Check against delivery

Reading copy

Cyber Security

(IDSA, 16 May 2012)

S.Menon

Dr. Arvind Gupta, DG IDSA,
Shri Nitin Desai, Chairman of the Task Force,
Members of the Task Force,
Ladies and Gentlemen,
Friends.

I am delighted to speak at the release of the IDSA Task Force report on India's Cyber Security Challenge. The wealth of experience and expertise in the task force is impressive, as is the quality of the report that you have produced on a subject that should be of wide interest. I, therefore, wish to thank the IDSA and the Task Force members for this very useful initiative.

The report is also topical, coming as it does when Government is in the final stages of preparing a whole-of-Government cyber security architecture. There is also considerable and increasing concern in the strategic community and the general public about cyber security. Your report is therefore well timed.

Our increasing dependence on cyber space and the internet is evident. We had over 100 million internet users in India over two years ago. Add to this the 381 million mobile phone subscriptions with internet connectivity and the increasing seamlessness with which all sorts of devices connect to the internet. There are well over 2 billion internet users in the world -- a number that doubled in the five years between 2005 and 2010. These numbers are growing exponentially and give one some idea of the increasing reach of the internet and our growing dependence upon cyber space. Most of us in one way or other use and depend on cyber space in the performance of our work and in our daily lives.

Public concern about cyber security is rising, partly because of the weight of anecdotal evidence that is building up about cyber war and attacks. Stuxnet and Ghostnet, for instance, appear to most citizens as unseen forces having apparently magical effects in the real world. It is also fear of the unknown, because most persons lack a conceptual framework or understanding that would enable them to deal with the issue. The Task Force Report is therefore welcome as a significant contribution to increasing understanding of the issue of cyber security and of what we should be worrying about in this field.

The other reason for public concern and anxiety is the anarchic nature of the domain of cyber space, glimpses of which naturally cause alarm. When this is combined with the potential effects of malicious attacks and disruptions in the cyber world upon such basic social necessities as power supplies, banking, railways, air traffic control, etc. it is only natural that people should worry about cyber security.

Nor do experts help to allay concerns in their choice of terms to describe these phenomena. We speak of cyber crime, when these acts are not a traditional law and order problem. Nor can they be dealt with as such, thanks to problems of attribution, lack of legal frameworks and without enforcement capabilities and punishment.

We also speak of cyber war, even though conflict or attacks in the cyber world do not follow the rules or logic of war as understood so far in other domains. In this new domain of contention war, espionage, surveillance, control and the traditional security functions, activities and crimes occur but differ from those in traditional domains. Here we have to unlearn some of the lessons we learnt earlier. Traditional deterrence hardly works in a battle-space like the cyber world where operations and attack occur almost at the speed of light. At these speeds there is a premium on attacking first, or offense.

The effect of ICT on warfare is evident in 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.

The ICT revolution has also 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, ICT has redistributed power within states.

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, intelligence and espionage increasingly rely on what are euphemistically called national technical means, namely cyber penetration and surveillance. The same technologies also empower the state in terms of its capacity for internal surveillance, interception and so on. 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 this 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, information technologies and their effects have made asymmetric strategies much more effective and attractive. In situations of conventional imbalance between states we see that asymmetric strategies are increasingly common. 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.

In the name of defence 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, state and non-state.

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 threats to cyber space and risks arising through cyber space. This will be a step towards the "coherent and comprehensive cyber security policy" that the Task Force Report rightly calls for on page 25. 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 to harden our critical networks. And we will develop metrics to certify and assure that our critical cyber networks, equipment and infrastructure are secure. We also need to create a climate and environment within which security is built into our cyber and communications working methods. And, most important, we must find ways to indigenously generate the manpower, technologies + equipment that we require for our cyber security.

As your report rightly points out, 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 laboratories, universities or in our private sector firms.

I therefore welcome the main recommendations of the Task Force as a useful contribution to the evolution of national cyber security policy. There is only one part of the Task Force's recommendations with which I personally have a difference of emphasis. It speaks about "proactive diplomatic policy" on cyber security, and suggests that multilateral efforts for international internet governance are useful. The Report itself recognizes that most proposals for international internet governance are thinly masked efforts to control or shape the internet, and that some are ideologically driven. Inter-governmental rules of the road are certainly desirable. No one can argue against them. But in my personal view we must be clear that they will not have practical effect or be followed unless they are in the clear self-interest of those who should be following them. Let us therefore concentrate on putting our own house in order. That should be our first priority

One final point. I do hope that the Task Force Report will also bring some reason and proportion into our discussion of cyber security.

To cite one example, there is invariably a big hullabaloo when one of our websites is hacked. But websites are meant to be hit. Their success is measured by how many people access or hit them. So when a website is defaced by hackers, as happened to the CBI website, it is not necessarily a security breach, though it might hurt one's pride. It seems to me that available resources would be better used to defend and harden our critical cyber infrastructure, expanding what is secure, from the known to the unknown. The Task Force report suggestions on how we could do so are very useful.

I therefore have no hesitation in commending the central messages in the report to those interested in cyber security in India as we work together to strengthen India's cyber defences.