Synopsis

Conflicts in Cyberspace: Strategies & Structures of Major States

Webinar Summary Report

Publishing Date 07 Jul 2022

Published By: The Current and Strategic Affairs Forum

Acknowledgements:

The webinar **CASA WEBINAR SERIES: CYBERSPACE OPERATIONS Episode 1 Conflicts in Cyberspace: Strategies & Structures of Major States** was held on 03 July 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:

Panelists:

Dr (Prof) Nishakant Ojha, Chief Strategic Officer-BECIL

Mr. Glenn Murray, Former MD & CEO Sapien Cyber, Australia.

Lt Gen (Dr) Rajesh Pant, National Cyber Security Coordinator, Prime Minister's Office, Govt of India.

Moderator: Lt Gen (Dr) RS Panwar, AVSM, YSM, 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, (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:

Introduction

Lt Gen Gautam Moorthy , PVSM, AVSM, VSM, (Retd), founder of CASA Forum began the 28th webinar (7th 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. The main purpose of this four part series was to examine the status of cyber security in some of the leading countries in the world and compare them to what we have achieved thus far and to imbibe useful lessons therefrom. Special attention would be placed on offensive operations and cyber influence operations. Without further ado General Gautam handed over the stage to General (Dr) RS Panwar (Retd), also a distinguished Fellow, USI, to conduct further proceedings of the webinar.

Gen Panwar started the discussion by first thanking Gen Moorthy and the CASA Forum for organising such an eminent panel of speakers and for choosing him to moderate the discussion.

With a view to setting the stage for the webinar, the General began by giving us a brief overview of the increasingly potent and strategic effects being achieved by many players in cyberspace. He began by citing the ongoing Russia-Ukraine war which is the first such war where cyber capabilities were exploited in large scale by both the belligerents. Such a scale of usage of cyber would have been unthinkable a few years ago. He also referred to significant cyber-attacks of the recent past- the 2010 *Stuxnet* attack on Iranian nuclear centrifuges that took out approx. 20% of Iran's centrifuges. This attack has been widely attributed to the US and Israel and for the first time led to physical destruction of the target via a cyber- attack. A second major cyber-attack was in 2015 when the Russians took out the Ukrainian electricity supply network. This was the first time an adversary's infrastructure was attacked and rendered inoperable. The third example cited pertained to the alleged influence operations carried out by Russia during the 2016 US Presidential elections. Hilary Clinton's loss to Donald Trump was widely suspected to be the result of Russian influence ops via cyberspace. The 2017 *NotPetya* malware attack attributed to Russia is supposed to have caused 10 billion USD globally & is the costliest malware attack till date. Just before the launch of the special military operations against Ukraine, Russia is suspected to have used *Wiper* malware to destroy thousands of satellite modems used by customers of a communications company *Viasat*, which served many European customers besides the Ukrainian military. This attack disrupted Ukrainian C&C networks during the initial stages of the invasion. This was the first time such large scale offensive cyber- attacks were launched in support of conventional military operations by the attacker country against the defender country.

From the examples cited, Gen Panwar expected the panellists to answer the question as to what is stand of International Law on the legality of offensive cyber operations by one country against the other. Secondly, in what manner and under what conditions could a victim state respond to such attacks? So far clarity has eluded us on how cyber- attacks could be also clubbed with other conventional

forms of attacks on the sovereignty of the victim state, despite many UN initiatives up to last year. Intense debates are ongoing in various international for a for a treaty regarding the treatment of Cyberspace as a global commons much like the oceans or to fragment the global nature of cyberspace through artificially created cyber walls that insulate one country from another etc.

