Institute for Defence Studies and Analyses

INSTITUTE FOR DEFENCE STUDIES & ANALYSES

Edited Transcript of IDSA Cyber Security Report Release & Panel Discussion

16 May 2012

Contents

Release Function

Panel Discussion on "India's Cyber Security Challenge"

Welcome Address by DG, IDSA

The Report is the outcome of a Task Force set up at the IDSA to explore the diverse dimensions of cyber security challenge that India is facing. The Task Force was headed by Shri Nitin Desai, former Member of the NSAB, and comprised of Lt Gen (retd.) Aditya Singh, former Member of the NSAB; Dr. Kamlesh Bajaj, CEO, Data Security Council of India; Shri B J Srinath, CERT-IN; Shri Salman Waris, a Lawyer in a Delhi based law firm; Shri Amit Sharma, DRDO; Dr. Ajey Lele, IDSA; Dr Cherian Samuel, IDSA and Shri Kapil Patil, Indian Pugwash Society.

The report, written in a non-technical style, is aimed at raising awareness about the dynamic nature of cyberspace and cyber security challenges that India is facing. In analyzing the various dimensions of cyber security challenge to India, the Task Force argues that India must foresee and plan for various challenges arising out of the growth of internet and digitalization of governance. Failure to do so can be catastrophic and could affect national security, Indian economy and social stability. India is particularly vulnerable to the threats from cyber crime, cyber terrorism, cyber espionage and cyber warfare. India's critical infrastructure is also vulnerable.

The threat of cyber warfare, discussed in the Task Force Report at length is looming large even though as yet there is no agreed definition of cyber warfare. The attacks on the websites of Estonia in 2007 and of Georgia in 2008 are chilling reminders of the potential of cyber warfare. It has recently been reported that the US considered cyber attack on Libya last year but deliberately gave up the idea as this would have escalated warfare in cyber space.

The report argues that it is a matter of time before cyberspace becomes an Independent theatre of war. The US has begun to regard cyber space as the fifth domain of warfare. It has set up a cyber command. The cyber doctrine says US reserves the right to respond in an appropriate manner, if attacked in cyberspace. Many countries are responding by setting up similar structures. Several countries are doing R&D on cyber weapons raising concerns regarding weaponisation of cyberspace.

The prospect of cyber warfare has invoked discussions on the application of the laws of armed conflict and use of force in cyber space. These are however grey areas with little clarity. Discussions as to what constitutes conflict in cyber space are still inconclusive. Meanwhile**, a**t the various international fora, demands have been raised to chalk out a code of conduct of dos and don'ts for state behavior in cyberspace. Russia has come up with a draft convention on information security, which incorporates many of the concerns regarding the use of cyber space for destructive activities as well for de-stabilizing regimes and society. A group of academicians and experts at MIT is examining how cyberspace will affect the international relations.

The convergence of multiple technologies with the internet and mushrooming of social networking sites has added an altogether new dimension to discussions on cyber security. Internet has empowered billions of people across ideological divides. They use the web and social networking sites every day. Monitoring cyberspace raises the issue of freedom of expression. Moreover, it is impossible to carry out surveillance of all that happens in cyberspace. Many analysts believe that internet played a critical role in heralding and spreading the Arab Spring. Even in the developed countries, curbs are being contemplated on social networking sites. The rapid advancement in technologies has led to new forms of threats which need to be understood and tackled.

In analyzing the various dimensions of cyber security challenge to India, the Task Force argues that India must foresee and plan for various challenges arising out of the growth of internet and digitalization of governance.

Access to internet is growing rapidly in India. E-governance has contributed to national well being. But cyber security best practices require to be incorporated in the governance architecture we are building. The report discusses at length the nature of cyber security challenge India is facing and makes recommendations as to how vulnerabilities in cyber space can be reduced. The report underlines the urgency of having a cyber security policy & institutional structures to address the emerging challenges. Protection of critical information infrastructure will require robust policies and sustained public private partnership as much of internet infrastructure is owned in the private sector. India will also have to ensure that there is coordination, cooperation and uniformity of legal measures internationally.

The recommendations made in the report are meant to initiate a debate on cyber security challenge, India is faced with.

Speaking from think tank perspective, India needs to step up its intellectual efforts and multidisciplinary R&D to figure out the implications of cyber security. The Task Force discusses some of these issues although much deeper analyses as required.

Introductory Remarks by Mr. Nitin Desai, Chairman, IDSA Cyber Security Task Force

The primary target of this report is the lay man, and I count myself as one. I got involved in this exercise after I left the United Nations in 2003. The then Secretary General Mr. Kofi Annan asked me to continue as his advisor on Internet Governance. For seven years, I chaired a group that had certain oversight functions over the way the internet is managed. During that time, it became increasingly clear to me that this is going to be a key area of global governance.

This report is less to do with internet governance and more focused on cyber security. For me, it was of the utmost importance that this should be a public report since this is a sphere that cannot be managed just by governments. When we say that cyberspace is emerging as an independent theatre of war, independent of the existing theatres of air, land, outer space, and water, the issue is not about the use of Information Technology in these traditional theatres of war; that in any case has to be protected by those that have been given responsibility of securing these domains, and they have to find ways of coping with new developments and advances in technologies.

