiest maritime trade routes in the world and closer home, the proxy war being waged by Pakistan against India.

Complex Deterrence Theory recognises that the credibility of the deterrence threat has been increasingly compromised due to the ambiguity and fluidity of the international system.<sup>29</sup> As a similar perspective to this, it is being pointed out that the growing complexity

of international nuclear order has played a part in exacerbating the uncertainty of nuclear deterrence.<sup>30</sup> Ironically, Emanuel Adler reasons that the asymmetrical power relationship between or among actors in the international political arena following the Cold War has given rise to the so-called deterrence trap.<sup>31</sup> A deterrence trap refers to a situation in which a major power is unable to deter the actions of a relatively weaker actor, no matter whether the major power threatens the weaker actor with retaliation or abstains from threatening and appeases the weaker actor. For example, even if America threatens to use force in order to deter Iran from nuclear development, there is a possibility, Iran will turn America's threat against it in order to fortify its position on its nuclear development plan.<sup>32</sup>

### **Cyber Deterrence**

Cyber deterrence based on traditional deterrence theories is difficult and deterrence by retaliation, in particular, has been thought of as unworkable. However, recently cyber deterrent forces are being established, including ones that identify the sources of cyber-attacks and threaten to retaliate against such attacks. There is even talk that cyber-attack response could be war where nuclear weapons could be used as a means of retaliation.<sup>33</sup> However, it will not be a credible threat if announced by India or any nation. Some defence experts and Think Tanks feel that unless nations can deter cyber-attacks, the appeal of cyber-weapons to hostile forces will increase and the credibility of extended deterrence, including the nuclear deterrent, is likely to be undermined.<sup>34</sup> Chinese cyber intervention is a known practice and they are targeting India, and we need to protect ourselves against all adversaries and create robust and real time counter cyber warfare capabilities.

New niche technologies, and even low end and low-cost technologies, employed enmasse will further exacerbate the deterrence relationship between nations and even non state actor(s) but will also initiate a new arms race which has already commenced in the nuclear and niche technology domain of AI, robotics, space etc. Deterrence too has red lines which are sometimes stated and generally presumed by the adversary. The stronger powers possibly would like to spell out the red lines.

### **Conclusion**

Similar to important factor of 'Surprise and Deception' in warfighting/



competition, Deterrence Operation too has generally appeared as an abstract operation for most ground soldiers even at the theatre level, but it impacts defensive or offensive action by the adversary. We have now entered the complex world of multi and cross domain competition and deterrence which needs to be synergised at the apex level with concerned agencies involved. At the military sphere, once the political directive (hopefully in the form a National Security Strategy) has been promulgated, strategic military deterrence will be planned and coordinated by the Chiefs of Staff Committee (COSC)/Chief of Defence Staff (CDS) Committee when formed and executed by the Services while operational deterrence is executed by Joint Theatre Commanders. Currently it is happening automatically and intrinsically like raising of new mountain corps for operations along Chinese border; strategic command assets and deployment; induction of nuclear submarine, aircraft carriers and modern fighter squadrons. Establishment of National Cyber Agency, creation of post of Director General Information Warfare (DGIW) and Deputy Chief of the Army Staff (Strategy) are steps in the right direction, thereby acknowledging the vital role of IIO and MDO. It needs to get institutionalised and synergised strategically and tactically, especially the non-military domains. When US intervention and multi-national activities to protect liberal rule based world order are not considered hegemonistic, India needs to think, prepare, plan and execute strategy to dominate its area of influence and interest.

To conclude, for the question 'Is the Indian deterrence effective against adversaries', some specific questions need to be probed. Do our CNP and military capabilities and capacities prevent Pakistan from waging proxy war against us? Does our immediate neighbourhood constantly keep our strategic interests in mind? Are we confident that China Pakistan collusivity will not initiate a localised conflict? Does China act on contentious issues keeping Indian interests in mind? But the flip side is that similar answers may be received by our adversaries and even USA in some domains. However, militarily speaking, no nation can afford to threaten USA, China and Russia. So the answer is 'in today's multi polar multi domain world', for an aspiring regional power and security provider in IOR, the rating has been downgraded to a no or at best 'not yet'. The main reason for this is not just our nation's CNP and current military capability and capacity to prosecute MDO and MDW, but demonstration of credible will, intent and lack