Liberal Democracies that believe in the free flow of information are averse to granting nations sovereignty over their cyberspaces. Against this backdrop, countries across the world have shown great agility in evolving structures and organizations to deal with threats to their cyber security. He cited the raising of the US Cyber defence structures from as far back as 2010 with constant revisions ever since. In 2018 the US Cyber Command was elevated to a Unified Combatant Command, one of the 11 commands of the US Dept of Defense. China raised its PLA Strategic Support Force (SSF) during its reorganization in 2015 The SSF centralizes most PLA space, cyber, electronic and psywar capabilities. Russia's organizations for cyberwarfare are arguably the best in the world today. The Russian Federal Security Service (FSB), Foreign Intelligence Service (SVR) and the General Staff Main Intelligence Directorate (GRU) are the primary centres overseeing its information security and cyber operations. In the UK the cyber security mission is led by the National Cyber Security Center (NCSC) which is a part of the GCHQ with organizations being established as recently as last year. Australia issued its national security strategy in 2020. Its cyber security organs such as the Australian Cyber Security Center (ACSC) function under the Australian Defense Force HQs, Signals Directorate since 2018. It is a part of the Australian Security Intelligence Organization and is a joint responsibility of the MOD. The strategies of all these five states are their clear intention to develop and use offensive cyber capabilities to thwart all forms of cyber security threats.

We in India expect our national cyber security strategy to be announced soon. Though our National Cyber Security Policy was issued in 2013 we have just set up the National Cyber Coordination

Center (NCCC). Our Computer Emergency Response Team (CERT-IN or ICERT) under the Min of Electronics and IT of the GOI has been in existence since 2004 under the Information Technology Act 2000.Among the many organizations newly set up is the Defense Cyber Agency of 2019 as a Tri-Service command of the Indian Armed Forces. As of 2021 all three services have established their respective Cyber Emergency Response Teams (CERTs). Gen Panwar then turned to the panellists to put forth their views and suggestions with regard to formulating an offensive-defensive cyber security stance as already briefed by Gen Gautam Moorthy in his opening remarks.

Professor Nihakant Ojha

After thanking CASA and Gen Panwar for giving him the opportunity to speak on this most important topic, the professor made the following points basically confining himself to his area of expertise in combating cybercrime:-

- The very nature of future warfare is changing from physical platforms like tanks, guns, ships and aircraft to an entirely different dimension that is intangible and unseen.
- Every major nation is involved in securing its cyber space and developing offensive capabilities to degrade its opponents in cyberspace thereby interfering in its command and control abilities to direct and exploit its physical forces on the battle field.
- Data is anonymous and moving between countries in a manner wherein we are still not quite clear as to how we can regulate and monitor it.
- Our foes do not have to launch attacks from their own soil. The anonymity of data and the use of the Cloud allow an adversary to launch attacks against us from anywhere.

- The difficulties in securing evidence and conducting search and seizure operations have undergone massive changes with the advent of large scale cyber- crime.
- European countries have banded together and created the General Data Protection Regulation (GDPR) by expecting its members to take “appropriate” actions to ensure cyber security measures while processing personal data using technical and organizational measures. Its existence has allowed all member countries to exchange and work with all forms of data including biometric across national borders.
- Reference to the Budapest Convention on Cybercrime enacted in 2001 and made effective from 2004 was made and it was informed that India along with Brazil never became a member of it on the plea that we were non participants while it was being drafted!
- Even though 66 or 68 countries have signed on to the Budapest Convention, UK, an earlier signatory, is now moving away and is in the process of creating its own GDPR. Russia too is keeping away.
- India still lacks a robust environment to enforce and practice cyber security. Presently 43 countries have signed on to the Council of Europe Convention on Cybercrime as of 2006. A UN treaty on cybercrime is still being formulated as of Dec 2019.
- Masking of attacks prevents an investigator without access to traces and data from the cloud from progressing his investigations. For getting such access, India must have multi-level treaties with many countries.
- Interpol is not a very robust source for information on cybercrime since countries do not allow it access to the data they have about their citizens in the absence of any protocols that ensure data safety and protection of privacy of their citizens.
- Lacking a universal data sharing protocol, India has concluded bilateral data sharing arrangements with about 18 countries till date. This is a slow process and not an ideal method for sharing data on a real time basis.