The real issue is cyberspace as something which is independent of this and what we are talking of is not the physical space, the physical facilities such as the submarine cables, towers, exchange facilities, the defence of those is part of the responsibility of the traditional spheres of war. What we are talking about is the capacity through cyber attacks, of reducing, eroding, even eliminating the functionality of cyberspace. It can affect your banking system, air traffic control, power system, even government itself. The problem will become even more complex when we move from the exchange of information and knowledge to the internet of things, using the internet to control physically certain process. As is already happening, we have SCADA systems, we have the case of Stuxnet which attacked centrifuges, and even earlier episodes of pumpsets in gas pipelines being manipulated. etc. This will become more widespread as the use of internet for manipulating things increases. Preserving functionality is going to be the real challenge for cyber security and cyber defence . It cannot be done by using defence forces in the traditional way, but has to be done in partnership with others such as the banks, air traffic control. How do we do that? How do we make that kind of partnership to function effectively? This is going to be a major challenge. But this was done during the Commonwealth Games when different agencies along with the security agencies came together and functioned effectively.

> *"Preserving functionality is going to be the real challenge for cyber security and cyber defence"*

Another dimension to the problem is that when you say cyberspace is going to be a new theater of war, can you look at cyberspace as an entirely defensive operation? Can you defend your airspace and say you will do it as a purely defensive measure? Even if your goal is defence, any sensible security analyst will tell you that we need both passive and "positive" defence. Other countries are already doing it; the US has set up an independent Cyber command, the UK has its GCHQ, China has

a large presence, and they even see it as their area of strength in any future conflict. There are many things that will have to be done in the conventional security framework.

Our purpose in writing this report was to raise awareness, and to suggest the need for an open mind in how these security issues can be handled given the fact that they have to be addressed by government and private sector jointly. The scenario included in the study makes you realize that prevention cannot be done only by security forces in conventional sense but also by a proactive defence by the people who run those facilities. Let me end by saying this report is itself a partnership between people from different backgrounds and affiliations, it involved people from the NASSCOM side, from DRDO, and the data security side who have an interest in this issue.

Keynote Address by NSA

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.

The Task Force Report is 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.

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. ln 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.

ln 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 is 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.

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.

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. S0 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 lndia as we work together to strengthen India's cyber defences.

Q&A with the NSA

Q 1. My question not about the cyber security *per se* but more about the internet freedom…for past couple of years government is giving mixed signals about internet freedom and especially the statements made by Shri Kapil Sibal suggesting that some content should not be allowed on internet. So does the government have a coherent policy as far as internet freedom is concerned? India's stance on this issue has invited lot of criticism on this issue. Thank you.

A. I think we have a very simple policy. We are for it. But what content is objectionable, what is not and what do you about it, this is a social issue. Ultimately this is something which polity and society decide within itself. Now what Kapil Sibal was objecting to is some of the content which was put on the internet. Now that's one set of argument, what you do about that. If you find it objectionable, if you agree and if you have a proper way among yourself as a society, as a polity to decide its objection and what you do with it. We have no interest in controlling the internet. The fact that some content is objectionable, and might have consequences for a society, that is somehow converted into a debate on internet freedom which frankly is unrelated entirely. It doesn't matter what medium do you use, you would have the same argument if you use film, you use television or you use radio. But there is something about the anonymity of the internet which we have to admit among ourselves, which tends to relax the normal inhibition to what people say and do and maybe it's in the nature of the medium. But that as I said, it has nothing to do with government attitude to internet freedom. Certainly the simple answer is we are for it. But as a society as a polity, it is natural, we sit and wonder about where do we draw the line and how do we make it work among ourselves.

Q 2. What are your views on public private partnership as suggested by the report and how do you wish to address private sector's concerns on the cyber security?

A. Once we finalize the guidelines, we will start talking to DSCI, NASSCOM. We will start talking to them what kind of issues we are facing and hear from them what we can do together and see how we can carry this forward and we have scheduled it for the last week of June. It cannot be done entirely by the government. We must bring together all the elements of government and once we do that we then need to get all the society and all the technological resources that are available in the country, we need to apply. There is no question; private sector is a big part of that. There is lot of talent there in labs and universities and there are a lot of people who know about it. My own feeling is that, we in India have two great opportunities. We have what most countries don't have which is the human resource you need for this. Secondly we are secure because we not so extensively connected. We therefore have an opportunity to leapfrog. We can actually put in place and do things we need to. Trouble is that it is a moving target and it is going to keep moving. So we should never say, the solution is found. I think that's the wrong word. What we need is to have an architecture, which enables us to deal with cyber security as it grows, as it develops and to do what we need to do. That's the way I look at it and that will need working together and there is no other way of doing it.

Q 3. You mentioned that India was a target of many cyber attacks launched by non-state actors, could please share with us some of the details and what did you about it?

A. Well, the whole problem in this field is attribution. If you read the report it tells you. It is easy to suspect where it came from but it's a global internet and you really don't know who is attacking you and where it is actually coming from. Some of it comes in the open and some of it doesn't. The problem with the field is people don't share. Nobody wants to say what happened to them and how they were targeted. People suspect each other. If you look at international cooperation in this area, there is lot of talk about how we have do cyber security together. But when it comes to actual cooperation there isn't that much and its bit of a problem. So if you ask me if give me the details, you won't get much.

Q 4. Was there any major attack that was ever recorded publicly?

A. Take the example of "Common Wealth Games". We had over 8000 attacks what to me are crazy. These are ticketing networks, these are scoring, timing and other things and that's pure malice. I can't see any commercial advantage or any other. But it was staggering to see you had over 8000 attacks in the period of two and half weeks during the Common Wealth Games. That's just a tip of iceberg. There are important things in this country that are worth going after. And that's the problem.

Q 5. What is your take on ethical hacking and that too sponsored by the state?

A. I think it's hard to qualify when it's ethical, as I said it's a completely anarchic domain. There is no agreed definition what is ethical and what unethical. Just because state sponsors it, does not make it ethical. Since there are no agreed rules of war in this area, I find it difficult to make use of these terms or any other adjective. I think everybody does it and don't make it ethical or unethical.

