Synopsis

Cyberspace Operations: Role of the Armed Forces

Webinar Summary Report

Publishing Date: 25 Aug 2022

Published By: The Current and Strategic Affairs Forum

Acknowledgements:

The webinar CASA WEBINAR SERIES: CYBERSPACE OPERATIONS Episode 4: Role of the Armed Forces was held on 24th August 2022 at 5pm 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:

Maj Gen Suresh Menon, VSM (Retd), Defence Cyber Security Expert

Air Vice Marshal Makarand Ranade, AVSM, VM, ACAS (Space)

Commodore MP Anil Kumar, NM, Cmde Safety, IN Safety Team

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 to 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 any other statutory body. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior permission of the CASA Forum.

Introduction

Lt Gen General Gautam Moorthy welcomed everyone to the 31st CASA webinar-the fourth and final one of the CASA series on Cyber Security being held on the very special occasion of the eve of our nation's 75th Independence Day. He went on to explain the purpose of the series as being to review the policies and strategies of major world cyber powers and compare them to India so as to draw relevant lessons. The four webinars were held in continuation, a fortnight apart. He gave a brief summary of the discussions and outcomes of the previous three webinars. He then introduced the panellists and the moderator for the present webinar and handed over the floor to the moderator Gen RS Panwar for the further conduct of the webinar.

Gen Panwar began by thanking Gen Moorthy and CASA for giving him this platform for the conduct of this webinar series. He welcomed all the three panellists as well as the distinguished members of CASA and others who had logged on for the webinar. He explained the four-part series was conceived primarily to focus on offensive cyber ops and cyber influence operations as the two are the main facets of cyber operations. He further went on to clarify that cyber operations could be classified as Cyber Deterrence, Cyber Defence and Cyber Influence Operations. He would therefore steer the discussions towards offensive cyber operations. He would not discuss Cyber Crime or Cyber Espionage. He wanted the focus of the discussions to remain on offensive cyber operations that can cause damage to or destroy critical infrastructure. He further explained his understanding that all infrastructure belonging to the enemy that are considered legitimate targets in a kinetic war should also be considered legitimate targets for cyberattacks. Therefore, use of cyber weapons must also conform to all international laws and conventions that govern kinetic operations to which India is a signatory. He repeated what he had said at previous webinars in this series ie that all cyber operations must remain within the domain of the armed forces. Gen Panwar further stated that based on the charter given to the armed forces in the physical domain, the same should also apply in the cyber domain and discussed the responsibilities of the armed forces, external agencies like R&AW, NTRO as well as the MHA. The charter for the armed forces is grounded in Article 51 of the UN Charter that provides for the right to self-defence.

The key difference between kinetic and cyber operations lay in the ability of countries to indulge in offensive cyber operations below the threshold of kinetic war known as 'Grey Zone'. In the absence of clear-cut laws and conventions, offensive cyber operations could become like the old 'Wild West' and therefore it is best if all offensive cyber operations are handled by the armed forces. Considering the huge spectrum of tasks in involved, he also opined that our Defence Cyber Agency (DCA) was too small and not adequately manned and compared it to the PLA's SSF and the assets available to it. He further revealed that in a peer comparison of 30 potential cyber powers, under the category of offensive cyber capabilities, China ranked fourth while we came in at 28! He therefore pitched strongly for rapid upgradation of the DCA to a Tri-Service Cyber Command. With this as a backdrop Gen Panwar gave out the three questions for which he hoped to get answers during the course of this webinar:

- Are the armed forces the best suited to carry out offensive cyber operations in cyberspace as part of their multi-domain operations? If not, then how should this charter be allocated?
- Assuming that a Cyber Command with several thousand personnel needed to be raised as a Cyber Force, how should we go about doing so?

- Views of the panellists on cyber influence operations which is slightly different from offensive cyber operations.

Gen Panwar than invited the first speaker of the day, Maj Gen Suresh Menon to present his views.

