Cyber Terror Threats to Nuclear Command and Control

An Issue Brief

Cyber Terror Threats to Nuclear Command and Control

By

Gp Capt GD Sharma, VSM (Retd)

Aligned with the Future

सत्यमेव जयते

Victory through Joint Knowledge

Centre for Joint Warfare Studies (CENJOWS)
New Delhi

ISBN : 978-93-84492-09-0
Price in India : ₹ 150 /-

The views expressed in the book are of the author and not necessarily those of the Centre for Joint Warfare Studies/publishers.

Printed in India

Printed by
Xtreme Office Aids Pvt. Ltd.
Basement Bhanot Building (Below Syndicate Bank)
Nangal Raya Commercial Complex, N.D-110046
Ph.: 9311156526
E-mail: xtremeofficeaids@gmail.com
Website: www.xtremeonline.in

Cyber Terror Threats to Nuclear Command and Control

The damage and radiation caused by Fukushima disaster of 2011 are well known. This accident was caused by nature. Now, consider that the damage is not by nature or nuclear accident but, by a cyber-attack or physical attack on a nuclear facility. As many countries are turning towards civil nuclear energy in quest for clean energy to meet their energy need, the threat of cyber or physical attack on the nuclear establishment has increased manifold. There is a significant and continuing threat of nuclear terrorism from misguided elements and likes of terror groups such as Al Qaeda and ISIS. Latter, having taken control of large swath of territory in Iraq and Syria is reported to have shown interest to acquire the weapons of mass destruction to blackmail the world towards its aim of consolidating and expanding the self declared Caliphate.[1] The alarm for this possibility has also been sounded by the former Britain's home Minister Theresa May too; who while suggesting fresh measures against the group, warned that the group could become the first terrorist state and threaten Britain with nuclear and chemical weapons.[2] The probability of threat has magnified in view of increased pressure on the outfit by Iraqi and Syrian armies and their partners which may motivate these outfits towards acquiring nuclear capability. A nuclear blast at the hands of terrorists or a rogue states would be catastrophic and if the victim state responds, it would result in thousands of casualties, disruptions to markets and commerce, long-term implications for public health and the environment with possibility of aggravation. The international community is aware of this threat for past two decades and has been looking for the answers to contain the threat. In the past decade, in particular, there has been significant rise in the discourse involving

[1] The Times of India 06 Oct 2014. The news report titled," ISIS planning war on Iran for nuclear weapons."

[2] The Times of India 01 Oct 2014. The news report is titled,"ISIS could become the world's first terror state warns UK".

the terrorism and nuclear weapons. The United Nation too is fully conscious of it. In 2005, the UN Secretary General while delivering a key note address at the plenary session of the summit held at Spain on democracy, terrorism and security has labeled nuclear terrorism as one of the most serious threats of our time saying, "Nuclear terrorism is still often treated as science fiction. I wish it were. But unfortunately we live in a world of excess hazardous materials and abundant technological know-how, in which some terrorists clearly state their intention to inflict catastrophic casualties."[3]

Motivation for Attack

What could motivate the terror group to acquire and use the weapon of mass destruction is a complex affair and it happens in a dynamic and evolving circumstances. A perceived threat to their religion is a sufficient motivation to a religious fanatic. A religiously inspired terrorist thinks that any action how so ever heinous, since it leads to his perceived divine end, is justified. Revenge is yet another factor that can enormously motivate a terror group to choose a nuclear path. For example, in the aftermath of US intervention in Afghanistan to destabilize and neutralize the AL Qaeda, the revenge and identity became dominant in the thought process of Al Qaeda.[4] ISIS by promising a caliphate has its ranks being filled by men and women from all over the world, who see Muslims as underdogs, and have the sense of privilege and pride for being chosen to fight to restore the past glory to Islam.[5] They have hijacked the Syrian uprising and transformed the Middle East as their battle ground.

