WHAT MILITARY DETERRENCE CANNOT DO, CYBER DETERRENCE CAN DO TO IRAN: EXPLORING THE IMPLICATIONS OF MANIPULATIVE INCESSANT USAGE OF THE TERM 'PRE-EMPTIVE'

Sanghamitra Nath

Jawaharlal Nehru University, New Delhi, India

Email: sanghamitranath@hotmail.com

-Abstract-

Does international politics today face a crisis in conceptual clarity? Curiously so. The Israeli threat of *pre-emptive* military strikes against Iran for its current uranium enrichment program is essentially a threat of *preventive* attack in anticipation of a probable security risk in the distant future. Conversely, it is Iran which faces an imminent threat from Israel and can resort to *pre-emptive measures* on grounds of self-defense. This terminological confusion is a political manipulation to avail of the exception to the threat or use of force under Article 51 of the UN Charter as well as legitimize the exercise of **cyber deterrence** through Stuxnet and Flame viruses. Cyber deterrence must be the latest addition to the conventional military deterrence strategies as it embodies the threat of Unilaterally inflicted Assured Destruction (UAD), particularly through cyber war. Since cyber wars can transform conflicts or wars into asymmetrical battles for power, they can dangerously impede self-defense. Thus, the international community should unanimously consent to abandon the use of cyber deterrence strategies for a peaceful and safe present and future.

Key words: Pre-emptive attacks, Preventive attacks, Cyber Deterrence, Cyber War, Unilaterally inflicted Assured Destruction (UAD)

JEL Classification: N45 - Middle East, H77 - Intergovernmental Relations, F51-International Conflicts, F52 - National Security, D74 – Conflict and Conflict Resolution, O33 - Technological Change: Choices and Consequences and Diffusion Processes, D82 - Asymmetric and Private Information, K42-Illegal Behavior and the Enforcement of Law

1. Introduction

Strangely, international politics has displayed an unmistakable crisis in conceptual clarity in the recent issue of 'Iranian Nuclear Crisis'. A closer look at the Israeli threat of *pre-emptive* military strikes against Iran reveals that it is essentially a *preventive* attack against a probable threat in the distant future from Iran. Conversely, it is Iran which faces an imminent threat from Israel and can resort to *pre-emptive measures* on grounds of self-defense. Concepts like 'Pre-emptive' and 'Preventive' do not mean the same and, therefore, should be used discretionally in any serious unbiased discussion on world politics.

For any pre-emptive strike, there must be an imminent threat which is presently lacking from the Iranian side. (BBC, 25 April 2012) Iran does not pose an imminent threat to Israel for two reasons: firstly, the International Atomic Energy Agency (IAEA) is yet to confirm that Iran has the nuclear bomb, and secondly, the mere presence of a nuclear bomb does not automatically translate into an imminent threat for the neighbouring countries. If it did then Pakistan, India and China would be continuous sources of imminent threat to one another. Moreover, Israel would be problematising its very stance on the Iranian nuclear issue as it is the sole possessor of nuclear warheads under the policy of nuclear ambiguity in the nuclear free Middle East. (Middle East Online, 20 September 2012) And, interestingly it does.

However, the 'preventive' strike has been made synonymous with 'pre-emptive' strike precisely to absolve the former of the illegality in international law. A direct equation of 'preventive' strikes with 'pre-emptive' can avail of the advantage of Article 51 of the United Nations (UN) Charter, that is, the exception to the threat or use of force for the purpose of self-defense. In other words, the terminological collision is politically motivated to acquire the immunity under the right to self-defense with threat or use of force.

1.1. What is pre-emptive war?

A pre-emptive war is a war in self-defense provided that there is the threat of an "imminent and certain attack" by one state upon another. (Williams and Williams, 1974:139) There is a mutual expectation of attack and a pre-emptive war aims to neutralize the impending attack by a first attack by the defending state. (Kurtulus, 2007:225) According to Lt Gen Benny Gantz, Chief of Staff of Israeli Defense Force, Iran has not yet decided whether to build the nuclear bomb and thus, it does not pose any imminent threat to Israel. (BBC, 25 April 2012)

1.2. What is preventive war?

According to David Luban (2004:220), the characteristics of a preventive war are (a) imminence of military threat is reduced or lacking (b) the military threat is a distant probability. These features transform a preventive war *from* a war of self-defense *into* a war to prevent a state from adopting a policy conducive to commit crimes against peace in the distant future. Therefore, preventive war is a war of law enforcement and resembles more of a war of aggression. (Luban, 2004:213)

It is argued that Israel condemns the uranium enrichment activity itself as an unacceptable threat irrespective of whether it is a weaponisation program. (Waltz, 2012:3) Moreover, Israel is the only nuclear weapons state (NWS) in the Middle East and if Iran at all becomes a NWS, Israel will not only lose its nuclear monopoly in the region but also expect a shift in the balance of power greater than the cost of war. In such a situation, Israel could lodge a preventive war against Iran to retain the status quo in power as well as its offensive/defensive technological capability. (Bas and Coe, 2010:2) This explains Israel's incessant usage of the term 'pre-emptive' in order to conjure the illusion of an imminent threat to justify its forthcoming assault on Iran legally, politically and morally.

