Check against delivery

Technology and National Security

(Technology Day, BAARC, 11 May 2012)

Chairman AEC, Dr. R.K. Sinha,
Distinguished scientists,
Ladies and Gentlemen.

Thank you for asking me to speak at the National Technology Day celebrations in BAARC today. This is indeed an honour and a responsibility, for two reasons. One is the responsibility of speaking to an audience of elite scientists and engineers who are among the best in India and the world in their respective fields. The other is the importance of the occasion that we are marking when we celebrate National Technology Day on May 11.

There are two days in May that every Indian of my generation remembers. They are 18 May 1974 and 11 May 1998. Each one of us can recall where he was when he first heard of Pokhran I and of Operation Shakti, and of the pride and joy of that moment. We, as a nation have good reason to proudly mark those achievements of our scientists and indigenous science. The years have borne out the wisdom of the technology and political choices that India made in the early years after independence, which led to the successful tests of 1974 and 1998. For the choices made then have contributed to our national security in several ways.

Today as we mark your contributions as scientists to our national security, I would like to discuss the broader issue of the contributions that technology makes, and the challenges that it throws up, for our national security.

Definitions

We each tend to define national security in terms of our own experience. Today we use the word security loosely. We speak of energy security, food security and even of human security. In other words, security is what we seek in every aspect of our lives in a world full of risk. Our definition of security has grown through history. Today we speak of soft and hard power and use the language of security to describe even corporate dealings! But one thing has been common throughout history. Technology and its changes have consistently been one of the major drivers of the security calculus.

Jawaharlal Nehru and Homi Bhabha were among the earliest Indians to recognise this fact. They also recognised relatively early that in the atomic age, which had just dawned, technology had become critical to India's security. This is why, despite widespread scepticism in India and abroad, they set about ensuring that we mastered and indigenised the most advanced technologies then known to man. They realised that if our goal is to transform India, eliminating mass poverty and enabling every Indian to realise his (or her) potential, we must rely on science and technology not only for the economic basis for prosperity but for the strength that secure the peace we need to develop and protect India.

What they sought was not autarky but self-reliance, and the mastery of science and technology and innovation that would lead to true self-reliance. In that quest they were ready to cooperate with the rest of the world and to make our knowledge and facilities available to the rest of the world. The effort, investment and encouragement that the early generation put into India's quest for scientific self-reliance was unique among developing countries at that stage of development. In practice I am afraid that our successes may have been short of their dreams, but there is no question that they have been greater and in many more fields than expected by sceptics in India and abroad.

Consider some of the contributions that technology makes to our national security.

Contributions

It is today hard to think of a single aspect of national security that is not influenced by technology.

What the atomic energy programme did for our nation's security is evident. Our strategic programme and nuclear weapons make us more secure than before, deterring those who may wish us harm. In addition, the atomic energy programme was the crucible in which much of our scientific and technical talent was nurtured. It is remarkable how many of those whom the country depends upon in other fields of scientific endeavour are drawn from the atomic energy fraternity. This is true in metallurgy, the early our space and missile programmes, and several other fields. Much of what we depend upon for our intelligence, surveillance, and communications comes from technologies that we had to master ourselves. (At the same time we must remember that May 18, 1974 and May 11, 1998 surprised the greatest powers of the world despite all the technological sophistication of their intelligence gathering.)

Using a broader definition of security, technology is what has made it possible for us to progress. Food security has come in the past from the application of modern technology to our agriculture in the Green Revolution, and it is a second Green Revolution that we will need if we are to achieve food security in the future. Our hope for energy security, given our poverty of fossil fuel resources, must lie in the creative application of technologies such as atomic energy to generate renewable energy. I do no need to tell this audience more about this aspect.

So no matter how one defines security, whether only in the hard terms of national defence and law and order, or in the broader sense of food, energy and human security, technology has already proved itself crucial and essential to our national security.

Challenges

But the very same technologies which enhance our security, also pose new challenges. Let us look at two aspects in a little more detail, namely, the effects of nuclear weapons and ICT on our national security.

Nuclear Weapons

The use of atomic weapons, with their unparalleled force and their after effects, prompted a revolution in military affairs and in strategic thinking which is still working itself out. For one it was soon apparent that there was a difference between those who still thought of them as war-fighting weapons, different only in degree and power from previous weapons, and those who did not. Nehru and Bhabha saw very soon that these were primarily political weapons. The elaborate war-fighting doctrines developed by some did not fool them. Today the world still faces the issue of whether these are political or war-fighting weapons.