- The suggestion was not to wait for a universal treaty on cybercrime to come about but to speedily conclude bilateral arrangements with maximum number of countries.
- Another suggestion was for India to take the lead in formulating a GDPR type of arrangement for South Asian countries, ME countries, ASEAN countries etc. so that we can build up a robust regional anti cybercrime network where data could be exchanged in real time.
- The example was cited of a consortium being developed between Russia and Iran on these lines. Once small arrangements with few like- minded countries are successfully created across the globe then it will become easier to integrate A to B to C etc. to eventually form a global network.

Mr Glenn Murray

He began by thanking everyone for the opportunity to interact with our august forum and recalled having spoken at many similar fora around the world. He began by giving an explanation as to why cyber is now being considered the fifth domain of warfare after the traditional domains of Air, Land, Sea, and Space. Many think that cyber can be the main domain for future warfare but currently it is a domain that makes war fighting capabilities in other domains more efficient and lethal. He cited the impact of the number of cyber- attacks taking place in the context of the ongoing Russia-Ukraine war to buttress his observation. This war has shown us that a cyber-attack designed to hit one person goes out into cyberspace and anyone within that space gets affected. That is why a cyber-attack is termed as a virus since once released it spreads throughout the world. There are no geographical boundaries here. The other significant aspects he covered in his presentation included:-

- Cyberattacks happen from anywhere in the world and attribution of that attack is often difficult.

- Critical infrastructure of countries is vulnerable to cyberattacks. This is the new soft underbelly of nations that foes can attack.
- The infrastructure itself need not be attacked but a supply chain linked to that infrastructure can be attacked.
- He cited the acute shortage of cyber proficient personnel to tackle the humongous numbers of malware being identified daily as well as the number of cyberattacks being launched daily. By citing these huge numbers he was making the point that this is not one country's problem but it is a global problem.
- Australia set out on the path of amending security laws to deal with cybercrime. The attempt was to secure critical infrastructure and its linked supply chain from being attacked by cybercriminals or during the course of cyberwarfare.
- If planning to disable a military base the opponent will look at disrupting vulnerable supply and logistics services to that base- water supply, hospital services, etc. The base itself need not be subjected to a costly military attack. The whole meaning of critical infrastructure has undergone change- from sewage and treatment plants to education systems – practically every aspect of human life has now become a part of critical infrastructure.
- New legislation defines the detection and responses to any cyberattack launched from anywhere. We as yet do not have any in-built cyber security devices in the equipment that form these critical infrastructures.
- A new convergence is emerging between the IT (information Technology) and the OT (Operational Technology) of these devices that go into critical infrastructure.
- Cyber security implies three things- the confidentiality of the user; the integrity of its use and its availability to the user.
- Countries are up against the ability of their foes to go out and hire a company to design and launch a malware against its critical infrastructure. The threats are manifold and multiplied across domains.
- The importance of data sharing between countries was again re-emphasized in conclusion.

Lt General Rajesh Pant, PVSM, AVSM, VSM (Retd)

The General who is the National Cyber Security Coordinator for India in the PMO began by complimenting CASA for organizing this series of webinars that seek to bring greater awareness to the environment of the issues related to cyber threats and the methods to mitigate them. He made known his intention to cover the facet related to "strategies & structures" of the conflicts in cyberspace as he would cover other issues in the forthcoming webinars of the series. In his presentation, the following points were stressed upon:-

- Strategies and structures form the most important aspect for ensuring a safe and secure cyber space.
- Referring to Gen Moorthy's opening remarks about India rising to the 10th position from the 47th, he touched upon the vital necessity of having a well-defined National Cyber Security Strategy in place for the governance of cyberspace.
- We are currently witnessing a shift from cyber security to cyber power.
- The style of the strategy and structure is governed by the type of government creating them. In an autocracy like China there will be a very strict direct control over all aspects of cyber security. The system is designed to directly operate under President Xi's control. On the other hand, in democracies like the US and UK there is an ecosystem where cyber security professionals move around between their government job, private industry and academia. Even their budgets are prepared by consultants in the private sector before it is tweaked and issued by the government.
- The time taken by a country to address cyber security incidents too has a bearing on good governance of cyber security. In the case of the Colonial Pipeline hack by a criminal cyber group known as *Darkside* in the US on 05th May 2021 which led to widespread fuel shortages on the East Coast, the US came out with a presidential order on 12th May 2021 as to how the nation would henceforth deal with such cyber- attacks. In our case,

things happen very differently since many ministries are involved and all work in their own silos thereby imposing considerable delay in decision making.

