CYBER DETERRENCE: STRATEGIC IMPERATIVES AND OPERATIONAL CHALLENGES

ASHISH GUPTA

Nuclear deterrence, in the era of the Cold War, was the single most important determinant in preventing the destruction of our planet from the scourge of nuclear weapons. During the Cold War, the deterrence theory was the lynchpin of the US' strategy for containment of the former Soviet Union, protection against nuclear attacks and nuclear blackmail. Deterrence is a broad phenomenon that involves using threats of harm, usually to be inflicted by force, to convince others not to do designated harmful things.[1] For a credible deterrence posturing, the inalienable requirement is development of commensurate capabilities, their overt visibility and frequent deployment as a way of issuing and resurrecting threats, particularly in the wake of a crisis/ confrontation. Deterrence is used to manipulate the perceptions and actions of others and altering or reinforcing behavioural responses or to contain belligerent posturing and, in case of its ineffectiveness, it entails use of coercion or threat of use of force, or overt use of force emanating from acquired deterrence capabilities.

Drawing parallels with nuclear deterrence and contextually applying these concepts for evaluating the veracity and effectiveness of 'cyber

Group Captain **Ashish Gupta** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

1. Emanuel Adler and Vincent Pouliot, *International Practices: Cambridge Studies in International Relations* (Cambridge : Cambridge University Press, ,2011), p.141.

In the cyber domain, the lack of clear lines of demarcation—in terms of intent, motivation and geographical location—makes the task of identifying the true perpetrators, apportioning responsibility and undertaking reprisals a herculean one.

deterrence' might turn out to be futile and counter-intuitive due to varying nuances of intent, applicability, participants and consequences. In the context of nuclear deterrence, the potential enemy is clearly identifiable in form and intent, and deterrence will remain convincing and credible as long as the survivability of the weapon systems and delivery vehicles is ensured. A nuclear threat emanating from a non-state actor is almost non-existential. Adm Michael Rogers, commander of the US Cyber Command while appearing before the House Select Intelligence Committee, on November 20, 2014, commented, "I often hear people use the nuclear analogy in terms of how we were able to develop the concepts of deterrence, norms and behavior. I try to remind people to remember that the challenge of the nuclear analogy is… that [nuclear weapons] were controlled by a very small number of nation-states – two really."[2] The main assumption underlying nuclear deterrence is to contain the threat of nuclear annihilation by stemming the motivation of states with nuclear arsenals to cross the nuclear threshold.

In cyber space, the enemy may employ disguises, masquerade or hide behind the 'digital veils' without a verifiable or discernable objective or motivation. The primary perpetrator may be an individual, an organisation, a non-state actor or a nation-state. In the cyber domain, the lack of clear lines of demarcation—in terms of intent, motivation and geographical location—makes the task of identifying the true perpetrators, apportioning responsibility and undertaking reprisals a herculean one. The problem of deterrence in cyber space is exacerbated due to several reasons: its inherent

2. *Cybersecurity Threats: The Way Forward*, Hearing of the House (Select) Intelligence Committee National Security Agency, November 20, 2014 (statement of Adm Michael Rogers, commander, U.S. Cyber Command and Director, National Security Agency), https://www.nsa.gov/public_info/_files/ speeches_testimonies/ ADM.ROGERS.Hill.20.Nov.pdf. Accessed on January 12, 2016.

asymmetric nature, difficulties in accurate and timely attribution of hostile activities, level of threshold above which an inimical act warrants punitive reprisals, overarching dependence on technological prowess and a plethora of potential adversaries having the requisite intent and capabilities.

The overt demonstrations of intentions to leverage the innate, acquired or developed deterrent capabilities in order thwart threats against targets and interests as enumerated in the deterrent declaration comprise the hallmark of effective and preponderant deterrent posturing.