When India carried out nuclear weapons tests in May 1998, twenty-four years after first displaying the capability to do so in May1974, she also became the first nuclear weapon state to publicly announce and debate a nuclear doctrine rapidly thereafter. That we were able to do so was thanks to the preparatory thinking and work of a remarkable handful of people who had thought this through beforehand.

I will not repeat the doctrine as you no doubt are already familiar with it. Instead I will only highlight a few of its main features. For India nuclear weapons were not meant as a war-fighting weapon, to compensate for a perceived inferiority in conventional or other spheres, (as is the case for Pakistan and North Korea).

For India, from the start the purpose of nuclear weapons was to deter nuclear attack and to prevent the sort of nuclear coercion or threat that we had faced in the seventies and eighties. It was therefore logical for the doctrine to promise “no-first-use” against others, and to threaten assured and massive retaliation if attacked with nuclear weapons. In other words, it assumed a secure second-strike capability for deterrence through assured retaliation. In order to assure retaliation, the force had to be reliable and have survivability.

The no-first-use and assured retaliation concepts naturally had significant direct implications for our nuclear strategy and posture:

- for one it became essential that we develop a genuine delivery triad as soon as possible, not only to ensure survivability of our second strike capability but to assure retaliation.
- Matching the number of warheads and missiles that our adversaries have became less important than the reliability and survivability of

our own weapons. (This is relevant today when, by all accounts Pakistan is building two new Plutonium producing reactors and a large reprocessing plant and is increasing the rate of manufacture of nuclear warheads.) While first-use equals aggression, no-first-use equals deterrence. And deterrence requires the minimum number of weapons to make the threat of retaliation credible --- in other words, credible minimum deterrence. We can thus escape an expensive arms race in nuclear weapons while safeguarding our security.

- As these are weapons of deterrence rather than war-fighting weapons, it is crucial that our adversaries believed that they would be used if certain thresholds were crossed.
- [For the same reason, calibrated deterrence was ruled out. Instead counter value targeting, rather than counter-force targeting was the logical posture. It is for this reason that our nuclear armed Prithvis with their limited range are effective deterrents, since the only real targets for them are the cities of the Pakistani Punjab.]
- If you rule out first use of nuclear weapons, you need to possess other means to deal with non-nuclear threats and challenges.

Interestingly, as expressed, our doctrine is closest to China's declared doctrine. Like us China had declared a (somewhat more hedged) no-first-use policy. After toying in the late eighties with a shift to tactical nuclear weapons, she reversed that decision in the mid-nineties. For a very long period, since 1964, she has accepted a huge asymmetry in the numbers of her nuclear weapons compared to those of her main potential adversaries the USA and the Soviet Union/Russia. She concentrated instead on the survivability of her arsenal to assure retaliation. China has so far not made a direct nuclear threat against India, as one would expect from a country that does not regard its nuclear arsenal as a war-fighting weapon. In recent years China has concentrated on technical improvements in her nuclear arsenal (such as MIRVing and MARVing her warheads) and in producing nuclear class missiles in vast numbers and equipping them with PGMs as well, so as to confuse the adversary and maximise strategic deception.

On the other hand, there is a clear difference between our doctrine and Pakistan's. In the red lines that Lt.-Gen Naqvi made known, for instance, Pakistan clearly wants us to believe that she will employ her nuclear weapons for tactical uses if certain thresholds are crossed. During her Azm-i-Nau exercises in 2010 she signalled to us that she was preparing to use nuclear weapons against Indian forces if they were on Pakistani territory, (a counter to what they think “Cold Start” means).

Our Experience

I would draw three lessons from our experience as a nuclear weapon state so far.

Firstly, the decision to go overtly nuclear in 1998 has been vindicated by our experience since then. These weapons were meant to prevent nuclear coercion and blackmail. They have done so. The only direct threat since 1998 was by Pakistan in May 2002, during Operation Parakram when they were convinced that India was on the verge of launching military action against them. As it was not our intent to do so, the threat was meaningless and did not affect our behaviour. Not having been deterred by nuclear threats in 1971, 1987 or 1990 from following our course when we were in a much weaker position, our overt nuclear weapons status makes us much less vulnerable to them today.

Secondly, India-China deterrence is stable and is likely to remain so despite its reaching equilibrium at progressively higher technological levels as both strategic programmes develop increasing sophistication.