- India was one of the first nations with our IT act in 2000 that was amended in 2008. Our Cyber Security policy had come out in 2013 though work on it had begun in 2011. The policy of 2013 is the framework under which India has created cyber security organizations. Another example is the I4C- Indian Cyber Crime Coordination Centre that acts as a nodal point in combating cyber-crime was created in 2018 by the MHA.
- India has some organizations that are external facing, some that are internal facing and yet others that are both. We created our Defense Cyber Agency as a part of the Integrated Defence Staff (IDS) in 2018. Each Service then has its own Service Cyber Groups. There are separate entities under the DRDO that also handle cyber security. All these organizations under the MOD are therefore both internal and external facing. Exclusively external facing organizations are like the NTRO operate under the MEA, R&AW etc. The internal facing ones are the ones under the MHA like the I4C, CERT-In (Computer Emergency Response Team-India), National Cyber Coordination Center, HTQC (Hardware Testing and Quality Control) a standardization scheme for cyber security. In the ministries we have the CSIR Teams- Cyber Security Instant Response Teams.
- In our states too we have state level CERTs looking after their own local or wide area network security under the guidelines issued by the national level bodies.
- Referring to Australia raising its tally of critical infrastructure from 4 to 11, the General posed a counter question as to what is not critical infrastructure today. In India we had identified 7 sectors which we considered critical. Post the pandemic our dependency on digital technologies has increased exponentially and today it is difficult to classify anything as critical or non-critical.

- In the legal sphere, India being a non-aligned nation focuses on strategic partnerships and has tie-ins with 36 nations as part of the International Counter Ransomware Initiative 2021. Within the QUAD, apart from the 9 verticals there is a Quad Senior Cyber Group. At the regional level there are numerous cyber security initiatives like in BIMSTEC, ASEAN, SCO etc. where India is participating. India has always believed in UN lead initiative which is why we are not a part of the Budapest Convention.
- At the UN Level it is very difficult to bring about consensus since each word in a law/convention is contested.
- The General concluded by a brief mention of other aspects of cyber security that touched upon:-
    - Education & awareness of Cyber threats.
    - Capacity building of the work force.
    - Predictive analysis of threats.
    - Audit of risk assessments.
    - Data sharing on threats.
    - Incident response &recovery
    - Cyber diplomacy
- The paper on a whole of government approach towards cyber security based on CBDR principles (Common but Differentiated Responsibilities) is awaiting approval at the CCS level.
- Guidelines for cyber security have already been issued to the telecom and power sectors.

Questions & Answers

There were many questions of which the moderator chose one by Brig Sanjay Agarwal who wanted to know the three things that the government could do faster, better and more focused. The answer from Gen Rajesh Pant listed :

- Faster approval of the National Cyber Security Strategy.
- More spending on cyber security education and awareness.
- Encourage indigenous cyber security products.

Mr. Rishi Atreya and Col Manoj Channan wanted to know if cyber security protocols existed in the nuclear establishments, ATCs, Metros etc. Gen Pant assured them that they did exist and are being constantly improved. In the digital world as well as in the post pandemic world there are two mantras for security- ie Personal hygiene and Cyber hygiene.

The three hard truths of the cyber world as listed by Gen Pant are:

- Vulnerabilities will continue to exist.
- Attacks will continue to take place.
- Attribution of attacks will be as difficult as they are today.

The webinar closed with the moderator and Gen Gautam Moorthy thanking all the participants, panellists, Mr. Shankar Mahadevan and the backup team.