The strategy of using deterrence is meant to maintain a frozen status quo. As per William Kauffman[3], "Deterrence consists of essentially two basic components: first, the expressed intention to defend a certain interest; secondly, the demonstrated capability, actually to achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort to him." The potentiality and potency of the deterrent declaration is directly proportional to its credibility. The overt demonstrations of intentions to leverage the innate, acquired or developed deterrent capabilities in order thwart threats against targets and interests as enumerated in the deterrent declaration comprise the hallmark of effective and preponderant deterrent posturing.

In the present time, deterrence as a cornerstone to strategy has been pushed down to a lower rung on the *hierarchical ladder*. After all, the Cold War of more than 40 years ended rather unspectacularly, without the usual march of great armies, unfurling of victory flags and roars of cheerful crowds with expectant jubilation. Nuclear deterrence which was the mainstay of the Cold War era and the nuclear arsenal that supposedly saved the world from nuclear war because of the certainty of Mutual Assured Destruction (MAD), suddenly were stigmatised as liabilities rather than strategic assets. Nuclear deterrence today appears to be an antiquated solution to a dominant

3. William W. Kaufmann, *The Requirements of Deterrence* (Princeton: Centre of International Studies Princeton University, 1954), p.4.

problem of the past. With changing times, strategic considerations have also changed and contextual solutions are emerging from ideas best suited for the present. Although deterrence is conceived and executed as part of a coercive strategy to deter unfriendly behaviour, its effectiveness is totally dependent on the consent and intent of the deterree. The efforts to shape that consent by deterrence are vastly inferior in quality in comparison to the control secured by military action which effectively deprives the enemy of the power to make a wrong move. [4] In addition, the possibility of potential foes rejecting the perceived rational behaviour paradigm and functioning irrationally from the stand point of strategic logic, is high. The whole premise of deterrence is based on mapping the enemy's rational intent. Besides, if the intended deterree is either unwilling or unable to be deterred, then deterrence cannot work.[5] In addition, deterrence has its limitations against asymmetrical threats which cannot be consistently and tangibly fitted into any threat evaluation model.

The classical deterrence doctrine is based on the basic premise that abidance or violation of established rules or conventions stems from the rational calculation of risk of reprisal or punishment versus potential advantages accrued from an act. A deterrence doctrine, which is capricious, uncertain and is not leveraged by commensurate capabilities, fails to be amenable to rational actors. For the deterrence doctrine to be effective and credible, it essentially requires the amalgam of three individual components in equal measure: **severity, certainty, and celerity**.[6] The 'severity' of a punitive action will deter a rational state to commit an act of perceived wantonness or malice against another state. Punishment should be calibrated based on the extent of the crime, at an appropriate severity level. 'Certainty of punishment' is the expression of inalienable resolve to punish the offenders, irrespective of the cost. Infliction of punishment closer to the commission of an offence will reinforce the veracity of the deterrence

4. Colin S. Gray, *Maintaining Effective Deterrence* (Carlisle, PA: US Army War College, Strategic Studies Institute, 2003).
5. Colin S. Gray, *Explorations in Strategy* (Connecticut : Greenwood Press, 1996), p.32.
6. Ronald L. Akers, *Criminological Theories: Introduction and Evaluation* (New York : Roxbury Publishing Company, 1999), p.15.

posture. Deterrence works most efficaciously when it can rely, not upon the potency of explicit threats but rather upon the fears of deterrees, who are discouraged from taking action by their anticipation of the damage that adventurous behaviour would bring down upon their heads.[7] Deterrence, for the manipulation of cost/benefit calculation and for generation of fear, is a form of coercion requiring two essential elements: the credible capability to harm and the credible intent to carry out this harm.[8] Deterrence in cyber space aims to dissuade or discourage potential enemies from carrying out activities detrimental to perceived interest. If an adversary intends to wage war in the cyber domain, he will have to weigh his options and decide what will yield commensurate dividends: a daring cyber attack with proportionate returns or exercise of restraint to avoid the retaliatory wrath of the deterrer.