of national synergy. Deterrence should be aimed to achieve strategic and operational outcomes and may never stop tactical actions by our adversaries (even countries holding compellence capability against its adversaries may not prevent tactical actions). A collusive China-Pakistan in our immediate neighbourhood, rising trend of ultra-nationalism infecting our immediate neighbours and contested strategic space of Asia, fluid internal security situation dictate that India needs to get its act together, continue building its CNP, militarily transform into a MDO capable armed force and gets its multi domain deterrence capabilities in place for specific nations and scenarios. In a sense 'deterrence' has become a victim of its own success. India must rethink its deterrence strategy in changing geo-political and strategic environment including psychology of decision making. Even with diminishing returns, ensuring 'Deterrence by Denial' against adversaries will remain the first priority for India.

### Endnotes

<sup>1</sup> James J. Wirtz, "Conclusions," *Complex Deterrence*, pp.322-328, pp.322-323. The outbreak of the Bosnia-Herzegovina conflict in 1992 and the Rwanda genocide of 1994 can be cited as examples of this.

<sup>2</sup> In competition, the adversary takes actions to achieve objectives below the level of armed conflict, as well as to posture forces to support the escalation of activity into armed conflict. His primary aim is to separate or isolate friendly forces politically, limiting a coordinated allied response and destabilizing target states internally to attain its objectives below the threshold for armed conflict. The adversary in competition may consider itself already engaged in national conflict and, therefore, employ all elements of its national power with few procedural limitations in a coordinated approach before own elements/forces receives authorization to respond. The adversary also positions systems to fragment own force capabilities and make a potential response costly and ineffective in the event of escalation.

Source Para 2-4(a) of Draft Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0 October 2017

<sup>3</sup> The original of this pragmatism is generally conceded to Lord Palmerston (John Henry Temple) of Great Britain, but most world leaders have invoked it at one time or another to justify their policies and actions

<sup>4</sup> Coined by Thomas C Schelling the Nobel Price Winner in Economics in 2005 in his book *Arms and Influence* (1966)

<sup>5</sup> Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills: Sage Publications, 1977), pp.28, 31-43.

<sup>6</sup> 'The Eroding Balance of Terror: The Decline of Deterrence' by Andrew F. Krepinevich, Jr, Foreign Affairs Journal, Jan-Feb 2019 Issue

<sup>7</sup> Inputs available from a galaxy of articles, papers and online material on international relations, security and strategy.

<sup>8</sup> *Relations Regions and Powers; The Structure of International Security*, Cambridge Studies International, Barry Buzan and Ole Wæver, CAMBRIDGE; [www.cambridge.org/9780521814126](http://www.cambridge.org/9780521814126)

<sup>9</sup> Harold A. Winters with Gerald E. Galloway Jr, William J. Reynolds and David W. Rhyne, *Battling the Elements: Weather and Terrain in the Conduct of War*, The Johns Hopkins University Press, Baltimore, MD, 1998, p. 4.

<sup>10</sup> Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*, Fontana, London, 1989, p. 111.

<sup>11</sup> 'Multi Domain Warfare in the Indian Context' by Lt Gen PR Kumar (Retd); 36<sup>th</sup> USI National Security Paper of 2018

<sup>12</sup> An important activity/word in multi domain warfare - In competition, the adversary takes multi domain actions 24X7 (political, economic, military, diplomatic, information, cyber, space etc) to achieve objectives below the level of armed conflict, as well as to posture forces to support the escalation of activity into armed conflict. His primary aim is to separate or isolate friendly forces politically, limiting a coordinated allied response and destabilising target states internally to attain its objectives below the threshold for armed conflict. The adversary in competition may consider themselves already engaged in national conflict and, therefore, employ all elements of its national power with few procedural limitations in a coordinated approach before own elements/forces receives authorization to respond. The adversary also positions systems to fragment own force capabilities and make a potential response costly and ineffective in the event of escalation. **Essence** taken from Para 2-4(a) of Draft Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0 October 2017

<sup>13</sup> Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, 1999, pp. 221;189.