Dr Nitin Desai:

Just a word on ethical hacking…The term ethical hacking is used for something very specific. These are highly professional organizations which are security advisors. What happens is, you go the guy and tell him this is my system, try and hack into it because I want to know how secure my system is. The idea is for him to help discover what are the vulnerabilities in the system. Let me give you an example. There was a nuclear plant in Europe and they said our control system is full proof. It is not connected to internet in any way and there is no way anybody can get into it. But they asked the ethical hacker to try hacking into it. He got right into the control system that was controlling the reactor. They asked him, how he got into it. There was a tiny point of contact between the control system and the information management system which was accessible to the managers. This tiny lever of control was in the production center. The hacker got in through that, Now that's ethical hacking. The idea to test the vulnerabilities in your system and I strongly recommend companies to access the service of the hackers to secure the data. Ethical hacking in this field means people providing this kind of service. But it's your choice whether you choose to trust these people or not.

Q 6. Sir, you mentioned the absence of conceptual framework in the realm of cyber security. So when we don't have conceptual frameworks in place, how do we formulate policies? Besides the technological momentum is so fast which many governments find it difficult to keep pace with. So how does NSCS formulate policy when there is no conceptual framework?

A. Well, if you wait for perfect knowledge, you will never formulate any policy. I don't think we have proper framework to understand how international relations works. But that doesn't mean we don't

have foreign policy. Just because we don't understand war in all its manifestations, doesn't mean we don't conduct it and we don't have defence ministry and army etc. So let's not frighten ourselves with the lack of conceptual clarity. You will have conceptual clarity 7000 years after all this is over, may be. But that doesn't mean we don't have to do, what we have to do. Secondly, I am not claiming that government knows everything or government knows the technology. But it's more than technology. Government has to work with those who have knowledge of the technology including the labs, the technologists, the scientists, and the firms everyone. But the reason I said government is evolving architecture is because we are not laying policy cast in stone. Here this is rigorous and we will follow it for all the time to come. No, because it exactly the reason you said. Lack of clarity and it is evolving so fast. We will have to create an architecture which will be able to deal with it and we can learn as it grows and I think that is not beyond our capability. We have done it before and we will do it again. We are starting it afresh and we can do it for ourselves. In India we can think for ourselves and put systems for our own needs. You don't have go around imitating what other people do.

Q 7. My question relates to protection of citizens from blackmail that happens on the internet and with regard to privacy policies. You wish to have an access to a website, you cannot access it without signing it. So you say yes and the next page appears. That's one part of it. And secondly what is the government's policy to protect the data centres in the national boundaries?

A. There is a technological problem with both but there are also issues of legal authority involved today. Part of what we are going to discuss with the private sector is to discuss these kinds of issues what you have raised. Today, the way the internet works, the national boundaries may apply notionally, they may apply legally but they don't work in practice. But you cannot cut off yourself.

Individual's right to privacy is something we have been working for past two years. We also need to work on data protection, date retention and there is set of things which we identified we need to be doing. Ultimately we need to discuss these things among ourselves and then start working on these things among ourselves.

Q 8. How serious and how much of a threat does India face from the neighbourhood countries like China, Pakistan and intelligence agencies from those countries and terrorist organization from Pakistan.

A. First, these things can't be attributed and secondly my job and I am paid like other government agencies to think bad thoughts and to prepare for them make sure they don't happen. That's what we do. There is no accepted international matrix which tells you can measure the level of threat and how much they have done and so on. So there is no such thing as measured threat what you get is somebody's personal opinion and it's not worth much quite frankly.

Q 9. You said human resource is not a problem.

A. It is a problem because you know because everybody wants it and we have it, which is better than many countries in the world you can say and we have an ability to generate many more people when we need it.

Q 10. So would that mean developing a new policy to attract talent from the industry because the NTRO experience tells us, we couldn't get right people, though we have a cyber security division.

A. Even if they got the right people, they wouldn't tell you. That's part of the problem in this field. Nobody tells you the truth and they shouldn't. It is not open, transparent area. True cyber security is where nobody exposes their vulnerability and nobody exposes their strength. It doesn't make sense in this area. That is why as I said, the task force report like this is useful as it gets people talking about it, thinking about it.

Cyber Security Task Force Report Release Panel Discussion

Deputy NSA Vijaya Latha Reddy

When we talk about the way forward, we have to talk about the structure in the government and the kind coordination needs to be. I am not sure how many are aware of the fact that there are huge numbers of government agencies who are involved in coordinating cyber security architecture. Of course, the DIT (Department of Information Technology and DIETY (Department of Information, Electronics and Technology) and the DoT (Department of Telecom) remains the centre players. Particularly the use of handsets and internet the role of telecom has become very important whereas the IT was mainly seen in the IT departments. But apart from this for cyber crime and cyber terrorism there is MHA; for international cooperation issues particularly for the multilateral and regional mechanisms, there is MEA; the NSCS only provides a coordinating role where we try bring in all of the government agencies because we are not an operational agency. As I said, there will be intelligence agencies involved, there will be host of people involved here. So first thing is what the government should be doing and what kind of structures we should be setting up. The second issue is what is happening in the private sector; what is happening in the academia and what is happening in terms of HR development and what kind of PPP can we look at? What way we can cooperate with the private sector.