Cyber Threat

The threats from cyber-attacks are no longer from only private hackers or organized criminals but, also sponsored by the nation states. The real reason for this is a phenomenon of gradual shift in all areas from analogue systems to the digitalization of operational functions and working processes. As digitization increases in quality and efficiency, the nuclear facilities too world over, are progressively becoming

[3] http://www.un.org/sg/statements/?nid=1345

[4] Nuclear terrorism : The New Weapon of the 21st century IDSA monograph series No27 December 2013

[5] A write up on ISIS by Martin Chulov. Accessed from https://www.theguardian.com/world/2015/sep/17/why-isis-fight-syria-iraq

heavily reliant on digital instrumentation or digital control systems or computer based information systems (IS). This development has given rise to new threat of hacking of nuclear control and processes.[6] In general, a considerable progress has been made in traditional nuclear security arena but, the threat of a cyber-attack is a different cattle of fish, it is recent and escalating while being most unobtrusive and difficult to detect. Nuclear Threat initiative (NTI)[7] in its several writings has warned of the cyber threat to the nuclear establishments and claimed that at present, no country is immune of the threat and nuclear cyber security practices haven't yet caught up with risk.

The cyber threat in nuclear realm will manifest in two forms.

(a) It can be used to undermine the security of nuclear materials and facility operations, and

(b) It can compromise nuclear command and control systems.

The traditional nuclear security practices have been focused on preventing physical attacks by putting in place "guns, guards, and gates" to prevent:-

(a) Theft of nuclear materials to build a bomb,

(b) Sabotage of a nuclear facility, or

The hacker can shut down the security system at a highly sensitive nuclear materials storage facility, giving access to terrorists seeking highly enriched uranium to make a bomb. He could seize control of operations at a nuclear power plant with an aim to cause a Fukushima scale melt down. Worse still, a hacker by accessing command and control network could even spoof a nuclear missile attack, leading to a miscalculated retaliatory strike from the adversary that could kill millions.

Preparedness to Fight the Cyber Threat

The international community has traditionally focused on physical threats to the nuclear facilities. But, cyber-attack, a newer form of

[6] Ibid

[7] NTI is a privately funded organization of America which is engaged in studies on risk posed by weapons of mass destruction (nuclear Biological and chemical).

threat is presenting a challenge. The Nuclear Threat Initiative (NTI), a privately funded organization engaged in flagging the issues on Weapons of Mass Destruction, has sponsored two studies on cyber security . The first study is with the Institute of Safety and Security at Bradenburg University of applied sciences which has expertise in cyber security and security issues. The study assessed the nuclear cyber security environment of a sample of five countries viz; China, Germany, South Africa, Russia and United States wherein, it focused on the legal, regulatory, and institutional frameworks i.e., the range of measures taken to contain / mitigate the cyber threat at the national level and at the facility level. The study disclosed a wide variation in their national approaches to cyber security at the nuclear facilities. It emerged that while the procedures and plans were somewhat institutionalized in Germany and United States but, in other states these were still in state of infancy and lacked institutional backing or were partially institutionalized.[8]

The second study was led by cyber security expert, George Chamales, who convened a group of cyber security and nuclear security experts to develop a new approach for protecting nuclear facilities from cyber-attacks that could lead to the theft of weapons/ usable nuclear materials or an act of radiological sabotage. Drawing upon the expertise of both nuclear and cyber security experts, NTI is working to develop a set of guiding principles for cyber security at nuclear facilities.[9] At present the nuclear facilities of all the states including the developed states are facing the risk of cyber-attacks.

Constituents of Nuclear Command and Control System

The purpose of Nuclear Command and Control System (NCCS) is to provide the Nuclear Command Authority (NCA) a capability required to exercise his authority over the nuclear weapon operations. U.S. Congress Research Service in its report defines the Nuclear Command and Control System (NCCS) “as infrastructure which supports the President and his combatant commanders when they direct nuclear forces. It involves the designated combination of flexible and enduring elements including facilities, equipment,

[8] http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675

[9] http://www.nti.org/about/projects/addressing-cyber-nuclear-security-threats/

communications, procedures, personnel, and the structure in which these elements are integrated, all of which are essential for planning, directing, and controlling nuclear weapon operations of military forces and the activities that support those operations."[10]

In context to India, this will translate to the infrastructure required to house Nuclear Command and Control Centers for NCA, Strategic Forces Command (SFC), Chairman Chief of Staff, storage of delivery means, nuclear core and warheads and array of communication and personnel. Our nuclear command and control system (NCCS) must support situation monitoring, warning and attack assessment of missile launches, decision making, dissemination of NCA orders, choice of delivery, mobility of forces and finally management of geographically dispersed forces. A robust infrastructure, tied together by the command, control, computers, communication, intelligence, surveillance, reconnaissance, and planning architecture is the need of the day.