Maj Gen Suresh Menon

Gen Suresh began by thanking CASA, Gen Moorthy and Gen Panwar for giving him the opportunity to express his views. His mandate as he understood it was to cover the role of the ground forces (Army) in offensive cyber operations. In the time allotted to him he made the following points:

- Future conflicts would be characterised by the blurring of boundaries between kinetic and non-kinetic domains of waging war.
- Everything on the battlefield is digitally interconnected. These are vulnerable to attack during 'grey zone' operations too.
- Is there an overlap between grey zone and active operations?
- We are not able to learn much about cyber enabled operations or about offensive cyber capabilities of other countries. We are only able to infer from their overtly demonstrated capabilities. For the first time the Russian-Ukraine war gives us an opportunity to study the use of offensive cyber power in support of kinetic military operations. A simple Google search reveals a lot of information.
- Such studies may not be enough. We need to urgently review our policies for both offensive and defensive cyber power and the influence operation capabilities possessed by our rivals and where we stand with regard to them.
- Our review and analysis must include the following aspects:
  - Do they cover all aspects of cyber operations?
  - Can we consider offensive cyber operations as an option during any military operation?
  - If so, are we prepared and equipped for it?
- In answer Gen Suresh made the following points:

  - Our National Cyber Security Policy, 2013, is considered adequate It is however vague on the issue of offensive cyber power. Many agencies and ministries work in the cyber domain. Each has adequate manpower, a mandate and the required tools to carry out that mandate. We therefore, need to review and revisit all aspects to cover:
    - Adopt a pro-active approach towards employment of offensive cyber power. Should we await a cyberattack and then react or should we adopt a stance of cyber deterrence by a demonstration of our capabilities?
    - A second scenario where we counter attack by responding to a cyber-attack.
    - A third scenario wherein we launch a cyberattack in conjunction with kinetic operations when our national security is at stake in any manner.
- Our response to the above would be guided by certain key elements:
  - Strategists and Planners who would recommend if a cyberattack response is warranted.
  - Intelligence Agencies would have been continuously profiling likely targets like in any normal Intelligence Collection Plan. However cyber espionage comes under severe international criticism during peace time.
  - Coordination agencies would then analyse and optimise the resources available.
  - R&D agencies would design and develop the tools, cyber weapons and the methods of delivery.
  - Executive agencies who would finally carry out the plans followed by damage assessments.
- In all of the above, the armed forces have a role and therefore must be integrated into the effort at each stage.
- The ongoing Russia-Ukraine war has shown us the variety of targets that could be subjected to a cyberattack.

- The armed forces must remain involved in devising all protective measures for own infrastructure at both the strategic and tactical levels, especially when armed forces systems are integrated with civil systems and the vulnerabilities of both stand exposed for exploitation by the enemy. Examples were cited from the Russian-Ukraine war.
- Cyberattacks are a part of all-out wars and hence the armed forces must take the lead role in responding to a cyberattack, during pre-war grey zone activities or in actual combat situations.
- India's preparedness for cyberwar is suspect. There is urgent need for a well-defined policy that lays down clear-cut rules of conduct and responsibilities. We must decide whether our efforts for both control and execution must be centralised or only in control with operations being decentralised?
- The DCA must be upgraded to a Cyber Command that works closely with the NSA and others.
- There is need for better HR policies for cyber personnel by creating a Centre for Excellence at Army Headquarters to coordinate with DRDO and civil industry to create cyber tools and weapons.
- Emphasis on Intelligence collection and maintaining the confidentiality of our R&D into new cyber tools and weapons.

Gen Suresh Menon ended his presentation by quoting Lt Gen Rakesh Shukla from a previous episode by stressing the importance of statecraft over trade craft in the cyber domain.

Air Vice Marshal Makarand Ranade

The AVM while introducing his Power Point presentation stated that he would refrain from taking on some of the more sensitive issues. His talk together with his PP presentation contained the following:

- Explanation on what cyberspace operations involved- the main being it had no boundaries or timelines.