In this paper, the author intends to explore the implications of the manipulative incessant usage of the term 'pre-emptive'. Yet, the thrust of this paper lies in the exploration of the doctrine of cyber deterrence. In the light of the Stuxnet and Flame viruses, this paper seeks to analyse the advantages of cyber deterrence over military deterrence. Herein, cyber war is defined as one of the strategies of cyber deterrence which guarantees ***Unilaterally inflicted Assured Destruction*** **(UAD).** Lastly, this paper discusses the legality of cyber threat and cyber war under the garb of self-defense.

2. A Problematic Paradigm: The Unspoken Truths

An objective view of the conventional deterrence paradigm discloses that it is value-loaded from the beginning. The deterrence paradigm is conceptualised from the perspective of the defending state. *To deter a state* is to already presume that a *hostile* state is planning to launch a military attack against another state. Therefore, the deterrence paradigm recalls the Freudian psychoanalysis---'me'/ defending state and 'not me'/'other' state. The 'me' is purposively defined in opposition to the 'other'. The function of such a deliberate distinction between the 'me' and the 'other' in international relations is to legitimise why one should and the 'other' should not have nuclear weapons.

Within this problematic framework of deterrence paradigm, Iran's status is that of the hostile 'other' vis-a-vis the defending states of Israel and the United States (US). Iran's nuclear program is viewed as an offensive capacity build-up to harm them in the near future and therefore, it needs to be deterred (through economic sanctions and may be even air strikes at the sites of nuclear program). The fact that Israel and US seek ‘to deter’ Iran from carrying on its nuclear program overshadows equally relevant facts like:

- **Nuclear Weapon States of Israel and the US: Real Threat to Peace and Security**

Though the Iranian President Ahmadinejad announced, "We do not need an atomic bomb” (BBC, 6 March 2012) and declared its present uranium enrichment program was meant purely for peaceful purposes, the West (especially the US), Israel and the International Atomic Energy Agency (IAEA) refused to accept the same. Their underlying rationale for this opposition is that the mere possession of nuclear weapons by Iran will threaten international peace and security. If possession of nuclear weapons itself threatened international peace and security, Israel and the US should be the ‘hostile’ states.

It is an open secret that Israel possesses nuclear weapons at the Negev Nuclear Research Centre near the desert town of Dimona. (The Guardian, 23 May 2010**)** (Cohen 1998) As for US, the Nuclear Non-Proliferation Treaty (1968) permits the US to retain nuclear arsenals as well as recognizes it as a legitimate NWS. In contrast, Iran still does not have the N-bomb. In the IAEA report (November 2011), it mentioned that “Under its Safeguards Agreement, Iran has declared to the Agency fifteen nuclear facilities and nine locations outside facilities where nuclear material is customarily used (LOFs)” and these facilities and sites were “nevertheless under Agency safeguards”. (IAEA, 24 February 2012:3) If Iran actually pursued nuclear weaponisation program, it would have been detected by the watchful eyes of IAEA. In the exceptional case of Parchin, Yukiya Amano, director general of the International Atomic Energy Agency (IAEA), said that the IAEA and Tehran were near to signing an agreement wherein greater cooperation will be achieved for inspection of the nuclear sites and that inspection of the Parchin military site had been included in this agreement. (BBC, 18 May 2012)

- **The Principle of Proportionality: Zero is to Two**

Every nation has the right to self-defense according to Article 51 of the UN Charter. The corollary to this holds that every nation has the right to feel threatened. Every nation has the right to judge for itself who its enemies are and what offensives they are likely to face during heightened crisis. By this logic, the US and Israel have justified its possession of nuclear weapons. Then, why should Iran be excluded from the right to self-defense, the right to feel threatened and the right to possess nuclear weapons?

The argument here is, the right to self-defense, the right to feel threatened and the right to possess nuclear weapons cannot be treated as privileges. The very term ‘right’ inheres that everybody deserves to enjoy certain benefits. To permit certain countries ‘rights’ and not permit ‘others’ transforms rights for all into privileges for some.