On human resources as the NSA said, I think, we have huge numbers of people available; the young people who are willing to involve in cutting edge technology development but we have to provide resources to train them. We have to set up centre of excellence where we have to design courses in cryptology and cyber security. This is an overall issue of security studies which Arvind and I discussed before. We need more departments of defence studies but cyber security and cryptology will help. This will help you in getting number of experts who would be recruited in these agencies whether in government or in private and work together to ensure cyber security. The other point I wish to highlight is that there is no such thing as total safety in cyber security. We will never reach a stage where we can sit back or any of us can sit back and say that we are a cyber safe nation. It will always be a work in progress because the technology is advancing so rapidly. The minute you put a firewall, and block one kind of attack, there will be another kind of attack and breach the defence you put up. I thought I will just highlight some of these main issues.

I must say I have used both these reports. The one which is released today and the DSCI report which I have with me which is equally a good report done by the private sector experts, “Securing our Cyber Frontiers” which was released recently. Normally I take the scenarios from the DSCI report to alarm people and recommendations from the IDSA report to show that the government is open to take suggestions from both, the think tank- academia world and the private sector, which is why some of the conclusions are common as well. So without a further ado let me introduce the panelists on the dais.

I will start with Dr Gulshan Rai with whom I have worked very closely; he is an additional secretary in the DIT and the Director General of CERT (Cyber Emergency Response Team). He is the man who out together an excellent defence that the NSA referred to on the Common Wealth Games. He ran the operation with the experts from other departments. Needless to say, he is highly qualified and has

MS and M-Tech and PhD in Electronics, 25 years of experience in different areas of information technology including cyber security, e-governance, legal framework and the information-technology Act which governs most of our work on cyber issues. Dr Rai has been working since 1998 in the area of evolving legal framework to address issues in cyber space. He is also head of e-security and cyber law division in the Ministry of Communications and Information Technology. He was executive director of ERNET India and set up first scale large education and research network in close collaboration with the institutions in the country. He is particularly focused on developing security capabilities in this area.

Moving on to Lt. Gen Aditya Singh; he retired as GOC-in-C Southern Command, the largest command of the Indian Army. He was earlier Commander-in-Chief of the Andaman & Nicobar command after the Earth-quake and Tsunami on 26 December 2004 and also the Vice Chairman and the operational head of the Integrated Relief Command responsible for the Emergency Relief and Successful rehabilitation of the ravaged islands. He was also the member of the National Security Advisory Board in the NSCS from 2008-2010.

Mr. Harsh Jain is from the Ministry of External Affairs. He has been working very closely with us on the issue of international cooperation, the different aspects that are coming up in Geneva, New York, BRICS, IBSA and in our negotiations with different countries. This is one thing we did manage to do in NSCS to say that all the major players, DIT, DoT, MEA, NSCS should sit together and consider any proposal that comes for cyber security cooperation to make sure that we are speaking in one voice in all forums. He will say something to us on that aspect.

Major General H G S Sachadeva is Additional Director General, Information Warfare in the DGMO (Directorate General of Military Operations). He was commissioned in Gorkha Rifles in 1976 and has held various staff commands in the Indian Army. His last charge was commander of 36 Rapid and he is an alumnus of the National Defence College.

Mr. Felix Mohan is the representative of the Private Sector on the panel. No matter what we say on government sector and private sector; we will hear it from the horse's mouth. He is Global Chief Information Security Officer, Airtel. Prior to entering the private sector, he has held a broad range of technical and leadership appointments in the Navy including the top IT post as Director of Information Technology. Mr. Mohan has presented papers on information assurance and information warfare in various fora and he is an external expert on guiding fellowship research in information security. He was member of the information warfare committee tasked with formulating polices and creating infrastructure for warfare initiatives. He has written extensively on information security in national newspapers, technical publications and has been awarded the Vishishta Seva Medal in 1998 for his work in IT security. He has been a member of the national task force on information security under the auspices of the National Security Council. With that now I will let the panelists to take over and as I can see in the programme, the topic for today's discussion is "India's cyber security challenge: The Way Ahead".

Dr Gulshan Rai, Director General, CERT-In

The issue is how are we handling the challenges today and what's the way forward as the chairperson just said. As a part of CERT-In and having analysed incidents of cyber crime for quite some time, I would certainly not hesitate in admitting that we are not too bad and we are not too good also. The challenges are there and we have to surmount them. The entire IT technology today is characterized by the technological obsolescence and rapidly advancing innovations. When you deal with innovations, you come across issues that you did not foresee by any imagination. This is entirely a global kind of space. Any challenge that we have faced, we have to see it from global point of view, not from the local or country point of view because a cyber incident can happen in any part of the world and it can have effects all over the world simultaneously. This has been amply demonstrated in the cases of Georgia and Estonia. You won't be surprised to know that the traffic on internet is hijacked to some extent just to prove a point and show that you have the ability to disrupt. The technology which is used in defending the cyber space or preventing any cyber breaches plays a comparatively smaller role these days. It is the people and the processes that play an important role. So one has to keep in mind that it is a global phenomenon and attempt to formulate policy accordingly. As the chairperson pointed out, we do have lot of manpower but is the manpower adequately trained to handle the scenarios that we find in cyber space today?

I can give a number of cases. One of those that touches all of us is that half- a million modems in our country are compromised. It has not resulted in some sort of cyber terrorism or cyber incident but is an instance of entrepreneurship which has in turn created a cyber incident. Dial up modems sourced from a third country have been found to be compromised by a script on the chip that goes into the modem so that when someone tries to access an internet site by using that dial up modem, it fetches an advertisement and shows it along with the website that one is accessing. So this absolutely a global phenomenon and the challenge before us is that of capacity development and procedural awareness. We can buy technology from various sources but by carefully monitoring the procedural aspect we can reduce the breaches by 30-35 %. The entire expertise does not lie in one pocket, be it the government or private sector. We need close collaboration between all stakeholders be it government or public sector or private sector or academia and that for me is a challenge ahead. How do we bring the stakeholders together, how do we increase the procedural awareness and capacity to create a framework where we work together with a common interest, is a challenge because it affects each and everyone.