Some of the major functions that the NCCS must perform include:-

Situational Awareness. The command element must monitor the strategic intelligence both from classified means, electronic and from open sources. This will translate in to a decision on number, type, size, probable targets for attack and location of storage of the nuclear constituents.

Early Warning and Attack Assessment. Timely detecting and analyzing a potential attack is most vital as most other functions will follow this. This is obtained from reliable radars and satellite warning systems. With our policy of No First Use, this function looks unnecessary since India would only respond to the adversary's nuclear launch but, this function assumes great importance if the adversary chooses to repeat nuclear launch.[11] Even in the first instant, we need early warning to activate our active (Ballistic Missile Defence) and passive defences (disaster management).

[10] Nuclear Command and Control: Current Programs and Issues. CRS report for Congress 03 May 2006 asses at http://fas.org/sgp/crs/nuke/RL33408.pdf

[11] India,s both nuclear neighbours have capability to launch repeat nuclear attack.

Decision Making: Prime Minister as the head of the political council gets the advice of the executive council which is headed by the National Security Advisor (NSA). Latter forms his view with inputs from intelligence, DRDO and AEC heads and defence from Chairman Chief of Staff and Service Chiefs. NCA based on the threat assessment may ordain moving nuclear arsenal to a higher state of alert which would call for moving the strategic forces to their operational locations.

Management of Nuclear Arsenal. This relates to storage, transit of mobile deterrents to their op locations, mating/ arming of the warheads. The process also covers collection of operational information (deterrent forces available, location and their readiness status) and its presentation to NCA in the Nuclear Command and Control Center. This data is needed on day to day basis by the NCA to for decision making.

Control Strategy. This involves elements of positive and negative control of the deterrent. Former means that weapons will only be launched after receiving launch order from the NCA. Whereas, negative control relates to following procedures (two man rule etc.) and Permissive Action Links (PAL)/electronic locks which would deny any unauthorized or accidental launch of the nuclear weapon.

The entire gamut of operations can be performed, if the communication are secure, reliable, jam proof, hardened with ability to operate, in extreme heat, blast, EMP and in Nuclear, Biological and Chemical (NBC) environment. The National Nuclear Command Centers themselves should be geographically well dispersed and hardened to withstand NBC environment. The communication should support rapid connectivity at all level i.e. from leadership to nuclear forces and free from false alarms. The command and control System of nuclear forces in India is not in public domain but, it is believed that it is built in layers for redundancy, comprising point to point – fiber optics, satellites, and V/UHF/ELF which are encrypted and secure with all attributes as discussed above.

Susceptibility of Nuclear Command and Control System to Terrorism

Nuclear command and control has inherent weaknesses in relation to terror / cyber warfare. The terrorist aim could be to make the system non-responsive when ordered to operate or spoof orders to launch a weapon when such order has not been given thus, initiating an unwanted nuclear war. While secrecy and ambiguity in plans and processes are believed to provide security but, if compromised the terrorist/ terror group could exploit the situation at every stage viz; the early warning, storage, equipment, communications, procedures, personnel all are vulnerable to a terror cyber threat. For example. the intentional spoofing of the early warning on adversary's nuclear state could cause review of status of nuclear forces when it is not needed leading to heightening of the tension or even launch of nuclear weapons. This is particularly true in case of US and Russia which continuously maintain one –half of their strategic arsenal strategic arsenals on high alert **"Launch on Warning"**. A sophisticated attacker from the cyber space could spoof the US or Russian early warning in to reporting that missiles have been launched, which would demand retaliatory strikes according to their nuclear doctrines, even if warning later turns out to be false, the retaliatory strike would have already been launched and an accidental nuclear war will have occurred.[12]

The storage facilities and equipment could face theft/ sabotage, or cyber-attack. The security software could be targeted to gain access to the nuclear facility. While the equipment could be made dysfunctional by a cyber-attack.[13] The communications are vulnerable at every level, from decision maker down wards to the nuclear forces. Even personnel could fall prey to terrorist propaganda on the social media and get disaffected leading them to act against the interest of the state hence, a multifaceted approach is needed to defeat the terror threat.

