Synopsis

Conflicts in Cyberspace: Defending India's National Cyberspace: Governance Architecture

Webinar Summary Report

Publishing Date: 08 Aug 2022

Published By: The Current and Strategic Affairs Forum

Acknowledgements:

The webinar CASA WEBINAR SERIES: CYBERSPACE OPERATIONS Episode 2: Defending India's National Cyberspace: Governance Architecture was held on 17 July 2022 at 5 pm IST. It was organized by the Current and Strategic Affairs Forum (CASA). We would like to thank our moderator and panellists for their comprehensive analysis and for their candidly expressed views:

Panellists:

Lt General P R Kumar, PVSM, AVSM, VSM (Retd)

Mr. Jitin Jain, Director Voyager InfoSec

Mr. Brajesh Singh, Addl DGP, Maharashtra.

Moderator: Lt Gen (Dr) RS Panwar, AVSM, SM, VSM (Retd) Distinguished Fellow USI

We would like to thank the many other distinguished attendees including many senior veterans, business leaders, professors, think-tank researchers, contributors, analysts and others who took out time to participate as well as share their inputs, relevant Q&A and comments during the course of the webinar. We would like to thank Lt Gen Gautam Moorthy, PVSM, AVSM, VSM, ADC (Retd), former DG Ordnance Services and the Founder of CASA and Mr Mahadevan Shankar, Member of the CASA Core Committee and the IT Team for coordinating logistics, back end coordination and for live streaming the webinar on the CASA YouTube channel.

Disclaimer:

The views expressed in this webinar summary report are those of the presenters /participants and do not necessarily reflect the policies or opinions of CASA or

Introduction

Lt gen Gautam Moorthy , PVSM, AVSM, VSM, (Retd), founder of CASA Forum began the 29th webinar (8th this year), by extending a warm welcome to all the participants, the moderator and all those who had signed in from both India and abroad. He introduced the eminent panellists with a brief bio of each, dwelling on their vast experience and knowledge on the day's topic. He invited them to share this knowledge with all those attending the webinar and outlined the context in which CASA was hosting this webinar. He informed the audience that in the first webinar of the series held on 03 July 2022 the topic of Strategies & Structures was examined along with the existing organisations in many of the major states in the world and Lt Gen (Dr) Rajesh Pant, PVSM, AVSM, VSM, (Retd), now lead coordinator in the PMO for cybersecurity had dwelt at length on these structures (a synopsis of Episode 1 is available on our website). We had also examined the merits and demerits of offensive cyber capabilities as also the need for India to develop such offensive cyber capabilities accordingly.

General Moorthy informed the audience that in the present episode we would attempt to ideate on the governance architecture needed to defend India's national cyberspace and to further examine as to how a balance could be struck between the charters of the major actors involved, mainly the MOD and the Armed Forces along with other ministries, external and internal agencies as well as the private sector. While doing so, we would also examine the need to confine all offensive cyber capabilities within the MOD and the three Services of the Armed Forces on land, sea and air. General Moorthy then invited the moderator, Lt Gen RS Panwar to conduct the webinar.

Taking off from where General Moorthy had introduced the webinar series, General (Dr) RS Panwar made the following additional points:

- Though the stress of these series would be on offensive cyber operations as well as on cyber influence operations, it would not go into cyber espionage, but would be confined to those aspects of offensive cyber operations that would lead to suppression or destruction of enemy cyber targets.

- Today's webinar would be looking at governance of national cyber architecture from a national security perspective and not through the prism of cybercrime.
- The term defence should not be allowed to imply the absence of offensive cyber capabilities.
- Nations flaunt their offensive military capabilities in the physical world with great pride. However, in the cyber domain there is evident hesitation, despite all nations including India having declared cyberspace as the newest domain of warfare, to declare and own up to their possession of offensive cyberwar capabilities.
- Kinetic operations can be easily attributed to the perpetrator. Cyber operations are clandestine by nature and difficult to attribute to the perpetrating nation.
- The General enumerated the various types of cyber capable organisations and their years of emergence in many countries including that of India. It was pointed out that in the case of the US, China & Russia, offensive cyber capabilities were mostly exercised by military organisations whereas in the UK and Australia the same was controlled by a hybrid organisation comprising military and other external intelligence agencies.
- In the backdrop of what he had said General Panwar sought answers to the following during this episode:
  - Should India declare its intent to employ offensive cyber capability as part of its national cyber strategy?
  - What would be the recommended distribution of charter between various agencies for offensive cyber operations both during the period of grey-zone war and all-out war?
  - What should be the role of the MHA and the Private Sector in defending our critical information infrastructure?