Another issue is how to improve the physical security of the cyber assets. One way is through mock drills, and we have been doing these mock drills and the response is improving slowly and gradually. We wish to bring the industry on board in conducting the mock drills and evaluating our security posture.

The other challenge that the NSA has rightly mentioned is that of incident sharing. In 2005, we have had 5000 odd incidents reported but the actual numbers of incidents are much larger than are usually reported. This is where we were we have to put the framework in place to improve the cyber incident reporting, because this is the only way we can learn the magnitude of the problem and how to handle those challenges, how to disseminate information to the concerned people and ultimately to improve our cyber security posture.

These are complex issues and we need help of each and every stakeholder and we are very open to suggestions as to how to work together. For us in CERT-In, one of the major challenges is to systematize the interaction between the public and the private sector and improve the information sharing.

Lt. Gen Aditya Singh (Retd.), Member, Cyber Security Task Force

Good Afternoon Ladies and Gentleman and thank you IDSA for allowing me to be on this panel. I am not going to talk so much about cyber security; I am going to talk about the business of war and how war has taken a new frame in this 21st century. Let us ask ourselves and I will try and put it to you and ask you to answer yourselves two questions: A) 12 years past, what have we learned from 21st century? B) Are we safer today than the 20th Century?

The answer to the second question I think is universal. Today you have the hydra of terrorism in different manifestations, biological weapons. SARS, and other pandemics coming up. Look back to the trends and understand what have learned from the 21st century. The 21st century began with the 19 terrorists attacking the World Trade Center which started the global war on terror. The House of parliament was attacked by 5-6 terrorists on December 13, 2001, which started the two year deployment. 26/11 carried out by 10 people had the whole country up in the arms. The point I am trying to highlight is that in the 21st century, asymmetry is the key.

You have had disasters in the 21st century. The tsunami was there; you have weather patterns changing, you had pandemics, you had SARS, Swine Flu. The era of poisoning the cities and biological warfare is coming back. You got the rate and pace of change. We were thinking of kinetic weapons, but today we are in a different era, you have talked of the exponential growth, and more so in the knowledge domain. So I think the answer to what we have learned from 21st century is uncertainty and ambiguity; from analog to digital and from kinetic to abstract. So this is what I am gonna talk about.

Most of you would have seen a very interesting video that SONY put out in 2010, “Did You Know” and there are two points, I think that is relevant to our discussion on cyber war. The first point he said, “The top 10 jobs in 2010 were not even thought of in 2004”, Second, “you are preparing students for jobs that don’t exit”, “for using technologies that are not even invented”, “to resolve the problems that we do not know”. Related to internet, the way it’s grown, you will see the pattern changing. In 2004 there was a social networking site ‘MySpace’. It had three million members. In three years it was sold. It has died. You got facebook today with 900 million users. You have got twitter with 200 million tweets every day. The reason I am talking about the social networking sites and the NSA also mentioned, they are going to increasingly change the way people start thinking and working. When we talk of the private sector and as the internet dominates the global commerce and governance, I am convinced, most of the internet service providers must be having their internet armies to protect their systems. Have we as a government thought of that; and have we as a government, as Gulshan mentioned, as a Public-Private partnership, taken into account that there are these vast armies, where commercial interest dictate how these corporations decide their policies, and how we can combine to build a proper national response.

I am not going to highlight the points mentioned in the report, but will go through the scenario and some of you would say it cannot happen. There is this gentleman called Bruce Schneier, he raises your morale each time saying this bunkum will never happen. But can you tell me with some certainty that it will not happen and if it does, then as the NSA said, “we are paid to think bad thoughts”. For easy understanding let me relate to the war scenario of the 21st century to the game of football. The 21st century war is like a game of football. A proper Stadium with 11 players, fixed

goal posts, a period of 90 minutes etc… Lets us change that to a hollow sphere, a size of football field. You got moving goalposts, you got an uncertainty in the number of players, some of them are visible and some are not. You have players who got the capacity to float around in this miasma. The time is of irrelevance, there will be long periods of lull with a certain flash of activity. There is no start, there is no finish and all this is not in stadium but performed before the global audience. That is the kind of war which I see in 21st century. It is the no-contact war but it will affect everybody. Though cyber is technically limited to internet, but with the other mobile communicating devises connected to internet; the NSA mentioned 381 million phones; now has a global reach and will affect everybody. By 2015, there will be twice the number of devises connected to internet than there are people and that the usage of internet is forecasted to go up 9 times in India. Therefore you have a got a cause to worry.

As the resources are limited there will be an acute competition. Our large neighbour China, after the Gulf war, chose for the information warfare and has built up a strong capable force since 1980s. We know the war which was fought in 1962 is no more a reality today and if is fought in that manner, we can hold on. But what if they fight in this new foot-ball field of 21st century and I can tell you; having considered the analysis, our humiliations would be greater and more visible. Today, it's not the territorial systems that needs to be protected but it's the systems - banking, transportation, finance, health, civic services, e-governance etc all that will be affected. It is therefore important to maintain the reputation as a nation, faith in its growth, and investments, and ensure trust of the people.

India is a target and there have been *n* number of attacks. Please understand most of these attacks are in the nature of cyber exploitation. In other words they are silent. Any nation who wants to understand how your networks works, will never reveal it is identity and you will never know what is happening. They gather knowledge through espionage, intelligence; and there are enough indicators. China which incidentally has 1200 research labs, downloaded tetra bytes and mega bytes of information of defence networks and it is widely publicised.

The war today has different connotations and it is built up by the media, by the visibility it has. So few points I wish to highlight.