The concept of Mutually Assured Destruction (MAD) means that a state must have the capability to launch nuclear weapons even in the event of a decapitating strike. This requires having nuclear weapons spread out in multiple locations (mobility and redundancy),

[12] Franz-Stefan Gady " Could cyber attack led to a nuclear war "http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/

[13] Stuxnet attack on the Iranian nuclear centrifuges in 2011.

so that adversary is not able to destroy all capabilities. But, this also provides terrorists with multiple locations for attaining access to these weapons.

The concept of Mutually Assured Destruction also promotes a hair trigger launch posture and the need for launch orders to be decided on quickly. The terror groups could break in to the Command and Control network by falsifying commands which may result in launch of nuclear weapon and initiation of a unwanted nuclear war. Fortunately, in India, in pursuance to our policy of No First Use (NFU), the de-mated state of nuclear deterrent provides an inherent protection from terrorist induced/accidental launch of nuclear deterrent. In mated state however, our nuclear command and control is vulnerable. The vulnerability gets further aggravated with dispersal of arsenal, more particularly when it is mobile.

Why Cyber Terrorism Attracts Terror Outfits?

This threat in modern times have become a reality as militaries tend to place increasing reliance on computer networks, including experimental technology such as autonomous systems, as well as due to a desire to have multiple launch options, such as nuclear triad capability for reliable action. This also provides multiple entry points for terrorists. As nuclear capable states become more and more dependent on interconnected information technology for the military and civilian infrastructure, they become an increasingly viable target. Some automated response systems like, Perimeter, a Soviet system, was highly susceptible of being used by the terrorists. The system was designed for a retaliatory automatic launch of nuclear weapons at the designated target in response to a nuclear attack by the adversary, in the event, it was unable to establish communications with Soviet leadership which itself was highly susceptible to hacking by the terrorists.[14] In United States too, hackers have known to make multiple attempts to compromise the extremely low radio frequency used by the US Navy to send nuclear launch approval to submerged submarines. By using proxies, even multi-layered attacks could be engineered.[15] How debilitating is the cyber-attack can be gauged

[14] Hacking Nuclear Command and Control, a research paper by Jason Fritz BS (St. Cloud), MIR (Bond) for the International Commission on Nuclear Non-proliferation and Disarmament. Accessed on 01 Set 16 cnnd.org/Documents/Jason_Fetz_hacking-NC^2.doc

[15] ibid

from the fact that cyber-attack on the Iran nuclear network in 2011 had known to have caused extensive damage to their nuclear programme. The setback could be one of the indirect causes which led Iranians to abandon their pursuit of nuclear weapon programme. Features of the cyber terrorism are listed below:-

(a) It is relatively low cost, only requiring an off the shelf computer and an internet connection.

(b) A wide range of pre-written, automated, hacking tools are readily available on the internet and require little to learn.

(c) Cyber terrorism allows greater anonymity than traditional terrorism, as tracking the source of attacks is hindered by proxies, spoofed IP addresses, and legal hindrances. In terms of stealth, cyber terrorism allows for the silent retrieval of information from a computer, or the remote use of someone else’s computer to conduct activities. Cyber terrorists can strike an enormous number of targets around the globe without having to be physically present, thereby reducing the risk of death or injury to the attacker.

(d) This mode of attack enhances the speed of operations and eliminates the logistical problems of crossing borders. Reducing the risk of death, and the physical or psychological demands, makes it easier to recruit new members for their cause.

(e) Cyber terrorism has the potential to cause damage beyond the scope of traditional tactics, and when used in combination with traditional tactics, it can create synergy.

Modes Operandi of a Cyber Attack

The nuclear command and control must be survivable in the event of cyber warfare attacks. Therefore, it is important for the decision makers and operators to be aware of the potential danger posed by computer network operations.

Computers on Internet. All computers which are connected to the internet are susceptible to infiltration and remote control. These could be affected by a malware despite the fireballs and protective devices simply because; these are reactive and are developed after first appearance of the malware/virus.

Computers in Closed Network. Computers which operate on a closed network may also be compromised by various hacker methods, such as through wireless access points, embedded exploits in software and hardware, and maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. A disabling cyber-attack on the Iran nuclear network in 2011, greatly highlights the cyber threat to command and control network which could be exploited by the adversary and the terror network alike.

Terrorists could possibly fake a nuclear attack from the adversary by hacking and passing a command on its command and control channel to launch an attack. This is a much easier alternative for terrorist groups than actually building or acquiring a nuclear weapon or dirty bombs themselves. Terrorists would have the advantage of initiating fast attack at a relatively low cost, without compromising their secure location being far removed from the scene of action with geographical distance.

