NNSA – IWG WORKSHOP AND ROUNDTABLE ON

"SCIENCE COLLABORATION AND SECURITY : A NEW GLOBAL

OUTREACH TO KEY ACTORS" AT COMO, ITALY ON 20 JUN 2011

-

ABSTRACT OF PRESENTATION BY LT GEN P.K. SINGH, PVSM, AVSM (RETD)

DIRECTOR, UNITED SERVICE INSTITUTON OF INDIA

-

-

-

Security policies of nation's affect the scientific and technological advancements just as scientific and technological advancements affect national security policies. In today's globalised world, advances in one country affect policies in another country. There will be tensions between the security and scientific objectives both at the national level as well as at the global level. There is thus a need not only for the scientists and security experts to have a dialogue within the country, it is equally important to promote international cooperation between the scientific and security community. These interactions will also help reconcile national interests with the "global good". I am grateful to this forum for providing just such an opportunity to Surgeon Admiral V.K. Singh and to me to participate as also to learn from today's deliberations.

The theme of this session is "Outreach beyond national governments". Obviously all national governments have the primary and important role of collaborating with other governments and internationally recognised organisations. Yet there is a need for outreach beyond national governments. Some of the issues we need to look at are :-

Countering chemical, biological, radiological, nuclear and explosive (CBRNE) terrorism lies at the heart of any counter-terrorism strategy. Wikileak cables talk of global jihadist movements may "soon possess a deployable CBRN attack capacity" – even if this report is exaggerated, can we totally ignore the possibility of a "dirty bomb" getting into the hands of some terrorist / extremist / jihadi outfit ? While governments have undoubtedly understood the dangers related to CBRNE threats and have passed legislations and signed treaties and conventions, rapid technological advances coupled with the revolution in the IT field are beginning to outgrow some of these treaties and conventions. Today we see, not only convergence but technological cross-overs in the biological and chemical production methods. The question that needs to be asked is whether these advances lower the threshold for misuse by new entities like the terrorists or non-state actors ? We also need to see whether advances in engineering technologies including IT lower the threshold. Today cyber attacks can have a crippling effect not just nationally but globally and these can be carried by States as well as non-state actors. "Do you know who all have been lacked over the last 2 weeks? IMF, CIA, Sony, Citi Bank, Turkish Government etc. etc. As somebody has said today there are only "two types of companies in the world – those who know they have been hacked and those that don't". Ironically the value of the web is in its connectedness and the threat to it also comes from this very connectedness. So network systems will remain vulnerable – the challenge is to find an answer. Shutting down the internet or having just strong legislation or technical solutions alone may not work. Do we really understand the social, economic and legal aspects involved? Does cyber space have boundaries and effect only one or some nations? If the answer is no, then can a solution really be found in one country or one company or any one organisation?

Do you know that since 9/11 the USAF devotes 3100% more hours to flying for ISR and today with the new "Gorgon Stare" technology you can capture live video of an entire city but you will need 2000 analysts to process the data feed from just one single drone !! How do you protect all this data at various stages of its capture, interpretation and dissemination etc. I would also like to mention a few figures to highlight the magnitude of the problem :-

(a) 2 million malicious sites are created every month.

(b) Four years ago 4 million malicious files were required to be tracked on a daily basis. Today that figure is 60 million malicious files which require tracking.

(c) 25 million applications are available, on-line for downloading. However, one is not sure if all these applications have been tested and are safe for use.

(d) From millions of devices using internet the figure has now jumped to a trillion and keeps growing.

While there has been a discussion about rogue states we also need to look at a "rogue scientific genius" who could wreak havoc by carrying out a cyber attack on a nuclear facility leading to a possible melt-down or use a new biomedical technology to cause a global pandemic.

The other issue that needs looking into is the availability of CBRN material including dual use CBRN material as these are now used for more legitimate purposes and hence more easily procurable through international smuggling and proliferation networks (AQ Khan network easily comes to mind as one such network). Another connected issue pertains to the stockpiles of decommissioned military CBRN material.

I have talked about the convergence of biological and chemical production methods. So with this convergence taking place do we not need to have a re-look at the Biological and Toxin Weapons Convention and the Chemical Weapons Convention ? Are there any shortcoming which were not visualised when these conventions were being formulated ? Is there a need to bring in convergence between these two conventions and possibly have an integrated Biological and Chemical Weapons Convention ?

Another aspect that merits our attention is the aspect of expert control regulations – should it include broad areas of technologies ? Do these help or undermine international cooperation ?

So what is it that we can do to reach the national governments and beyond. We could look at :-

- promoting education and awareness on matters of national security and sensitive CBRNE sectors.

- enhancing coordination between organisations dealing with CBRN and security issues.

- creating a network of research laboratories and institutions which could share their unique expertise, knowledge and best practices.

- creating a global network of monitoring stations to provide early warning of nuclear and biological / chemical events.

- share information / intelligence to prevent proliferation of technologies and sensitive knowledge reaching into the hands of terrorists / criminals.

- encourage free flow of ideas to address emerging / future CBRN proliferation challenges. If this is not done, the treaties and conventions that we work out will always lag behind emerging technologies.

- encourage collaboration in science, technology and research forming an important part of any Strategic Partnerships between countries and / or regional organisations.

- capacity development should include knowledge management, human resources development as well as scientific and technical institutions for applied research and training.

- cooperate in the filed of nuclear forensics.

- support biosecurity educational programmes at the university level.

- cooperate in disaster management / mitigation programme.

Today, all technologies can be used for good or for evil by States as well as non-State actors. The challenge is to ensure that it is used for good. We have to find concrete and innovative ways to bring greater synergy between the security experts and scientists to prevent the misuse of evolving technologies.

Director's Page