I think we have got the national cyber security policy draft, but that broadly talks about security aspects. But we really need to classify the objectives to ensure deterrence because that's a visible document. That leads me on a legal framework. The IT Act provides strength under section 69 and 70 to ensure no miscreants take advantage of the internet. But alongside there are the Laws of Armed Conflict (LOAS) and section 51 of the UN charter provides you the Ability for Self Defence and Defence cannot happen in isolation without some offense action.

Protection of critical infrastructure, I think is covered. But we need to in the policy to enunciate measures of self defence. We should mention it as a part of the doctrine as we know; the whole world is doing it. The US has a "Proactive Operation group". The other reason why we need to build the offensive capability is 'War'. We are fully aware that Chinese as part of part of preparation of battle-field have hardened their networks, have used fibre-optic cables to make sure that they attack all your ISR, i.e. the Intelligence, Surveillance and Reconnaissance means to render your systems redundant or fail by a cyber attack. If so, we need to prepare for war and it is only a matter of time. Raising our own cyber command is obvious and the privacy concerns must be addressed when we are raising our own cyber command. We could follow the guidelines of the US Cyber

Command because that country like us is a deomocracy and these concerns need to be addressed if when we are raising our own. We can take questions on this later, but I think the structure for India, like the US; should form a part of our strategic forces command. Because the Strategic Forces Command in US has cyber command and the space command within it because both these domains have lot in common. It must incorporate the CERTs from each service, the intelligence operations, the defence communication networks, and the cyber operations required for the battle-field. The beauty about the Cyber as was mentioned by Nitin, is unlike the complicated and expensive weapon systems, it's a low cost option. It requires man-power and it requires fraction of the cost by which you can ensure proper defence in the scenario of no-contact war of 21st century. I think we need different contracts, systems, simpler and faster procedures to keep up with the time. To paraphrase the famous saying of the Battle of Britain, "you can by small cyber command, use so few to do so much for the country".

I would like to spend a little time of social networking. India today has 45.8 million users on facebook, that's four per cent of your population. I am just trying to give you the numbers. Four per cent of your population which is the opinion makers and as was brought out the Arab Spring, the London Riots used the social networking media. The states and governments must understand, while one wing will do utmost to damage the reputation of the government; they must be ready to interact in ways that cannot be public. I will leave it at that but we must definitely have people who are from the national security side on to the social network media; seeing what is happening; putting up public opinion and as I said, if you can get 4 million tweets on the IPL, surely somebody must be tweeting.

Language training is one aspect which I must highlight. Cyber war is one field in which ladies can play a big role. If you have seen the videos of Drone Controllers in Utah, US; half of them are ladies. So I think language training, continuity of job this has a great scope.

The last point I wish to make is where do you get the manpower and systems? How do we train so many people without need? I am convinced, and proved by the 26/11 attacks which produced 20 million jobs in the security sector, there is going to be tremendous need for cyber sleuths, doctors who can keep the internet going. But here is a huge potential and therefore it's a win-win situation and it will in my opinion become sustainable.

Somebody says that the cyber war is unseen. I will only conclude by saying, "see the unseeable, think the unthinkable, and do the undoable"

Major General H G S Sachdeva, Additional Director General, Information Warfare, DGMO

At the outset I must thank IDSA for giving me this opportunity to share my views on cyber security.

The advancement in technologies is changing the very form of the war, just as the industrial age led to the concept of mechanized warfare, the emerging enabling technologies are heralding the era of information war. The erstwhile physical attritional models are giving way to nerve-centric paralytical models. Combat superiority based on lethality, accuracy and mobility is increasingly going to share its importance with information assurance based on network resilience and redundancy. Similarly, society is also undergoing a change which has extensive implications on governance and security of a nation in peace as well as in war. The dividing line between the civil and the military has blurred and so are the consequent effects on the national security.

The threats that we in the armed forces perceive; although the scenario has already put in the report and elaborated by Gen Aditya; you add to this denial of service, attacks on the aviation sector, plunging air-traffic in disarray and making air-traffic management impossible. Railway networks sending trains on collision course and blocking strategic routes. Satellite communications, naval ports, and armed forces communications networks to name a few being attacked through cyber domain either planned during peacetime or physically by cyber warriors. The resultant effect: the mobilization of forces from peacetime locations is disrupted; the availability of force levels through different borders or launch offensives is reduced in the few initial and critical days. The command, control and surveillance capabilities are adversely impacted and there is loss of situational awareness and synchronization of military activities. The situation is now ripe for the adversary to launch his offensive against disorganized, disoriented, isolated blind and vulnerable forces. This is just a beginning. With increasing sophistication of military weapon systems that rely on automation for quick response and increased accuracy based on advance guidance systems, the danger is also from the embedded malware and reliance on services provided by foreign agencies. While the Scud missiles of Iraq may have failed to reasons of technology; strategic weapons failing due to malwares and providing duds in actual war are not only embarrassing for any nation but could throw the entire war-fighting strategy into disarray.

In a nutshell, the cyber war has the potential to ground the best laid out strategy and operational plans. Gentlemen, military defeat is not acceptable to any nation. Therefore this final instrument of ensuring national security can ill-afford to lose information war in cyber domain. The threat is real in this network-centric environment. Some of the challenges which we in the armed forces face: the transformation from conventional army to network centric army is throwing up number of challenges which need to be addressed on priority and we have to leverage the opportunities that are being provided by the cyber space. Security is all about people, process and technology and as such there is clear need on focusing people, and processes while attempting to use best available technological solutions.