Closely associated with the theory of deterrence is the 'theory of preemption'. It is widely believed that if an adversary cannot be deterred, poses 'clear and present' danger and its threat instruments can be neutralised by the available capabilities, preemption will be a better suited option. The centrality of the theory of deterrence is somewhat limited in its unambiguous applicability across the broad spectrum of present, perceived and potential adversaries. It somewhat relies on absorbing the consequences of a hostile act, identifying the perpetrators, and then undertaking punitive actions proportionally weighted or exemplarily applied. Against irrational actors such as terrorist groups, preemption may be more appropriate as terrorist organisations have very little to lose, cannot be trusted with rational disposition or checked by threat of retaliation, and their nefarious intent needs to be nipped in the bud before it can culminate into a terrorist attack.[9] Preemptive options, once exercised, are likely to stir up geo-political and strategic tensions. Preemption, as an instrument of policy, an adjunct to force posture and an occasional subterfuge against rogue actors, is essential. However, the policy of preemption cannot be the central strategic deterrence posture.

7. Gray, n.4
8. Austin Long, *Deterrence From Cold War to Long War : Lessons from Six Decades of RAND Research* (Santa Clara CA: RAND Corporation, , 2008), p.8.
9. Alan M. Dershowitz, *Preemption: A Knife That Cuts Both Ways* (London : W.W Norton & Company Ltd, 2006), p.10.

The applicability of traditional concepts of deterrence in an unmodified form to the realities of cyber threats has its own challenges and limitations. Cyber space does not comply with the classic definition of sovereignty as propagated by the dominant 'Westphalian conceptions'. In the realm of cyber space, the relative anonymity of an attacker makes the issue of attributability an arduous and contentious process. Cyber attacks can occur without any warning or without any obvious or subtle indications. Cyber attacks can remain undetected even when they stealthily cause intended damage—as perceptible physical manifestations of attack consequences in quantifiable attributes take time. The possibility and potentiality of a cyber attack remains the same, in war-time as well as in peace-time, without any apparent period of crisis or strained relations. Since an attacker can use the infrastructures of a third party—either in connivance with it, or under a tacit agreement, or without its knowledge—it limits the possibility of attribution and proportionate response against the true perpetrators. For credible deterrence, cyber weapons need to be developed, evaluated and checked for efficacy and factored into the overall deterrence policy. In response to a question, while appearing before the Senate Armed Services Committee (SASC), to head the US Cyber Command (USCYBERCOM) Adm Michael S. Rogers responded by stating, "The establishment of the US Cyber Command is an element of a deterrence strategy, but more work and planning will be required to evolve a solid national strategy. Classic deterrence theory is based on the concepts of threat and cost; either there is a fear of reprisal or a belief that an attack is too hard or too expensive. Cyber warfare is still evolving and much work remains to establish agreed upon norms of behaviour, thresholds for action, and other dynamics." Adm Rogers further stated, "A broad understanding of cyber capability, both defensive and offensive, along with an understanding of thresholds and intentions would seem to be the logical elements of a deterrence strategy, both for our allies and our adversaries, and as they are in other war-fighting domains."[10] The uncertain causal evidence and ambiguous consequences of

10. Sanger, "N.S.A. Nominee Promotes Cyber War Units", *The Washington Times* , March 11, 2014, http://www.washingtontimes.com. Accessed on January 10, 2016.

cyber attacks tend to undermine deterrent postures in cyber space. Despite these challenges, a deficient or inadequate deterrent in cyber space creates vulnerabilities that could be exploited by a determined adversary.