    - Ethics and codes for its waging too were blurred or undefined.
    - Grey zone was not to be seen as a prelude to war but was present at all times- before, during and after hostilities ended.
- Armed forces must be prepared and be suitably equipped to defend the nation’s cyberspace integrity and assets just as they do to preserve its territorial integrity.
- The structure created to carry out cyber operations was discussed and the slide included the DCA, Service Cyber Groups and the multiple agencies in the civil side. While explaining the slide the AVM too opined that the Tri-Service DCA needed to be reviewed and upgraded to a Cyber Command.
- The IAF Cyber Group and its activities was discussed next. He pointed out that the multiplicity of agencies dealing with cyberspace often led to duplication of efforts and wastage of scarce resources.
- Creating the expertise and retaining personnel with the desired skill sets was a challenge.
- Practical procedures needed to be evolved to create and operate the required infrastructure.
- The anonymity of the source from where the hardware & software was acquired was vital for cyberspace operations. Our present procedures need to be modified accordingly.
- Too many players compromise security. Different agencies hitting the same target at the same time will cancel each other out and the enemy will be alerted before any serious damage is done to him.
- The suggestions mentioned in the next slide included:
    - Synergy between agencies.
    - Whole of nation approach
    - Enhancement of cyber security awareness.
    - Maintain persistence in cyber operations.

In conclusion, the AVM summed it up in three words- Objectivity, synergy and whole of nation approach are key to maximise returns with the available infrastructure and resources.

General Panwar in his short comments on the AVM's presentation covered the following:

- Lack of morals and ethics in the cyber domain.
- The aspect of 'jostling' amongst agencies to enter the field of offensive cyber operations.

The floor was there after handed over to the next speaker- Commodore Anil Kumar.

Cmde Anil Kumar

The Cmde began by thanking CASA, Gen Moorthy and Gen Panwar for giving him the opportunity to state his views. At the outset he made it clear that he would restrict himself to the naval perspective of cyberspace operations and how it contributes towards naval operations. His presentation included the following points:

- The lack of defined and easily defined boundaries differentiated between war on land and the seas.
- Beyond 12 km from the shore (defined as territorial waters) the sea belongs to everyone and different classes and types of floating vessels operate on it.
- Naval vessels are restricted by the curvature of the Earth from being able to sight and target their long-range weapon systems. They therefore need networks and sensors to obtain target data beyond 80 to 100 km. These networks present a vulnerability that the enemy exploits to its advantage. To maintain our effectiveness, we need to protect and secure our networks from enemy actions to degrade/destroy them.
- Collecting and integrating data from all available sources is termed as Maritime Domain Awareness (MDA). Given the importance of networks to its operations, cyberspace and its use or denial to the enemy is part of the Navy's operations.

- The MDA uses data not only from military sources but also needs data from commercial sources like satellite data for commercial ship's identification and data pertaining to the international movement of aircraft along designated routes. For the Navy Cyber warfare includes civilian domains apart from the purely military. The Navy has to deal with all systems and infrastructure as part of its MDA.
- Cmde Anil Kumar was of the opinion that the use of the term "deterrence" in cyber operations was wrong since deterrence of any kind would demand demonstrated capability. Our mind sets in this regard reflects the old style of kinetic operations. Cyberspace is borderless and limitless just like the oceans and seas. Hence in offensive cyber operations differentiation of targets as strategic or tactical has no meaning. He further expanded on this theme by citing the example of a satellite ground station that provided satellite communications for a vital plant; disrupting the electric supply to the ground station could immobilise the plant. Thus a strategic target was being approached via a tactical target and its not possible to demarcate between the two.
- Offensive cyber capabilities are an ongoing process and cannot be limited to only hot-war periods.
- The Cmde also reiterated the point about our fragmented approach, too many agencies and the lack of coordination as had the previous speakers.

Conclusion

In conclusion Cmde Anil Kumar made the following points:

- Cyber warfare is to be considered as an extension of conventional warfare.
- The Navy must continue to build capability to ensure the security of its cyber infrastructure.
- The Navy needs to induct and train cyber warriors in large numbers.