Our effectiveness in cyber space to a great degree is predicated on our ability to train sufficient number of qualified personnel. There is an urgent need to train large number of cyber professionals and deepen the level of their training. But even as we strengthen our cadre, we must recognise that

long term trend in human capital is against us. There are issues of availability, training, retention, remuneration which even a country like US has recognized. Hiring an expert is an option but then there are issues of work ethos and organizational culture. How does one fit the uniformed disciplinarian working in a hierarchical framework with missions, orders, well laid out rules, with persons who defy any authority, set their own rules have no fixed working hours, detest uniforms and it's a bonus if they are wearing shoes. The situation demands out of box solutions, especially a change in the mindset of armed forces if we were to have pool of trained men at the disposal of armed forces.

Awareness: The present level of cyber awareness in our country, as brought out earlier, is not at the desired levels. The armed forces are no exception. There is need to enhance cyber security awareness by undertaking exhaustive awareness campaigns that inculcates better cyber hygiene and use of best cyber practices. A lot has been done in this field, and perhaps I can say, what has been done in past one year is more than in past five years. We need to create a cyber mindset at all levels. But in a force of a million, where every year we add 60 thousand new people, the task of creating this cyber awareness in immense. Social sites like Facebook, Twitter, Rout are already mentioned. There is alarming activity of hackers through these sites specially to target defence personnel and they have tremendous scope in perception management, manipulations of information and if I may say, laying honey-traps and gathering intelligence. In such a scenario, the moot point is, can we totally insulate armed forces from the impact of social networking sites. May be not since denial is not the solution…

Asymmetric warfare: Unlike conventional warfare, cyber war can be launched by nation or independent elements with a very few cyber warriors against a numerically and technologically superior adversary with devastating effect. Easy availability of technology and tools has empowered individuals to change power equations between the nations. So we need to worry about everybody. Unlike in the case of nuclear weapons, where only few countries have it as Indian Armed forces get more organized and networked, the threat is also increasing exponentially.

Staying in the Race: The threats are moving in geometric progression whereas the solutions are coming in arithmetic progression and the gap is widening all the time. The challenge therefore not only to armed forces but everybody, is to remain ahead of rogue nations, bad boys, anti-technology marches. The current management aimed at addressing cyber security issues perhaps need a re-look. Every passing day of inaction or no-action is putting us behind by weeks and forces us to play a catch up game all the time. Therefore we need path-breaking ways and means to overcome this friction.

Militaries across the world are exploring ways to achieve superiority in cyber space by investing time, resources and money like never before. We must understand the gravity of today's threat scenario and realize that strong cyber security measures cannot be evaluated in traditional return on investment or bang for the buck criteria. Sufficient funds need to be made available and heavy investments are required. The problem is the outcome will always be in intangibles and invisible. Like one American said, "there are no heroes here". The financial support therefore will always be accompanied with mistrust and doubt and therefore it is going to be hard to come by.

The requirement to undertake forensic investigation to draw correct lessons from incidents and establish correct procedures to prevent the same in future will increase. Forensic investigations are

challenging tasks as they require resources in terms of infrastructure and qualified personnel which are limited and painstaking efforts are required for detailed analysis. Mobile networks and further connectivity will increase the problem. I already mentioned the problem of embedded malware. To prevent this is a challenge. The vulnerabilities are not only applicable to software applications but can be present in hardware components as well. The majority of IT products used in India are manufactured overseas. So how to ensure that no malware is present in the procured systems is a serious problem and the problem is compounded by serious lack of worthwhile facilities in the country for detecting such vulnerabilities. While production may be the long term solution we need to focus at the short term. Another problem is, unlike the conventional warfare, cyber warfare is an ongoing activity and is in fact more pronounced during the peace time. In fact, peacetime is more of a misnomer and it might be going on now as we speak. It will be a challenge for all of us not only to install safeguards, but to stay one step ahead of all the types of adversaries all the time.

Towards the end I must say to prepare our forces for emerging cyber threat landscape, we need to give impetus to capability development in both defensive and offensive cyber activities and evolve a clear cut strategy to assist services to remain on the cutting edge of technology and infrastructure. I think the task force report is probably is a stepping stone to that. Also just as the military defends against hostile acts from land, air and sea, it must also be equipped and mandated to respond to hostile acts in cyber space if required in a quid-pro-quo manner.

Lastly Gentlemen, we need to change our mindset, processes and technology and change fast, if existing rules do not allow it then change the rules.

Felix Mohan, Global Chief Information Security Officer, Airtel

This is a report that was far overdue from the private sector perspective. To set the context of private sector involvement in cyber security, on just one day, 15 May 2012, Airtel experienced 6600 new never-before-seen viruses, excluding variants, 16,000 attacks graded as high intensity attacks, over 6 million probes on our servers, 2.5 million spam. 95,000 out of 150,000 subscribers had computers that were part of Botnets. Effectively, 70-80% of computers are not in control of their owners. In effect, we have a potential enemy army sitting there right in our midst which can be triggered to attack at a moment's notice. While we talk of capability building, education and training, awareness of end users, the layman, the ones who are using computers for social interaction is essential for cyber security. The Government and private sector have to work together and make huge amount of effort in different languages.

Though the Cyber report is pretty comprehensive, my view is that it is more biased towards defence and security. Cyber space by definition fosters economic growth and social values, but because of threats, we tend to focus on the security component forgetting growth component. What do we want of our cyber security policy? Policy should emanate from growth and societal vibrancy.