With that the Moderator invited the first speaker to take the floor to present the defence forces views on cyber architecture to defend India's cyberspace.

Lt General P R Kumar, PVSM, AVSM, VSM (Retd)

General P R Kumar began his presentation by thanking Gen Moorthy and the CASA forum for giving him this opportunity to place his views before such eminent panellists and a knowledgeable audience. He was of the view that in this new virtual non-kinetic domain of conflict if one neglected to keep up with the developments in the information space and in cyberspace one could face existential threats in case of sudden attacks by foes. The General's observations on multi-domain operations included:

- Space declared global commons by Outer Space Treaty of 1967.
- Cyberspace is in the virtual domain and in the realm of information.
- Armed Forces Officers must see themselves as 'National Security Professionals'.
- A conflict always existed between the commander/user and the technical expert in terms of domain knowledge and professional employment. The views of the commander/user must prevail at all times.
- Cyberspace is as important as physical territorial assets and must be defended as such.
- It is time to replace cyberspace with info space as a warfighting domain covering all three aspects of IW- cyberwarfare, electronic warfare and psychological warfare.

National cyberspace information infrastructure must include:-

- Critical information infrastructure.
- Defence Information infrastructure.
- Non-critical information infrastructure.

In the US it is the Cyber Command that is responsible for looking after all critical information infrastructure. In the UK apart from the National Cyber Security Centre established in 2016 they now also have a National Cyber Force since Nov 2020 as a partnership between the Armed Forces and the GCHQ. The UK army has launched a new cyber force namely 6th Division to focus on Cyber, EW, Intelligence, Information operations and unconventional warfare.

The General pointed out that in both cases of the US & UK, offensive cyber capabilities were in the hands of the military. He wondered if in our case, the government would allow our armed forces to be in exclusive control of offensive cyber capabilities. He also briefly touched upon the well-developed cyber capabilities of China and Russia. Offensive cyber capabilities are also vital in disabling the entire architecture of ground space links. The US has already declared that a cyber attack on its space assets would be construed as an act of war.

The Gen briefly spoke about the current stake holders in safeguarding our national information infrastructure apart from protecting their own cyber space :

- Ministry of Defence (5th domain of warfare)
- Ministry of Home Affairs (Internal Security)
- Ministry of Electronics and Information Technology
- Intelligence Agencies

Currently the agencies looking after cyber are:

- National Cyber Coordination Center (NCCC)
- Critical Information Infrastructure Protection Center (NCIIPC)- a unit of the NTRO and the CERT that function under the Ministry of Electronics and Information Technology.
- In addition and still in its nascent stage are :
    - Defence Cyber Agency (DCA)
    - Cyber and Information Security (C&IS) Division of the MHA.

In the current set-up it is to be noted that under the coordination of the National Security Advisor and the National Cyber Security Coordinator, there is an apparent lack of coordination, lack of synergy, tendency to work in silos and a palpable lack of direction. Our system is overly defensive in nature which is a severe limitation. It was highlighted further when the Gen pointed out that the Armed Forces have not as yet been mandated for offensive cyber operations despite it being acknowledged that cyberspace forms the 5th non-kinetic dimension of warfare.

The General then listed out some of his recommendations:

- Setting up a new Ministry of Internal Security as the MHA has become too large and unwieldly.
- Set up a Hybrid and Disruptive Technology Management Organization.

He then moved on to suggest a new approach to Information and Cyberspace Management Organization modelled on the existing pattern of the NDMA & DMF. The new organisation to be called the National Info-Space & Cyber Management Authority (NICMA) was then described by the General. Like the NDMA the new organisation too must be created through an act of Parliament.

The floor was then handed over to the second speaker.

Mr. Nitin Jain

He began his presentation by stating that there was indeed a need for restructuring the cyber architecture in India to bring about more synergy between different agencies that operate both under the central government and the state governments as also amongst the various specialist agencies dealing with cyber security themselves. Based on his over decade long experience in this field of cyber security he had the following observations:

- Before taking up the design of an architecture, India could examine and choose the structure best suited to its needs. He briefly outlined the existing structures in the US, UK and China.
- Despite having a National Cyber Security Policy in place since past 8 years we have as yet failed to create adequate resources in terms of trained manpower and requisite capabilities.
- Foreign models may not work well in India since our governance practices divide subjects between the states and the central government. He quoted the example of how Defence was a central government subject while law & order was a state subject.
- In other countries the integrity of institutions is maintained and strengthened whichever political party assumes power. Institutions are above politics and a form of oversight with clear allocation of mandate and responsibilities and reporting channels have been evolved.
- Questions of trust prevent our governments from giving complete control over offensive cyber capabilities to the

defence forces for fear that these capabilities could be misused by a party in power against its opponents.