The national interests, which a nation intends to defend, if threatened, have potentially debilitating ramifications and devastating consequences. A nation's interests consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunications, energy, transportation, banking and finance, and shipping. Inimical actors, ranging from mischievous hackers, to criminals, terrorists, non-state actors as also nation-states, are ready to exploit the cyber space for notoriety, power, money, state secrets or just for the thrill of it. A fraction of such attacks is reported, investigated and recorded. The origin of some could be traced behind the physical boundaries of a hostile state, thwarting even the investigative efforts, let alone concluding those with convictions. Some of them may be individual and isolated enterprises by disgruntled employees, cyber criminals, cyber terrorist groups, professional hackers, etc., while others may be closely coordinated acts of more sinister intents perpetrated by nation-states. It is difficult to discern the quantum of evidence which qualifies for retaliation. Investigating every breach in cyber space is not possible as it is a resource and effort intensive exercise. There has to be some discernible correlation between the magnitude of retaliation and the magnitude of damage. Loss of life makes a tractable threshold but cyber attacks have yet to claim their first casualty. If benchmarking a figure based on some monetary considerations justifies a retaliatory attack, how would it be communicated to the attacker that crossing this threshold would result in retaliation? The evolution of the deterrence theory / strategy in cyber space cannot be equated with the conventional deterrence strategy, as cyber space is unique in its physical characteristic, functionality, scope and context. The unique character of cyber space presents new challenges.

Unlike in the case of conventional attacks, where the source of an attack can be conclusively and irrevocably established, in the realm of cyber warfare, the question of attributability and accountability becomes controversial.

PROBLEM OF ATTRIBUTABILITY

The anonymity and impunity with which acts of cyber terrorism and espionage are being carried out has made the process of fixing accountability and subsequent prosecution extremely difficult. Cyber space, being a common entity, shared by government, institutions, companies and individuals, does not offer a sense of security like physical/ geographical boundaries do. The perpetrators with nefarious intentions do not have to undertake the arduous task of breaching the security over physical boundaries to carry out a cyber attack. Unlike in the case of conventional attacks, where the source of an attack can be conclusively and irrevocably established, in the realm of cyber warfare, the question of attributability and accountability becomes controversial. In a hypothetical situation, let us examine a scenario in which a group in State A assimilates computers located in State B into its botnet. The group then uses the botnet to overload computer systems in State C based on instructions received from State D. Though by the conventions of laws of natural justice, the attributability of the conduct rests with State D, it will take a long legal battle to exonerate State A and State B from the responsibility of conduct.

PROBLEM OF CREDIBLE RESPONSE

Almost all forms of retaliation are directed towards the vulnerability of the target. The quantum of retaliation will depend on near-accurate prediction of vulnerabilities. Through assiduous exploration and investigating key systems vulnerable in specific ways, potential adversaries may be identified, tagged, documented and mapped in overall orchestration of deterrence policy. While such actionable information may be reassuring to a certain degree in one's ability to respond credibly on a given day, a consistent deterrence posture requires the ability to respond as long

as the deterrence policy is operative. Vulnerabilities can be discovered and patched, rendering the effectiveness of the response initiated as punitive action ineffective. The quantifiable measure of the outcomes of such attacks may also be speculative. It has been postulated that use of many kinetic weapons will have the comparable problem when used against a large variety of targets. The damage assessment after cyber attacks on information systems will only be speculative, based on their resilience and patching up of vulnerabilities. Furthermore, the extent of damage to any information system is strongly related to the reaction of its human operators: for example, how quickly faults can be found and fixed; how easily damage can be routed around; how frequently the data is backed up; or extant contingency plans. Besides, complacency of the targets stemming from the belief that their systems face no serious threats, apart from those that have been anticipated and dealt with, may prove to be their Achilles heel. Once such targets are put at obvious risk, operators may no longer be so complacent and, thus, targets may not be so vulnerable. Greater complacency on the part of human operators makes the targets more vulnerable than they really are.

The quantifiable measure of the outcomes of such attacks may also be speculative. It has been postulated that use of many kinetic weapons will have the comparable problem when used against a large variety of targets. The damage assessment after cyber attacks on information systems will only be speculative, based on their resilience and patching up of vulnerabilities.