Terrorists could interfere the emergency communications within governments and post false information to unsettle the government functioning. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses.

Generally, hotlines are established between governments to deal and resolve tense or ambiguous situations which could precipitate a nuclear attack. Terrorists could disrupt or corrupt or knock out communications between these states so they even cannot discuss the situation and control it.

In the event of a warhead actually have been launched the terror group may even disrupt disaster relief operations by jamming or interfering the communications.[16]

[16] Report of the International Commission on Nuclear Non-Proliferation and Disarmament

India Nuclear Command and Control Structure

As per India's Nuclear doctrine, the retaliatory nuclear attack could be ordered if India and or its forces are attacked with weapon of mass destruction including Nuclear, chemical or biological weapons.

Nuclear Command Structure. The nuclear command structure has three components viz. the Political council, the Executive council and the Strategic Forces Command (SFC). In the Political Council besides, the Prime Minister who the chairs the council, there are Defence Minister, Foreign Minister and Finance Minister, in the council. The Principle secretary to the PM and the Cabinet Secretary are also present in the council. The retaliatory nuclear strike can only be ordered by the Prime Minister.

The Executive council is chaired by the National Security Advisor (NSA). The Cabinet Secretary, the Chairman Chief of Staff Committee, the Chairman Atomic Energy, the DRDO Chief and Commander, Strategic Forces Command (SFC) are part of the council with service chiefs in attendance. The council will provide inputs to the Political Council for decision making by the Prime Minister.

SFC has been established as the custodian and manager of the nuclear assets. SFC alone exercises the operational control of the nuclear weapons and all delivery systems. On receiving nuclear launch order, the SFC orders firing nukes using the appropriate launch vehicle. Thereupon, the DRDO and AEC which control the warhead and core respectively will mate the chosen weapons for use.

A clear step by step plan has been devised to eliminate the chances of any mischief or accidental detonation of the nuclear weapons.

How Susceptible is India's Nuclear Command and Control to Hacking?

Indian Nuclear command and control system is not in public domain but, it is positively not rudimentary. The fact that India possesses state of the art technology in communication, in the nuclear domain we positively would have established reliable communication as good as technology leaders like United States and others. In fact, the nuclear communication is claimed to be robust by the practitioners.

It is expected to have survivable, nuclear infrastructure comprising hardened operations rooms, layers of communications built on fiber optics, satellites based etc. with encryption and EMP compliance since India has declared the policy of No First Use and respond in retaliation to an adversary's misadventure of nuclear attack. India is also assumed to have safety locks to ensure that Indian nuclear warheads will explode only when desired. Our warheads are quite advanced therefore; it could be assumed that these safety locks are similar to PAL technologies.

India's nuclear command and control while not immune to such malicious intervention, has built in protection the way it is designed **Firstly,** as against the hair trigger nuclear posture as being maintained by five nuclear states, we maintain a recessed nuclear posture with our policy of no first use and choosing to launch nuclear weapon only in retaliation. **Secondly**, the weapons in peace time are in de-mated state with nuclear cores securely stored by Atomic Energy Commission while warheads and delivery vehicles are with DRDO and SFC/defence forces respectively. The overall system is so designed that at least three agencies i.e. service, AEC and DRDO will have to combine their efforts if the bomb has to be prepared for a launch. It is thus clear that in the de-mated state of the arsenal, the fear of any terror group hacking control of the strategic weapons is practically non-existent.

But when the armed forces go on full alert, then some of the nuclear cores are mated to the warhead and strike plans are reviewed. As the alert levels increase, the warhead is mated to the missile and the forces begin to lay out operational plans for moving it into launch positions. In the final stages, missiles may be moved to launch positions, targets are decided upon and a launch clearance in the form of an encrypted code is awaited that would give the order from the Prime Minister to fire. At the alert stage therefore, the threat of hacking would actually become potent.