This brings in the issue of the principle of proportionality. Iran is currently a non-NWS while the US *and* Israel are NWS. This makes a ratio of **none is to two** nuclear weapons *or* zero ‘right’ is to two ‘privileges’. Without concrete IAEA evidence of Iran actively pursuing a policy of nuclear weaponisation program, the threats by the US (economic and military sanctions) and Israel (pre-emptive strikes) against Iran challenge the principle of proportionality.

- **A Discriminatory NPT: Iran neither at par with nor secure from US and Israel**

Under the NPT (1968, ratified in 1970), only the P-5 are allowed to remain as NWS. As a recognised non-NWS, Iran can never be at par with the US. Furthermore, it is natural that Iran feels threatened by being branded as a ‘rogue’ state, the recent US sponsored collapse of ‘rogue’ regimes around it (Iraq, Libya) and the immunity granted to US by NPT despite its failure to gradually ‘pursue nuclear disarmament aimed at the ultimate elimination of their nuclear arsenals’. (Vanaik, 1988:1825)

Israel itself is a NWS under the policy of ‘nuclear opacity’ and refuses to be party to the NPT. In 2009, the IAEA had asked Israel to join the NPT as well as open its nuclear sites for inspection “under comprehensive IAEA safeguards” but Israel had firmly rejected both calls. (BBC, 6 March 2012**)** At the same time, Israel disallows Iran to have nuclear weapons retaining the right to self-defense and the right to feel threatened to only itself. Therefore, Iran is neither at par nor secure from Israel too.

3. Unleashing the Virtual Power: The Offensive Potential of Cyber Deterrence

In November 2010, the uranium enriching centrifuges at Natanz were shutdown with Stuxnet virus. (Wikipedia, 12 September 2012) In June 2012, the computers at the uranium enrichment site were compromised with Flame malware aimed to collect intelligence on mechanical and electrical equipment. (BBC 4 June 2012) According to New York Times (1 June 2012), the US and Israel were jointly involved in the surreptitious introduction of Stuxnet virus to the Iranian computers but no confirmed report has come on the creators of Flame virus.

Cyber deterrence strategy must be the latest addition to the traditional deterrence strategy. Rationally, cyber offensive techniques provide greater negotiation power for states in pursuit of self-defense. From the perspective of Israel and US, the creation, penetration and objective of the viruses were in pursuit of national security. From the perspective of Iran, the clandestine infiltration of the viruses was a violation of its sovereignty.

The cyber deterrence paradigm is composed of cyber tactics, offensive and defensive. The cyber tactics range from cyber attacks to cyber threats and finally, to cyber war. The range of techniques has been arranged on the basis of their potential to endanger national security.

3.1. Cyber Attack

This kind of attack is directed at the intellectual property (IP) essentially oriented around the nations' defenses. Therefore, a nation's defense-related IP becomes the object of target for the adversary. Computers of the nation's ministry of defense, private defense companies and defense officials are the databases of defense-related IP and cyber attack is directed to gain unauthorised access to the same. Cyber attack also includes attack on information stored in social networking sites like Gmail, Hotmail, Aol and so on.

Cyber attack can also be referred to as 'hacking' or 'data theft' or 'cyber espionage'. Data hack can happen in several ways for example, cracking of passwords, phishing, bots and more. The worrying aspect of cyber attack is , till now it has not been detected immediately at the time of occurrence. (BBC, 20 September 2011**)** Besides, one does not know what is done with the data hacked---what use it is put to, whom it is shared with or sold to and many more. If the attack is conducted from outside the nation's territory or from the adversary's territory, it is difficult to pin down the real attacker. Though the country of origin of the hack can been traced, the real individual hackers have often gone unpunished.

3.2. Cyber Threat

This phenomenon is definitely more dangerous than the previous one. The object of threat is the nation's digitally controlled infrastructure including defense, economy, communication and transport, water, power and more. The adversary's aim is to cripple those computers to halt the normal functioning of the country.

Estonia was the first country to be hit by cyber threat. Beginning in April 2007, this small Baltic country suffered three-weeks of cyber threat. Due to lack of clarity, the cyber threat was referred to as 'cyber attack' by Wikipedia (30 May 2012), and 'cyber war' by The Guardian (17 May 2007).

The pertinent question at this moment is, why an assault on digital infrastructure and digitally-controlled infrastructure should be labeled as 'cyber threat'. It needs to be so because it inheres the fear of Unilaterally inflicted Assured Destruction (UAD). The act of freezing a nation's critical infrastructure through cyber weapons (like virus) is the expression of the strength of the aggressive state as well as the realistic nature of the threats.