REESTABLISHMENT OF DETERRENCE POSTURE AFTER ATTACK

After an attack in cyber space, the threats designed as part of deterrence need to be realised. This will jolt the defender from its stupor and will energise it to protect its cyber assets with much more rigour and strength. An alert defender will carry out a critical review of existing systems and plug in the associated vulnerabilities. In the wake of this, reestablishing the

deterrence posture will require designing new threats with the potential to dissuade the adversary from undertaking another misadventure. Now the task will be much more gruelling as the vulnerabilities which were exploited and exposed previously would have been plugged in the targets hardened and the associated complacency dissipated.

CYBER DETERRENCE IN LIMITING THE NUMBER OF CONTESTS

In general, a conventional conflict takes place between two warring groups. The ideological, economic, political or allegiance imperatives may bring in third party interventions or associations. However, as the cyber space is so intricately interwoven, an unsuspecting and innocent party may get affected by an act of retaliation against an adversary in cyber space. It may inadvertently draw the affected party into the conflict, thereby expanding its quantum and dimension. This may prove counter-effective as deterrence posturing is aimed at controlling escalation.

EFFECTIVENESS OF CYBER DETERRENCE IN SAFEGUARDING PRIVATELY OWNED CRITICAL INFRASTRUCTURE

Critical infrastructures consist of assets in the physical and cyber domains. Many of the important infrastructures for subsistence, sustenance and security of the population are privately owned and operated. It is the responsibility of system operators to ensure operations of critical infrastructure without disruption and corruption. Formulation of a deterrence posture in the wake of this puts the spotlight on the attackers rather than the system owners who have an obligation to protect these. System owners may take the recourse of absolving themselves of any wrongdoing by arguing that cyber attacks are acts of war and may invoke the *force majeure* clause.

ESCALATION AVOIDANCE

The ensuing crisis following a cyber attack may force the aggrieved opponent to respond with kinetic weapons, thereby escalating the level of conflict. As a part of deterrence policy or strategy, in response to a cyber attack, if a retaliatory action is initiated in cyber space, there is no

assurance of restrainted behaviour from the other side. Article 5, which is a fundamental principle of the North Atlantic Treaty Organisation (NATO), stipulates that if a NATO ally is the victim of an armed attack, each and every other member of the alliance would consider this act of violence as an armed attack against all members and would take the actions it deems necessary to assist the ally attacked. In a policy endorsement, the principle that a cyber attack can constitute an armed attack was approved by the NATO defence ministers in September 2013. Similarly, Russia, without mincing words, has made it clear that, it may respond with strategic means at its disposal if a cyber attack directed against it crosses the strategic threshold. While retaliating as part of deterrence policy in cyber space could logically be constructed as a natural progression of events, the possibility of crossing a threshold and exacerbating the escalation potential of violence is real.

SANCTIONS AS PART OF OVERALL DETERRENT POSTURE

Sanctions – predominately economic and peripherally political and military—constitute an important element of deterrent policy. Sanctions, against a state or an entity, are employed as coercive instruments to elicit a behavioural change or to diminish belligerent posturing. In the post-Cold War era, the waning reliance on armed conflicts and wars, within and among states, for resolution of belligerent, contentious and complex problems has resulted in widespread use of economic sanctions. Sanctions have been used in support of foreign policy goals: to discourage armed aggression, cap the aspirations of potential nuclear states, rein in drug trafficking, expedite political change, discourage proliferation of weapons of mass destructions and dissuade support for terrorism.