However, there are issues about India-Pakistan deterrence post-1998, and particularly after operation Parakram, that merit continuing examination and that we need to think through. Pakistan has consistently sought to use nuclear deterrence to permit her to undertake adventurist actions against India, in J&K or elsewhere. Her Kargil misadventure in 1999 was an attempt to use the threat of nuclear escalation to prevent an Indian escalation in response to her conventional attempt to seize and hold territory in J&K. The attempt backfired, leading the world and US to intervene to push Pakistan to withdraw her troops. However, that it resulted in military and diplomatic failure for Pakistan is not widely understood in the Pakistan Army. In fact the Pakistan Army seems to have drawn the lesson that India’s decision to respect the LOC, (born out of a desire to legitimise the LOC), was a result of Pakistan's nuclear deterrence working to prevent an Indian riposte elsewhere or an escalation to full-scale conventional hostilities, thus limiting the conflict to Pakistan's advantage.

If the lessons learnt by the Pakistan Army from Kargil were mixed, their practice since Parakram suggests that they may have unfortunately drawn a more dangerous conclusion still. The Pakistan Army seems to believe that Pakistan's nuclear shield permits her to undertake terrorist attacks on India without fear of retaliation. This may well have been the Pakistan Army calculation behind the Mumbai attack of 26 November 2008. The Pakistan Army believes that their Brasstacks and 1990 nuclear threats worked and prevented Indian retaliation and action then, as after the Mumbai attack.

What then is the answer to this Pakistani belief in their immunity from retaliation against terrorism and other asymmetric attacks against India thanks to their nuclear deterrent? One response would be to revise our nuclear doctrine and strategy to a war-fighting one, developing tactical nuclear weapons and threatening to use them. But this is hardly credible. To threaten that a terrorist attack from Pakistan on India would be answered by the use of nuclear weapons would be like killing a mosquito with a shotgun and is unlikely to be understood by our own people let alone the international community.

The answer to asymmetric threats must therefore lie in a strategy of flexible response, outside the nuclear end of the spectrum of conflict. In Pakistan's particular case this would require a deliberate strategy of containment which raises the costs of terrorism as a state policy to Pakistan on a long term basis. There are several responses short of war available to a state like India.

It seems to me that rather than seeking answers in our nuclear weapons to all the threats that we do or may face, it is important that we maintain the fundamentals of our doctrine, treating our nuclear weapons as political instruments which deter nuclear attack and attempts at nuclear coercion.

As for non-nuclear threats, there are other ways of dealing with them which should not be beyond our ingenuity and capability to find.

There are of course several other issues related to our nuclear strategy that merit examination. Among them are: the effects on deterrence of the ballistic missile defences that both Pakistan and China are seeking to build; the risks from unauthorised use of nuclear weapons or their falling into terrorist hands as the Pakistani state withers away; command, control and custody issues when nuclear weapons are treated as war-fighting weapons as Pakistan does; and nuclear and missile proliferation in our neighbourhood as in Iran and North Korea, for instance. Each of these affects our security directly and will require analysis and responses in our nuclear strategy. If we can do what we have done so far, which is to think for ourselves and devise our own doctrines and solutions to problems, developing a nuclear strategy that is uniquely Indian, I am sure that we will be successful in dealing with these questions as well.

ICT

The other technological change that has made an enormous difference to the way in which we look at and deal with our security is the ICT revolution. It has created a new domain of contention, namely cyber space, where war, espionage, surveillance, control and all the traditional security functions, activities and crimes take place.

The effects of ICT on warfare are evident in the new methods of command and control, in the new surveillance and communication technologies and in cyber operations which have kinetic effects in the real world. We have seen a new way of warfare, a true RMA, since the early 90s, enabled by ICT. Equally intelligence and espionage increasingly rely on what are euphemistically called national technical means, namely cyber penetration and surveillance.

Compared to the nuclear revolution the ICT revolution has had four contrasting effects.

- It has brought power to non-state actors and individuals, to small groups such as terrorists. It has given small groups and individuals the means to threaten and act against much larger, more complex and powerful groups. Since the technology is now available or accessible widely, and is mostly held in private hands, (unlike nuclear technology), ICT has redistributed power within states.

- It has created a whole new domain of contention which did not exist until recently, cyber-space. And here we have to unlearn some of the lessons we learnt from the nuclear revolution. Traditional deterrence hardly works in a battle-space like the cyber world when the speed of operations and attack is almost that of light. At these speeds there is a premium on attacking first, or offense.
- In existing or conventional domains like maritime security and outer space ICT has changed the nature of contention. For instance ICTs are used in traditional domains like the sea by modern day pirates to change the balance in their favour. The use of GPS navigation, communication interception technology and the lethality of modern firepower have helped the resurgence of this old menace off the Horn of Africa.
- If nuclear weapons hardened and entrenched the balance of power between states, ICT changed the national security power calculus between states. After several centuries, once again the state is not the sole or always the predominant factor in the international system. In some cases, it is businesses and individuals who now determine our technological future and it is these units that a successful policy must now increasingly deal with.