If you look at our organization structure-there are 2 categories of ministries, ..ministries that foster growth like the Department of Information Technology, and those that protect like the Ministry of Home Affairs. There is usually a power balance that ensures that the interests of all sides are taken into account when formulating policy. If one view ends up being dominant, that will stifle the sector. For example, if the police had cars that go only at 30 kms per hour, and they therefore brought in a law that all cars can only go at a speed limit of 30 kilometers per hour since that's the only way they could chase you down. This is analogous to the encryption policy of the government. We are still grappling with the government to increase our encryption which has been set at 40bit. So, a solution would be that the cyber security structure should have one clear authority that can take a balanced view of these issues. The suggestion in the report of the NSA being the overall authority is an excellent one.

Partnerships are crucial to cyber security. Airtel operates in 20 countries..and all these countries see the public-private partnership as a trail blazer in India. For example during the Commonwealth games, Airtel put up the infrastructure. We were concerned about attacks, but largely flying blind. CERT-In provided us with precise, credible info, saying these are the IPs you should focus on , and we blocked almost 8,000 attacks.

During the Stuxnet breakout, a lot of work was by Airtel and other ISPs pushing information and signatures to CERT-In in realtime. In the case of the compromised modems, we got the info at 9:30 pm from CERT-In and sent out messages to end users by sms. We have received nearly 1400 letters from law enforcement agencies thanking us for our cooperation not just in cybercrime, but other areas where our help was required.

In 2009, CERT-In suggested simulating attacks on infrastructure. In the very first such exercise, there were only about 10 organisations with only Airtel from the private sector. We thought we were well prepared, but learnt a lot from the simulation. One of the outcomes was that we put honeypots in place. In the latest exercises, the number of organizations volunteering is massive,

and it has become a mark of prestige to have participated. I would consider it a wonderful example of public private partnership.

That is not to say that all is perfect. These partnerships can only be built on foundation of transparency and trust, but right now, the private sector is not trusted at all and this diminishes the value of what we bring to the table. If you look at Section 43(a) of the IT Act, it says reasonable security practices should be left to the private sector.

There is a tragedy of the commons, that individual companies don't bother to safeguard a wider common good since the risks get distributed. We welcome regulation but not over-regulation. The private sector is not involved in policy, and neither should they be. Certain objectives should be mutually agreed on, so that we can go beyond just deciding about policy and put our act together at the back end. In areas such as secure equipment, supply chain security. Common criteria, and 3gpp, we tell the government that while it looks good on paper, it may not work in practice since it's technically not feasible. If you take the different sources of vulnerabilities, in the case of category attacks, the policy says if one model passes certification, that means all the models are certified. Then there are the patch attacks; a software or hardware might be certified as secure, but they need regular patching and the patches might be trojanised and make the equipment insecure. The third vulnerability is in the supply-chain and distribution network; while a particular piece might be sent to the test lab and certified as secure, there is nothing to stop insecure and trojaned equipment being sent to the company. So, while a policy might seem feasible at a theoretical level, it might not work out at the operational level.

Incentivising the private sector, even in terms of recognition or tax breaks is important since a common good has to be safeguarded., New vulnerabilities ahead lie in the form of emerging areas such as cloud computing, mobile, social networks, and consumerisation of IT equipment. While we digital immigrants have carried over our concepts of security from the analogue world the newer digital natives have no concept of security.

Research is also an important area where the government will have to focus on, especially in the areas of cryptography, botnets, rootkit detection, traceability forensics, deterrence, and dynamic self-healing networks needed.

As far as cyber war is concerned, Cyber commands are biased towards an offensive role, defence can only be achieved in coordination with the private sector since the battlefields are the data centres, and the enemy troops are the botnets embedded in private infrastructure. The big question is how does one get the military, the public and private sectors all to work with each other in a close enmeshed way?

Harsh Jain, Director, E-governance&IT, Ministry of External Affairs

Good afternoon. My focus will be on existing international cooperation on cyber security. I think from what we have heard today, it is very clear that existing and potential threats in cyberspace are among most serious challenges in the 21st century.

We recognize there is a need for close global cooperation on cyberspace. This recognition has influenced our active participation in the international discussions on cyber security, both at the multilateral fora as well as in our bilateral dialogues. India has actively participated in the United Nations Group of Governmental Experts(GGE), at the Council for Security and Cooperation in the Asia Pacific (CSCAP) ,and at the deliberations on the UN Commission on Crime Prevention and Criminal Justice. India has formal cooperation agreements (MOUs) between CERT-In and its counterparts in Japan, US, and South Korea, and informal contacts with other countries. India also has a regular Cyber security dialogue with the United States, and regular cyber security and cybercrime consultations with the European Union. Moreover , it is now emerging as a key agenda in the strategic dialogue with several countries. Some aspect of this is also covered in counter-terrorism dialogue especially the misuse of cyberspace for terrorist purposes.

While the importance of international response to cyber security is recognized by all, there are differing views on how to respond to cyber security – some countries believe that existing international laws suffice, and they favour norms for state behaviour, other countries are asking for a legal framework to deal with cybersecurity but at the same time, any legal framework would also have to be based on principles. On cybercrime, there is a debate on whether Budapest Convention should be made the framework on cybercrime.

Our international cyber security strategy in terms of what the MEA deals with is largely informed by the domestic stakeholders like NSCS, DIT, MHA & DOT. There is however a growing feeling that there is a need for norms to deal with cyber space as well as rules. Norms could be a forerunner for a rule based legal framework.

On cybercrime, we are keeping an open mind and looking at all possible options on an international legal framework, including Budapest Convention.

(*Compiled and edited by Cherian Samuel and Kapil Patil)*

Photo Gallery

Report Release Function-1

Report Release Function-2

Panel Discussion

The report of the IDSA Task Force on Cyber Security may be accessed at
http://idsa.in/book/IndiasCyberSecurityChallenges

The audio files of the release function may be accessed at
http://idsa.in/podcast/IndiasCyberSecurityChallenge