Some political observers and decision-makers think of sanctions as a measured and proportionate response to a challenge considered below the threshold of perceived national interests at stake. In addition, sanctions can be considered as a form of expression or message-sending to communicate disapprobation of a particular action or behaviour. It was appropriately observed by America's Catholic bishops: "Sanctions can offer a non-military

alternative to the terrible options of war or indifference when confronted with aggression or injustice."[11]

In order to gauge the efficacy of economic sanctions and ascertain the underlying rationale, the analysis of sanctions against Iran provides some perspectives. In the case of Iran, in order to cap its supposedly illicit nuclear activities, the US, the member states of the European Union and others put in place a strong, inter-locking matrix of sanction measures relating to Iran's nuclear, missile, energy, shipping, transportation, and financial sectors.[12] The European Union (EU) embargo and the US sanctions played havoc with the Iranian national economy. Iran's oil exports fell drastically and in January 2013, Iran's oil minister acknowledged that the fall in oil exports was costing the country between US $ 4 billion and 8 billion each month. Iran is believed to have suffered a loss of about US $ 26 billion in oil revenue in 2012 from a total of US $ 95 billion in 2011. In April 2013, the International Monetary Fund (IMF) forecast that Iran's Gross Domestic Product (GDP) would shrink by 1.3 percent in 2013 after contracting by 1.9 percent the previous year.

In exchange for Iran's commitment to limit its nuclear capabilities and its pledge to limit its nuclear energy activities for purely peaceful purposes, the United Nations Security Council, on July 20, 2015, unanimously approved a resolution that created the basis for international economic sanctions against Iran to be lifted.[13]

Buoyed by the degree of success, albeit still speculative, as a result of the sanction measures against Iran, the US tried to buttress similar tenets in an entirely different domain. The US, wary of cyber-economic espionage initiated by Chinese hackers—perhaps with the tacit approval and support of the Chinese government—has suffered enormous monetary losses as well as

11. National Conference of Catholic Bishops, "The Harvest of Justice Is Sown in Peace: A Reflection of the National Conference of Bishops on the Tenth Anniversary of the Challenge to Peace" (Washington, DC: United States Catholic Conference, 1994).
12. US Department of State, "Diplomacy in Action : Iran Sanctions", http://www.state.gov/e/eb/tfs/spi/iran/ index.htm. Accessed on September 10, 2015.
13. Somini Sengupta, "UN Moves to Lift Iran Sanctions After Nuclear Deal, Setting Up a Clash in Congress", *New York Times*, July 20, 2015, http://www.nytimes.com/2015/07/21/world/middleeast/security-council-following-iran-nuclear-pact-votes-to-lift-sanctions.html?_r=0. Accessed on January 10, 2016.

loss of intellectual property and prestige. For the US, securing the cyber space represents the Holy Grail of "National Security." In response to the rising wave of cyber attacks exponentially growing in numbers and the potential severity of subsequent consequences, the US tried to put in place a framework intended to subject the Chinese companies and individuals, who have been direct or incidental beneficiaries of U.S. trade secrets through cyber theft by the Chinese government, to unprecedented economic sanctions.[14]

The provision of sanctions against the Chinese companies and individuals, once enacted and established as an expedient, would mark the far-reaching use of the Executive Order (EO) signed by President Barack Obama in April 2015. The EO, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", identifies increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, persons located, in whole or in substantial part, outside the United States as an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.[15] The EO explicitly specifies blockage of all property and interests in property in the US of persons responsible for, or engaged in, either directly or indirectly, cyber-enabled activities.

This US move is being described as the second serious and important shot at deterring China on the issue of cyber espionage. In May 2014, in a first-of-its-kind case, the US Justice Department indicted five Chinese military officers on charges of stealing data from six US companies. The US formally accused the Chinese officers and sought their extradition to face charges under US laws for infiltrating the computer networks of six US companies and for stealing data, which could be leveraged for benefit by their trade competitors. The Federal Bureau of Investigation (FBI) had

14. David Nakamura, "US Developing Sanctions Against China Over Cyberthefts", *The Washington Post* , August 30, 2015, https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html. Accessed on January 10, 2016.
15. The White House : Office of the Press Secretary, Executive Order: "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", April 1, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m. Accessed on January 10, 2016.