We see the practical effects of these changes all around us. Look at the social and political effects of the new technologies in the turmoil in West Asia. The cocktail of social media, 24 hour television, NGOs and Special Forces create a virtual reality which soon has effects in the real world. These are not just law and order problems, and they are not amenable to the traditional responses that states are accustomed to. We have seen technology place increasingly lethal power in the hands of non-state actors. The effects can range from the benign to the dangerous, though the technology itself is value neutral. In West Asia today we see its use by popular movements to mobilise people and influence opinion against regimes across the Arab world. Autocratic regimes across the world now take the power of ICT very seriously.

Equally, terrorism is technologically enabled and knows no boundaries today, even drawing on support from within state systems. Within states, the lethality of terrorism and insurgencies, and the strength, reach and lethality of groups like Al Qaeda and LeT are directly linked to their empowerment by these technologies. We felt the effects directly in Mumbai when the terrorists used VOIP communications with their handlers. These technologies have eliminated the State's monopoly of violence. Today the internet provides jehadi and other terrorists, separatists and LWE with an effective means of recruitment, propaganda and communication. There is a risk that we are ceding this space to our enemies, and as a consequence, may also be losing the battle for the minds of the young who depend increasingly on the internet for their information and opinions.

The same technologies also empower the state in terms of its capacity for internal surveillance, interception and so on. But their power and reach raise fundamental issues about the lines that a democratic society must draw between the collective right to security and the individual's right to privacy. What makes it more complicated is the fact that these technologies are not just available to the state, where laws and policies can control and limit their use. They are widely available in the public domain, where commercial and individual motives can easily lead to misuse that is not so easily regulated unless we rethink and update our legal and other approaches.

Between states, technology has expanded the spectrum, the line between conventional and non-conventional warfare has blurred. The definition of force, the classic marker of power, has now expanded, thus changing the utility of force as traditionally configured.

Information technologies and their effects have made asymmetric strategies much more effective and attractive. In situations of conventional imbalance between states, (like China and the USA), we see that asymmetric strategies are increasingly common. For instance, developing a ballistic anti-ship cruise missile against carrier fleets, building a very large missile force and a fleet of SSBNs and SSNs, and developing and displaying cyber war and anti-satellite capabilities, are uses of technology by a weaker state to neutralise or raise the cost and deter the use of its military strength by a stronger country.

All the major powers are developing offensive cyber capabilities as well as using cyber espionage. So are smaller powers who see ICT as an equaliser. One estimate speaks of about 120 countries developing the capacity for cyber warfare. But by its nature, as Wikileaks showed, the threats in this domain are not just from states. These technologies have also enabled individuals and small groups to use cyber space for their own ends. We in India are subject to unwelcome attention from many of them.

Government are in the process of putting in place the capabilities and the systems in India that will enable us to deal with this anarchic new world of constant and undeclared cyber threat, attack, counter-attack and defence. We need to prepare to deal with both risks to cyber space and risks arising through cyber space. While NTRO is tasked to deal with the protection of our critical security cyber infrastructure, institutions like CERT-IN have proved their worth during events like the Commonwealth Games in defending our open civil systems. We are making a beginning in putting in place a system of certification and responsibility for telecommunication equipment and are working on procedures and protocols which will rationalise communication interception and monitoring. We need also to create a climate and environment within which security is built into our cyber and communications working methods. This clearly has to be more than just a whole-of-government effort. It must include the entire scientific and technological strength of the country, whether in the labs, universities of private sector firms.

While these are practical responses to immediate phenomena, it is in science that we must seek long-term and lasting answers to these security issues and to the forms that they may take in the future. For India to pursue access to and mastery of the science behind these technologies therefore becomes crucial to our future and to our ability to provide the security that India’s continued growth requires.

Ironically, while the new ICT technology has led to a diffusion of political and military power, technology itself is increasingly generated, produced, and owned by an ever smaller number of countries and corporations, even while its products are manufactured in more and more locations around the world. The balance between defence and civilian technology has also shifted. In the past, most technological innovation (like radar and the internet) originated in the defence sector. Today communications and other technologies that are changing military affairs are largely products of the civilian sector.

Technology Security

There is a great deal for us in India to do as a result of these changes.
There is the immediate task of harnessing the fruits of science to the nation's security. By this I do not only mean building the nuclear weapons and other products of science that we possess and need for our security.
It also means setting up structures and institutions which enable us to use the new technologies and to answer the new threats they pose. The same ICT that empowers small groups is also available to and should be used by the state for intelligence, surveillance and counter-terrorism. It is for the state to show the same quickness in learning that its enemies have shown in the recent past.