<sup>14</sup> 'Multi Domain Warfare in the Indian Context' by Lt Gen PR Kumar, 36<sup>th</sup> USI National Strategic Paper, 2018

<sup>15</sup> *ibid*

<sup>16</sup> Draft 'Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0', October 2017

<sup>17</sup> 2018 Global Go To Think Tank Index Report, University of Pennsylvania, Scholarly Commons

<sup>18</sup> US Field Manual: Deterrence Operations Joint Operating Concept, Version 2.0, Dec 2006

<sup>19</sup> "Prompt Global Strike: China and the Spear," by Lora Saalman, APCSS, April 2014, [http://apcss.org/wp-content/uploads/2014/04/APCSS\\_Saalman\\_PGS\\_China\\_Apr2014.pdf](http://apcss.org/wp-content/uploads/2014/04/APCSS_Saalman_PGS_China_Apr2014.pdf).

<sup>20</sup> 'Modi hails 'India's successful establishment of Nuclear Triad', The Dawn, 05 Nov 2018

<sup>21</sup> 'Pakistan completes nuclear triad' by Kinza Asif, Foreign Policy News, 16 Jan 2017

<sup>22</sup> Pakistani nuclear forces, 2018, Hans M. Kristensen, Robert S. Norris & Julia Diamond, pgs 348-358I published online: 31 Aug 2018, 'Bulletin of the Atomic Scientists', Volume 74, 2018

<sup>23</sup> "Deterrence against Non-State Actors: Thoughts following Operation Protective Edge", by Yair Naveh, *The Institute for National Security Studies (INSS) Insight*, no. 663, February 11, 2015, <http://www.inss.org.il/index.aspx?id=4538&articleid=8720>.

<sup>24</sup> US-China Economic and Security Review Commission 2018 and US DoD Annual China Report 2018 (Military and Security Developments Involving the People's Republic of China) both of which are largely in synch and both are Congressional Reports.

<sup>25</sup> 'Prepare for War' President Xi Jinping tells military region that monitors South China Sea and Taiwan, South China Morning Post, 20 Nov 2018

<sup>26</sup> Political newspaper 'The Hill' dated 30 Oct 2018, published in Washington by Capitol Hill Publishing

<sup>27</sup> Special report in 'The Economist' Dec 25/27, 2017: The Future of war; Power Projection- Stay well back

<sup>28</sup> Like War: The weaponization of Social Media by PW Singer and Emerson T. Brooking, An Eamon Dolan Book, Houghton Mifflin Harcourt, 2018

<sup>29</sup> "Beyond the Nuclear Umbrella: Re-Thinking the Theory and Practice of Nuclear Extended Deterrence in East Asia and the Pacific", by Hayes and Tanter, Nautilus Institute for Security and Sustainability, 2011

<sup>30</sup> House of Commons Defence Committee, *Deterrence in the twenty-first century: Eleventh Report of Session 2013-14, Volume II* (London: Stationery Office, 2014), p. Ev w32, <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmdfence/1066/1066vw.pdf>.

<sup>31</sup> “Unconventional Deterrence: How the Weak Deter the Strong” by Ivan Arreguin-Toft. Citing Israel’s retaliatory attack against Hezbollah in 2006 as an example, Adler argues that although Israel’s use of military force was aimed at deterring any further terrorist attacks from Hezbollah, it instead resulted in a bolstering of Hezbollah’s international standing, thus putting Israel in a deterrence trap.

<sup>32</sup> “Unconventional Deterrence: How the Weak Deter the Strong” by Ivan Arreguin-Toft. Citing Israel’s retaliatory attack against Hezbollah in 2006 as an example, Adler argues that although Israel’s use of military force was aimed at deterring any further terrorist attacks from Hezbollah, it instead resulted in a bolstering of Hezbollah’s international standing, thus putting Israel in a deterrence trap.

<sup>33</sup> “Cyberwar and the Nuclear Option,” by Elbridge Colby, *The National Interest*, June 24, 2013, <http://nationalinterest.org/commentary/cyberwar-the-nuclear-option-8638>.

<sup>34</sup> *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* by Brian M. Mazanec and Bradley A. Thayer, Houndmills: Palgrave Macmillan, 2015, p.32