For example in June 1982, the CIA tampered the software of the computer-control system of the Soviet gas pipeline causing a massive blast that could be seen even from space. This is a good illustration of UAD wherein the enemy was not given a hint of the infiltration of its computer-control system of the Soviet gas pipeline. Most importantly, the Soviets were not given the chance to prepare for self-defense or counter-offensive precisely due to the lack of knowledge or detection of the infiltration.

Cyber threat, through the suppression of the nation's critical infrastructure, sets the stage for cyber war or UAD.

3.3. Cyber War

This kind of war must be avoided at all costs. It is a war whose objective is to preclude a section of humanity from the right to self defense during the assault on sovereignty and its territorial integrity. Therefore, cyber war is the actualisation of the threat of UAD. It is a performance of UAD with massive destruction of lives and property.

In this kind of war, first the enemy is made vulnerable by suppressing its defense system and other critical infrastructure like power. This is followed by military attack on the enemy's territory so that the sovereign is rendered completely defeated. Thus, this kind of war is best described as a combination of cyber threat *and* military assault including air strikes, army and the navy, on the enemy.

In the sphere of defense, computers have become indispensable. Once the computers are compromised with cyber weapons (like viruses) so that the vital functions come to a standstill, the stage is set for the final offensive attack. Moreover, the data sent from one computer may be intercepted, the flow of information terminated and/or replaced with misinformation which subsequently flows to the destination terminals. The longer the computers are compromised, the greater are the chances of the success of UAD.

4. What Cyber Deterrence can, Military Deterrence cannot: The Advantage of Cyber Deterrence over Conventional Deterrence

In conventional military deterrence, the objective is to communicate to the hostile state of the costs of non-compliance and the benefits of compliance. However, the threat of Mutually Assured Destruction (MAD) makes each state equally capable of destroying the other. Real deterrence looks for an opportunity to transcend equal capability. Cyber deterrence with its threat of UAD scores above military deterrence. Given Iran's recalcitrant behaviour, Israel and US may prefer cyber deterrence over military deterrence.

If Israel were to launch pre-emptive strikes to deter Iran, the Israeli Air Force (IAF) would have to overcome several obstacles. It would have multiple targets to strike, most of which are located underground. The war planes would have to strike from a "relatively close range… fight its way in and out of heavily-contested [Iranian] airspace" according to Robert Hewson, IHS Jane's Air-Launched Weapons. (BBC, 27 February 2012**)** Iran would have to obtain fly-zone permits from either Turkey or Saudi Arabia or Iraq for the IAF to reach Iran.

On the contrary, cyber deterrence can achieve more with lesser risks to Israel. The advantages of cyber deterrence are:

- The adversary can be struck from within the defending state's territory. Cyber deterrence uses cyber weapons to deter the enemy from pursuing a certain course of action. These cyber weapons like malignant virus, DDoS and other malware applications can be distributed into the enemy's server via the Internet irrespective of firewalls and anti-virus protection. The defending state need not send its force nor undertake the risk of a direct confrontation with adversary's military force. Consequently, it would eliminate IAF's need for fly-zone permits and the permit for air-to-air refuelling from its neighbouring states.
- Cyber threat can easily turn into UAD cyber war. Therefore, cyber threat is a more effective deterrent than the conventional deterrent.
- Sudden unannounced cyber threat can dangerously shorten critical reaction time for a well-strategized response and weaken self- defense. An unexpected cyber threat precariously leaves a target state susceptible to military attacks from outside.
- International law has not adequately developed on the issue of cyber threat, cyber war and cyber attack. In the absence of a global consensus on what constitutes cyber threat, cyber war and cyber attack, there is no proper provision in international law to deal with the emerging fifth domain of warfare. In the case of Iran, neither Israel nor the US has been made accountable for the damage

caused by Stuxnet virus. The US might justify its involvement in the Stuxnet virus cyber threat as a 'War against Terror' or 'War against Proliferation' by a 'rogue' state. Does that mean that Iran has lesser rights to self defense? The UN Charter does not specify that rogue states do not have the **right to self defense** under Article 51. As an independent sovereign, Iran has equal rights to self-defense as the US (and Israel).

5. Conclusion

Ironically, cyber deterrence should not be practiced precisely because of the advantages it offers. The advantages built into cyber deterrence makes it one of the most dangerous ways to deter a state. Cyber deterrence, with special emphasis on cyber threat and cyber war, violates Article 2(4) of the UN Charter which bans the threat or use of force. True, Israel's regional sole nuclear hegemony has provoked further insecurity in the Middle East. Only a rival nuclear power can counter the hegemony and bring stability to the region which justifies "Why Iran Should Get the Bomb". (Waltz, 2012:3)

Yet, the author is of the opinion that it is time to begin complete and immediate nuclear disarmament among all nuclear weapons states of the world. It is objectively, legally and ethically wrong to allow the world to be divided into rightful nuclear haves and have-nots.