We must also start to think of technology security as a national goal. I do not mean by this that we must aim for autonomy or complete indigenisation of every technology that could affect our future. But we must be able to guarantee and secure our own critical systems, and to generate enough of our own technology to do so. And we must do so seamlessly between civil and defence technologies, bridging this divide which has become so entrenched in the last fifty years.

We must do this work ourselves for the simple reason that access to high technology is controlled and limited by the holders under several intellectual property and technology denial and control regimes. Our experience of resuming civil nuclear cooperation with the rest of the world in 2005-8 shows that it is when you have shown the ability and will to go it alone and master technologies yourself that the world is ready to work with you.

Which technologies should we be concentrating on for the future? While certain strategically significant sectors pick themselves, betting on individual technologies is a gamble that is probably best left to scientists and individual entrepreneurs not the state. But it is essential in a technologically driven world that India makes the transition from being purely a consumer of others' technological products to becoming a producer and generator of technological innovation in critical areas. This requires the state to provide the necessary environment and incentives, tying defence acquisitions and R&D to that in the civilian sector. Today we are not even a manufacturer in several critical technological sectors. A few emerging economies have started making that transition, namely Brazil and China.

Our space and nuclear programmes prove that we have the capability to absorb and to develop our own technologies when government is supportive. But we are yet to show the same capacity or policy will in telecommunications, civil aviation and aerospace and other technologies of the future. In telecom, we are actually further behind today in terms of generating or owning our own technology than we were twenty years ago. Where we have made progress, in biotechnology and chip design, for instance, it has been thanks to some of our scientists, technologists and entrepreneurs.

India has two great advantages and an international moment that make it possible to aim at a much higher level of technology security. As our recent experience of the telecom sector shows, when we leverage access to our large domestic market, we can set rules and conditions that enable India to develop the required expertise and capabilities. Secondly, we do have people who are qualified to build our capacity, both in India and in our diaspora abroad. And in a situation where defence is increasingly dependent on the civilian sector to generate innovation, and export control regimes in major technology powers are being adjusted in our favour, we have a favourable concatenation of circumstances that we should be able to use to build the technological capacities that we need.

I would also regard the emergence of new domains of contention, cyberspace, outer space and the awareness of the global commons, as an opportunity for a country like India to leapfrog stages and to prepare for the future rather than the past.

National security in its broadest definition is and will be determined by our scientific prowess. By this I mean questions of energy security, food security, and access to critical raw materials, strategic materials and technologies, all of which would affect our quest to transform and develop India. Unfortunately we are not a natural resource rich country. In our quest to ensure the factors necessary for our own growth we therefore have no choice but to seek answers in our own science and technology if we are not to be totally dependent upon external solutions to several constraints on our development.

Unfortunately, the daily rush of business means that these issues do not always receive the sort of attention in our strategic calculus that their impact on India's medium and longer term future merits. We tend to leave these issues to the cognoscenti and the specialist. Yet the answers to many of these problems can only be found in science. This is true of water scarcity in a planet where 80% of the surface consists of water and where it is the energy cost and technology of desalination that are the constraint. It is true of food security where Malthusian predictions have so far been averted by scientific discoveries. It is also true of energy security where India is best placed and most in need of finding competitive and practical ways of using nuclear, solar and other renewable energy sources. These are all questions of India's future survival and security. Here again we must look to science and its practical applications in India for the answers.

Lessons

I think it is clear from this brief survey that our national security requires that we stay abreast of critical technologies if we are to be secure. This is what makes your work here in BAARC so important to the nation. Technology today is closely held though widely used. It is also a sad fact that the Lord seems to give to those who have. Our experience of civil nuclear cooperation with the rest of the world shows that. Once it became clear that we had mastered all the technologies of the entire nuclear fuel cycle, and, incidentally, also shown mastery of nuclear weapons technology, the world agreed to lift the sanctions and restrictions that our nuclear programme had been subject to from 1974 onwards. Strong indigenous capabilities of our own are an essential precondition for successful cooperation with the rest of the world in these sensitive technologies.

Equally, this is an area where our challenges are also our opportunities.

The challenge is to bring to bear all our national capabilities in a coordinated effort in these technological fields so as to enhance our security, as we did and continue to do in our strategic programme.

Conclusion

Today, as we mark our scientists' contribution to our nation's security, we are standing on the shoulders of those who came before us, those who conceived and built BAARC and our other institutions of scientific and technological excellence. I am sure that in years to come you will make even greater contributions to our national security.

-------xxx-------