In India, a complicated nuclear structure minimizes the risk of unsanctioned use of nuclear weapons. The experts call in question the reliability of the system's functioning under the condition of the first-nuclear-strike by the adversary. The reason is while the Prime Minister decides to launch a retaliatory nuclear attack, but in case he and council of minister are incapacitated after a nuclear attack on the capital, the nuclear weapons control system will be practically beheaded. While there are alternative ways for taking a decision on retaliation however, unlike Russia or the U.S., India, has not brought this procedure to perfection yet and on the other hand, there is a probability that country might be late in launching the attack on the enemy, says Pyotr Topychkanov, an expert at the Carnegie Centre, as unlike in other nuclear states, the chain of command is not clearly spelled out and remains a weak area in India. The non disclosure of the chain of command as in other nuclear state gives the credence that Indian nuclear decision takers views are contrary to the above belief.

Further, a Chief of Defence Staff (CDS) similar to those in other nuclear powers does not exist. Some groups in India oppose carrying out reforms in the nuclear weapons command and control system. They express fear that the appointment of a senior officer to head the system will lead to a growth in the authority of the armed forces and as a result enhance their influence disproportionately on India's internal and foreign policy. They have example of Pakistan before their eyes where the military control nuclear weapons and consistently interfere in the political process.[17]

In year 2000, a Group of Ministers, led by the then Deputy Prime Minister L.K. Advani, had recommended the appointment of a Chief of Defence Staff, the then Prime Minister, Atal Bihari Vajpayee, however, shelved the idea after resistance from politicians who are wary of creating a single-point military leadership. There seems to be rethinking on this issue. The incumbent Defence Minister, Mr. Manohar Parrikar on more than one occasion has stated that solution to the problem is being probed and eventually resolved.

The Command and Control situation could change after Indian-built Arihant nuclear-powered submarine is commissioned. To be a reliable deterrent, it could have nuclear arsenal in mated state as in other nuclear weapon states. The reason here is that the submarines sailing deep in the seas or oceans are capable of launching retaliatory attacks even when the country's armed forces are destroyed as a result

[17] PyotrTopychkanov an expert of of Carnegie Centre

of a nuclear attack. After becoming operational, these submarines will have nuclear weapons on board ready for use. Towards above aim, in March 2015, India test-fired a submarine-launched ballistic missile. This missile is capable of delivering an up to 2,000-kilogram-warhead to a distance of 3,500 kilometers. The Arihant and other future submarines will be equipped with these missiles. The current command control system for use of nuclear weapons will have to reformed to meet the changed situation

Further, we also need to be on guard as terror elements taking advantage of stated nuclear policy and antagonistic attitude of our immediate neighbour could provoke a nuclear response by even spoofing biological or chemical attacks emanating from it. In Indian context, we always have to remain alert from such spoofing attacks from our immediate neighbour as their close proximity significantly reduces the transit time of an incoming missile, making the rush to react even greater while not giving time to NCA, to coordinate if so felt.

The cyber threat has expanded dramatically in recent years, with a series of damaging, high-profile attacks that have made headlines around the world. Nuclear facilities and critical command and control systems are not immune to cyber attack—such an attack could facilitate the theft of weapons-usable nuclear materials or a catastrophic act of sabotage. In addition, there is even the possibility that nuclear weapons command and control could be compromised. NTI has in its report have brought several cases of theft and mishandling of radiating /fissionable materials. Between January 2013 and December 2015 it reported occurrence of 514 such incidents,[18] involving practically most states,which is cause of worry and calls for fool proof regulatory actions .

Unlike physical theft of material, cyber-attacks on the nuclear facilities are less obtrusive therefore, these are difficult to detect. While the operators and regulators around the world are working to understand and minimize these vulnerabilities, but cyber threats are becoming more sophisticated every day. Nuclear Threat initiative (NTI) is working with a global group of experts to reduce the threat

[18] http://www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/

and strengthen the means to protect nuclear facilities from cyber threats as well as to strengthen global capacity to respond to a cyber-attack on nuclear facilities.[19]

Advantage of a Robust Command and Control System

A robust command and control system is a prime ingredient in nuclear deterrent equation. In presence of robust nuclear command and control, the desire for the adversary to initiate an attack is hopefully decreases as the chances of executing a successful decapitating strike gets diminished. Moreover, with a survivable command and control system, a nation has better ability to communicate intentions and actions which in turn contributes in maintaining a stable relationship between the belligerents. There is a perception in India that with our 'No First Use' policy, we don't need elaborate command and control system as available in the developed countries. We could react appropriately after damage assessment and considering pros and con (military and geopolitical fallout) of the launch including the possibility of damage to the infrastructure by the EMP which invariably wreck the command and control infrastructure. Precisely for this reason, in our context, a robust C2 is needed which could direct conventional military operations, aid continuity of government in crises, and support civil authorities during natural disasters or emergencies. The effectiveness of the command and control can be assessed in only crises.