Similarly, the author strongly recommends that the world should unanimously consent to abandon the use of cyber deterrence. According to Rawls, to promote a sense of justice in the international system, each state "is to have an equal right to the most extensive liberty compatible with a similar liberty to others" (Freeman, 1999:48). Therefore, if one state practiced cyber deterrence through surreptitious cyber technologies then it would be unjust to preclude other states from resorting to the same. If no state exercised the choice of cyber deterrence and especially cyber war (UAD), it would set an example for others to abide by.

Bibliography

1. Middle East Online (20 September 2012), *Israel steps outside flock: Summit on nuclear-free Mideast unrealistic,* http://www.middle-east-online.com/english/?id=54478, [Accessed 26.09.2012]
2. Reynolds, James, BBC (25 April 2012), *Iran undecided on nuclear bomb - Israel military chief,* http://www.bbc.co.uk/news/world-middle-east-17837768, [Accessed on 25.04.2012]
3. Williams, Geoffrey Lee and Alan Lee Williams (1974), Crisis in European Defense: The Next Ten Years, London: Charles Knight & Co Ltd.

4. Kurtulus, Ersun N (2007), "The Notion of a 'Pre-Emptive War': the Six Day War Revisited", *Middle East Journal*, Vol. 61, No. 2, pp. 220-238.
5. Luban, David (2004), "Preventive War", *Philosophy & Public Affairs*, Vol. 32, No. 3, pp. 207-248
6. Waltz, Kenneth N, Foreign Affairs (2012), *Why Iran Should Get the Bomb*, http://sistemas.mre.gov.br/kitweb/datafiles/IRBr/pt-br/file/CAD/LXII%20CAD/Pol%C3%ADtica/Why%20Iran%20Should%20Get%20the%20Bomb.pdf, [Accessed 13.08.2012]
7. Bas, Muhammet A. and Andrew J. Coe (2010), "Arms Diffusion and War" *Department of Government Harvard University Working Paper*. Cambridge: Harvard University
8. BBC (6 March 2012), *Q&A: Iran nuclear issue,* http://www.bbc.co.uk/news/world-middle-east-11709428, [Accessed 6.03.2012]
9. Tisdall, Simon, The Guardian (23 May 2010), *Israel's nuclear weapons: the end to nods, winks and blind eyes*, http://www.guardian.co.uk/commentisfree/2010/may/23/israel-nuclear-weapons, [Accessed 24.05.2012]
10. Cohen, Avner (1998), Israel and the Bomb, New York: Columbia University Press
11. International Atomic Energy Agency (24 February 2012), *Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran,* http://www.iaea.org/Publications/Documents/Board/2012/gov2012-9.pdf, [Accessed 24.05.2012]
12. BBC (18 May 2012), *UN nuclear chief to visit Iran for talks,* http://www.bbc.co.uk/news/world-middle-east-18122752, [Accessed on 18.05.2012]
13. Vanaik, Achin (1988), "Why NPT Is Unacceptable", *Economic and Political Weekly*, Vol 23, No. 36, pp. 1825
14. Wikipedia (12 September 2012), *Stuxnet*, http://en.wikipedia.org/wiki/Stuxnet, [Accessed 16.09.2012]
15. Lee, Dave, BBC (4 June 2012), *Flame: Attackers 'sought confidential Iran data'*, http://www.bbc.com/news/technology-18324234, [Accessed 6.06.2012]
16. Sanger, David E, New York Times (1 June 2012), *Obama Order Sped Up Wave of Cyberattacks Against Iran,* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all, [Accessed 6.06.2012]

17. Wikipedia (30 May 2012), *2007 cyberattacks on Estonia*, http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia, [Accessed 17.06.2012]
18. Traynor, Ian, The Guardian (17 May 2007), *Russia accused of unleashing cyberwar to disable Estonia*, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, [Accessed 17.02.2012]
19. Marcus, Jonathan, BBC (27 February 2012), *How Israel might strike at Iran,* http://www.bbc.co.uk/news/world-middle-east-17115643, [Accessed 27.02.2012]
20. Rawls, John (1999), "Justice as Fairness", (in: Samuel Freeman-Ed., *Collected Papers: John Rawls,*), New Delhi: Oxford University Press , pp 1- 672