A nation's resolve to deter cyber attacks needs to be part of its overarching defence strategy, encompassing all instruments of national power: diplomatic, economic, informational and military.

gone to the extent of putting the faces of the five officials on 'Wanted' posters.[16]

However, some US officials within the government cautioned against such moves and questioned their overall efficacy in the long run, arguing that sanctions might not act as a deterrent and would exacerbate tensions in the already tumultuous diplomatic relations between the United States and China. Besides, the US taking the moral high ground appeared to be dichotomous, when the US itself is accused of perpetrating cyber espionage, mass surveillance and other forms of information gathering directed at its allies and adversaries. The whole exercise orchestrated by the US appeared to be an attempt to "send a strong message" to Beijing, probably as an attempt to bolster its cyber deterrent posture.

Sanctions alone cannot bring in a paradigm change in the sinister and belligerent cyber behaviour of a determined adversary. A nation's resolve to deter cyber attacks needs to be part of its overarching defence strategy, encompassing all instruments of national power: diplomatic, economic, informational and military. The shroud of anonymity behind which cyber criminals operate has made the process of establishing the identity of transgressors an arduous one. Attribution is the first step in assigning responsibilities and seeking appropriate recourse against transgressors. The economic linkages in this global era have become much more interdependent and entwined and economic prudence does not justify such mutually incriminatory measures. On the other hand, it may adversely impact the mutually beneficial economic ties between two counties as reprisals frequently lead to counter-reprisals and further escalation in already tense bilateral relations.

16. Eric Holder, "Chinese Military Officials Charged with Stealing US Data as Tensions Escalate", *The Guardian*, May 20, 2014, http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage, May 20, 2014. Accessed on January 10, 2016.

CONCLUSION

The fruition of a credible deterrence strategy built on traditional threat evaluation is in itself a complex process, and the complexities are further exacerbated when ambiguities associated with operations in cyber space are factored in. Historically, the measures of successful conduct of war manifest in territorial gains or attrition or annihilation of enemy forces. Deterrence, by contrast, is an exercise in shaping the mindset of adversaries and fanning the fear of retaliatory actions far exceeding the cost of potential misadventure. The process involves formulation of policy, proportionate capacity building, overt display of capabilities and convincing the adversary of one's intent. With nuclear deterrence, the deterrence posturing involves exploiting the primordial element of fear.

While gauging the impact of cyber weaponry and overall threat of cyber war looming large in the near future, it is worth the effort to try to ascertain its footprint on the global geo-political landscape.

While gauging the impact of cyber weaponry and overall threat of cyber war looming large in the near future, it is worth the effort to try to ascertain its footprint on the global geo-political landscape. Cyber weapons have yet to prove themselves as capable of altering the strategic military balance among states engaged in military conflict. Some critics point out that a cursory comparison between cyber and nuclear weapons is enough to prove the vanity and vexation of cyber weapons. In the context of nuclear weapons, James Chadwick discovered the neutron in 1932 for which he was awarded the Nobel Prize, and in 1945, the world witnessed the devastation and destruction by the first atomic bomb. Its use ended World War II, followed by shaping the strategic relations between the superpowers over the next five decades. The possession and the ability to launch nuclear weapons within the available temporal window are central to inter-state power relationships, as lucidly illustrated by the Iranian and North Korean examples. In comparison, close to 15 years have passed since the tenets of cyber warfare started intriguing the strategists and practitioners of warfare, and the world

has yet to witness a state forced into subliminal subjugation let alone overthrown, exclusively or even primarily by cyber attacks,

The argument does not in any way question the validity of deterrence in cyber space. Establishing deterrence in cyber space is not an easy task owing to the lack of a clear delineation of a cyber attack from technical glitches, cyber crimes or a blatant act of war. The detection, categorisation and initiation of response commensurate to the severity of attack will require technical scaffolding and a policy framework. The existential chasm between deterrence theory in cyber space and its practice is broad and needs to be bridged with clearly stated, and substantiated by, policy, procedures and guidelines.