To assume that India's command and control would be immune to malicious intervention is a fallacy. This has not been claimed by even United States. On the issue of accidental and unauthorized nuclear launch, there is sense of concern in strategic circles. Todd Sechser, a research analyst at the Centre for Strategic and International Studies, has been for long urging the US government to face the reality of nuclear proliferation. He has recommended that the US "should declassify basic nuclear safety technologies and permit the sale of electronic locks and early warning systems to nascent nuclear powers such as India and Pakistan".

[19] http://www.nti.org/about/cyber/?subject=cyber

Is the Terror Nuclear Threat to India Real?

Recently a shocking revelation was made by the dreaded Indian Mujahaiddeen co- founder Yasin Bhatkal during his interrogation by security agencies that he sought to explode nuclear bomb in Surat. Bhatkal had even asked his Pakistan-based boss, Riyaz Bhatkal, over phone whether he could arrange a small "nuclear bomb" to which Riyaz responded, "Anything can be arranged in Pakistan."[20] This revelation has brought in focus two issues. **First**, problem of nuclear terrorism is real; **secondly**, it raises a question mark on the safety of Pakistan nuclear arsenal whose safety Pakistan government repeatedly has affirmed.

There is a growing concern for nuclear terrorism in India. India's nuclear security discourse has significantly undergone change in a global debate after Sep 9/11 attack which highlights that the terror network would not hesitate from launching major attacks. The evolving strategic ties between the United States and India could lead us to situation of being targeted by Al Qaeda/ISIS which considers United States and its allies as primary foes. India's apprehension about nuclear terrorism also stems from the prevailing instability in Pakistan which in its several parts also provides the safe haven to the terrorist's.

Over the years, Pakistan's poor proliferation record and its strategic nuclear programme has been portrayed a major concern by the international community. The history of Dr. Abdul Qadir Khan alleged complicity in illegal transfers of highly sensitive materiel for nuclear weapon programs in Iran, Libya, and North Korea between 1989 and 2003,[21] the internal instability in Pakistan and the fact that it also houses several active terror groups such as Tehrik-i Taliban Pakistan(TTP) , Lashkar-e- Taiba (LeT) etc, all point at the susceptibility of Pakistan to become nuclear terror safe haven. A 2010 study by the Congressional Research Service titled 'Pakistan's Nuclear Weapons: Proliferation and Security Issues' noted that even though Pakistan had taken several steps to enhance nuclear security

[20] http://www.saharasamay.com/nation-news/676545252/yasin-bhatkal-planned-nuclear-attack-in-surat-alarm-bells-for-in.html

[21] Paper of WMDC at http://www.un.org/disarmament/education/wmdcommission/files/No2.pdf

in recent years, “instability in Pakistan has called the extent and durability of these reforms into question”.[22] The acquisition of fissile material or crude RDD by terror elements is possible . This possibility has even been admitted by Lt General (Retd) Talat Massod in an article in Tribune on 24 March 2014, “that potential terrorists groups seizing nuclear material or weapons has increased since September 11 , 2011 attacks in United States”. He further says that, “acquisition of nuclear weapons or material through clandestine means cannot be ruled out. This could happen by accessing of radiating materials through some misguided scientists or through theft”. “The presence of terror safe havens in tribal belt and omnipresent threat of terrorism in Pakistan remains a source of serious concern for the international community despite repeated assurances made by our government officials and scientists of the safety of our nuclear material and weapons”.[23]

Protection Against Unauthorized Use of Nuclear Materials .