- The charter of the DCA must be expanded to conduct all offensive cyber operations against enemy cyber capabilities and infrastructure.
- There is a need for clear policies and mutual trust between agencies.

The end of the presentations by the speakers was followed by a brief overall summing up by Gen Panwar before moving on to the questions and answers section of the webinar.

Questions & Answers

The first question to be taken up was from **Gen Daljeet Singh** who wanted to know as to at what level is cyber intelligence shared and how is it ensured that it reaches the agency best suited to tackle it.

Gen Suresh Menon's answer to the question was that to get an effective cyber enabled operation going it was vital to have effective cyber intelligence. The intelligence had to be collected well in time by tapping numerous sources through cyber espionage. If too many agencies home on to the same target at the same time, chances are that the target would get alerted and devise the means to thwart the attack. Thus timing and the specification of the agency to carry out the intelligence collection as well as the agency to carry out the attack must be coordinated at the highest levels.

The next question was from **Sankesh Khadkare** who wanted to know if any efforts have been made to conclude an international cyber law. **AVM Ranade** answered that while numerous efforts are going on since long, no agreement has been reached as yet since no country would like to be tied down right now. **Cmde Anil Kumar** added that it was difficult to draw a boundary between cyber crimes and offensive cyber operations. There is no consensus between countries on this. The issue of attributability also holds up this consensus since no attacker will use his own or an identifiable IP address and always uses some other IP address. **Maj Gen Suresh Menon** was of the opinion that India has already come a long way in the field of cyber and space operations and instead of approaching different countries separately/bilaterally we must join an international grouping like the 64-member (July 2020) Budapest Convention that is in existence since 2001. We could then use that forum to approach individual countries. It was pointed out by **Gen RS Panwar** that India is not a signatory to the Convention and that the Convention applies to cyber crime and not offensive cyber warfare.

The next question was from **Col M K Channan** who wanted to know as to how the Services are training their cyber warriors- centrally or service wise? **Gen Suresh Menon** opined that cyber training had to be conducted at three distinct levels- cyber warrior level, the middle level and the higher level. Such training existed in all three Services. However, there is a need for a Joint Services Cyber Training Establishment. **AVM Ranade** spoke about how the IAF JAWC conducted training for all three Services. Regular exchange of best practices does take place but true joint training is still a work in progress. **Cmde Anil Kumar** stated that student exchanges between Services are already taking place. Cyber defence training is also important depending upon which service is using which equipment. **Gen R S Panwar**, being the ex-Comdt of MCTE, stated that Cyber operations courses for all the three Services is going on since some time now. We are fully geared up to run our own offensive cyber operations training. However, as the spectrum of skill sets needed is so vast we may have to approach the civil sector for some types of expertise which too over time, would become redundant and all offensive cyber training would become a purely Services affair.

The last question also from **Gen Daljeet Singh** sought to know how coordination is to be achieved between offensive cyber operations and kinetic operations at both the strategic and tactical level? **Cmde Anil Kumar** stated that for the navy all operations are network dependent, hence to differentiate between tactical and strategic operation is not possible. Coordination at the highest level (DCA) is a must for offensive cyberattacks as already covered.

Gen Panwar keeping the time factor in mind concluded the webinar at this stage after thanking all the panellists and those who had logged on before giving the last word to Gen Gautam Moorthy.

Conclusion

Gen Gautam Moorthy thanked everyone of the panellists for a fascinating webinar that brought in so much knowledge to all the participants. He had a special word of thanks for Gen RS Panwar for curating the entire four part series so painstakingly. The series has been an eye opener for most CASA members and to those who joined in. He would request Gen Panwar to pick up salient points from the summaries on all four episodes and prepare a draft a note for the Govt from CASA for taking whatever action they deem fit. He ended by thanking Mr Mahadevan Shankar from Australia who with the IT Team led by Ms Barnali have rendered yeoman service in taking care of all coordination and back end work for CASA and its YouTube channel.