- He cited the example of the spyware termed Pegasus that could have been created or acquired by our cyber agencies but it was not done for fear of adverse political opposition.

He too strongly advocated bringing all different agencies dealing with cyber issues under one common umbrella organization. He further outlined his idea of a body like the Election Commission which gets all powers transferred to it during elections but reverts to its normal state once the elections have been conducted.

For both offensive and defensive cyber capabilities, he suggested an oversight body fully under civilian control during normal times with these being transferred to the Defence Forces during periods of grey zone war or hot war. However, he cautioned that since today we do not suffer from lack of funding as in the past, we must curb the tendency for every cyber organization vying for funds and indulging in an uncontrolled 'free-for-all' type of creating offensive cyber capabilities and using them independent of each other without a real mandate to do so.

A complete system of accountability must be catered for in the processes governing the use of offensive and defensive cyber capabilities. So far we have failed to create adequate sources for trained manpower and mostly it is the same 500-600 persons that are kept rotating on postings between organisations. The tendency of our agencies to outsource 70% of their work to agencies outside their remit is not desirable when it comes to cyber security domain.

He suggested that it would be better to bring the trained manpower held by these outsourced agencies within the system and thereby enhance accountability. The need to ensure deniability in case things go wrong must also be catered for- outsourcing is an attractive way of doing this with least effort.

Thus far, organisations involved in cyber security have mostly focused on the forensics part of cyber security. Given the developments in our neighbourhood, we must rapidly invest resources to create offensive cyber capabilities, technologies and requisite manpower. Whatever governance structure we create/recommend, our focus must prioritise creation of resources and trained manpower first.

The floor was the handed over to the next speaker.

Mr Brajesh Singh, IPS

The very senior police officer began his presentation by stating that the MHA has no mandate for offensive cyber operations internally within the country or externally outside the country. Presently, India has not mandated any agency/organisation to execute offensive cyber operations. He made the following additional points during his presentation:

- So far a reactive approach has been the norm when faced with cyber- attacks to our critical infrastructure.
- Boundaries in cyberspace are blurred and hence the difficulty in assigning mandates. He cited Justice Hidayatullah who commented on how public order, law and order, crime and national security could be represented as concentric circles with the first being the largest.
- Creating jurisdictions and boundaries so necessary for bureaucratic functioning around such blurred areas is a flawed approach.
- There is danger in blindly copying models from other countries since our Constitution is different and we have evolved differently from others. Our governance practices are unique and we need to think of structures that are compatible with our practices.

Should India decide to create an offensive cyber capability, a clear mandate must be given to whichever agency or organisation is tasked for it. He cited the example of the FBI and its investigations involving penetration of a paedophile criminal gang (The Play-Pen case of 2014) when the court refused to accept evidence citing the ‘poisoned fruit’ meant that the tree on which it grew was itself poisonous. Given the nature of cyber warfare we must think in terms of a hybrid organisation rather than entrust offensive cyber capability to any existing agency. We need to do a gap-analysis to identify where we stand in today's world and then plan/create an organisation to defend our cyberspace.

Q&A: Closing Comments

Gen Panwar summarised what the three speakers had stated in their presentations and highlighted the following:

- It is important for the Defence Forces to see themselves as national security professionals rather than mere service officers.
- Cyberspace must be seen as sovereign territory and must be defended as such.
- NICMA as suggested by Gen P R Kumar and the hybrid organisation mentioned by Mr Brajesh Singh are very similar in concept.

The Q&A taken up for discussion brought out the following:

- The creation of a hybrid overall control structure was validated.
- There is a need to identify and differentiate critical infrastructure, offensive cyber operations and influence operations from each other. The governance structure created must be capable of dealing with all three areas of cyber operations.
- Attribution for various examples of cyber operations from the ongoing Russia-Ukraine war must be studied to understand which agency did what, where and when.
- Today, in the defence forces in India, the Army's Corps of Signals does have the capabilities for offensive cyber operations but not the mandate for it.
- Even when studying the Russia-Ukraine war we must bear in mind that none of this cyberwarfare existed even 10-15 years ago.

General Panwar brought the webinar to a close and invited General Moorthy to give his closing comments.

Conclusion

Congratulating everyone for a very informative and no-holds barred discussion on this very vital topic, the General thanked each one of the participants. He also informed the audience of CASA’s plans to formulate a paper based on all 4 webinars in the present series and send to the government for consideration in formulating our policies towards cyber security and offensive cyber capabilities. With that the webinar drew to a close at 6:45 pm IST.