In India, the Cabinet Committee on Security (CCS) has cleared a project of Rs. 285 corers of the Ministry of Defence for developing systems and equipments for protection against Nuclear, Biological and Chemical (NBC) weapons. Under the project, DRDO has been tasked to develop quick and fast detection systems in case of an NBC attack on our vital installations and cities or leakage in any installation dealing with these materials. BARC has hi-tech Ariel Gamma Spectrometry System (AGSS) which is capable of swift and effective assessment by aerial surveys, it also periodically monitors major cities and Emergency Planning Zones (EPZs) of nuclear power plants to generate baseline dose arte data. In addition to these, Compact Aerial Radiation Monitoring System (CARMS) is also in use for remote aerial monitoring. There are 18 Emergency Response Centers are located across the country equipped with latest technology to respond to a situation at short notice. Indian government is taking further steps to develop Nuclear Forensics within the country. As per a plan, a Nuclear Forensics would be built

[22] The international commission on Nuclear Non-proliferation and Disarmament observes,” It is now known that Al Qaeda some years ago attempted to obtain enriched uranium, and that senior members of the group had at least one meeting with two Pakistani nuclear experts”

[23] http://tribune.com.pk/story/687141/nucler-security-a-global-challenge/

in Karnataka by 2018/2019.We also need to establish archive of nuclear and radiological samples and closely coordinate with other nuclear states for keeping track of nuclear material and technology as well as facilitate inter-laboratory forensics exercises worldwide as nuclear forensics and other processes alone can serve as useful tool for unauthorized nuclear proliferation.

A Way Forward.

The NTI study[24] has shown that we need to model our nuclear security at the national level giving due importance to both Physical and system aspects if we are to avoid the Stuxnet[25] type of attacks. The study had focused on protection measures at the civil nuclear facilities but, these have much greater relevance for the military nuclear sites. The study recommends a holistic approach which begins at the facility level and widens to the national level. At facility level, it explains the relevance of physical barriers, security system, approved procedures, Intrusion detection systems, good operating and maintenance practices, training and qualification; and Quality assurance programme. At the national level, there is a requirement of licensing process, regulatory frame work and specific legislation.

Countries in the sample (China, Russia, Germany, South Africa and United States) of the NTI study while generally conformed to the requirements but, their laws and regulatory authorities mostly dealt with generic issues and lacked specific provisions to deal with cyber security aspects or partially dealt with these. The reasons for this was that legislation and regulatory provisions were drafted much before the cyber security threat has emerged hence, did not address the issues of cyber threat to the nuclear installations. All suggested measures seem to be in place in India too. We have enacted legislation[26] and regulatory authority to deal with the issues but, similar issues need to be addressed in India too. The cyber security policy 2013[27] has been issued, it sets an aim to have trained work

[24] http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL.pdf?_=1445548675

[25] As per unconfirmed report Stuxnet is a malicious computer worm whichtargeted the Iranian enrichment nuclear facilities in 2011.

[26] Atomic Energy Act 1962 and its amendments of 1986 and 1987.

[27] National Cyber Security Policy -2013accessed at http://deity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf

force of 50000 professionals under a national nodal agency in next five years but, the policy is generic and meant to deal with a cyber-attack in any government and non-government entities and makes no reference to nuclear cyber security.

Following a standard generic approach the nuclear facilities cannot be expected to be protected from the cyber-attack because the potential consequences of a failure are not just financial, they could be physical. The current approach depends on an adhoc collection of tools that attempt to detect and block the cyber-attacks. These tools fail when new attacks are created, and new attacks are being created at an increasingly fast pace. As a result, nuclear facilities will remain at the mercy of attackers and new attacks that bypass even the most up-to-date attack-centric defenses. Attacks may help the terrorists acquire weapons-usable nuclear or a radiological material which is potentially dangerous.

In reality, when you attempt to respond to a cyber attack to the nuclear computer, you are already losing the battle. George Chamales who was sponsored by NTI for a study concludes in his report that the current, attack-centric approach to computer security is incapable of adequately protecting the systems. He accordingly recommends "adopting a new approach, vulnerability centric security, which enables nuclear facility operators to prevent successful cyber attacks while enhancing the day-to-day operation of their systems"[28]. The protection of nuclear computers would need to be in place based on the vulnerability and not in response to the attack. The approach is based on the premise that basic functional systems would suffice and unnecessarily packing several functions makes the computer based system vulnerable.

With these developments in the field, it is incumbent to establish a specific system and process in place for robust nuclear computer security, in place of current common approach. The details of the system would need to be worked by the experts in the field.

[28] A Paper titled " A new approach to nuclear computer Security " by George Chamlesaccessed at http://www.nti.org/analysis/reports/new-approach-nuclear-computer-security/

In conclusion it is opined that secure line communication, encryption of transmissions and coded commands etc can provide some answers but, these can never be assumed fool proof. The combination of the technological fireballs and dual/multiple human confirmations alone can provide some protection.