India's new Defence Cyber Agency—II: Balancing Constitutional Constraints and Covert Ops?

CCG NLU, DELHI *on* OCTOBER 4, 2019

8 MINUTE READ

By Gunjan Chawla

In our previous post on India's cyber defence infrastructure, we discussed the new Defence Cyber Agency (DCA), one of the three tri-service agencies announced at the Combined Commander's Conference last year. Under the leadership of Rear Admiral Mohit Gupta, appointed as its head in April this year, the DCA is expected to serve a dual purpose—first, to fight virtual wars in the cyber dimension and second, to formulate a doctrine of cyberwarfare. In doing so, it is expected to contribute towards a cybersecurity strategy policy which integrates cyberwarfare with conventional military operations. In June, Lt. Col. Rajesh Pant, the National Cyber Security Coordinator announced that the new cybersecurity strategy policy will be released early in 2020.

The utilisation of cyberspace for military operations holds the potential to infuse a certain 'jointness' among the Army, Navy and Air Force. Lt. Gen. (Retd.) DS Hooda pointed out the herculean task that lies ahead of Rear Admiral Gupta– "to find a way to work around vertical stovepipes into which the three services have enclosed themselves". The tri-services nature of the DCA could potentially compel the three services to share operational information and resources on a regular

basis, which would further help to formulate a comprehensive and robust cyber defence infrastructure for the country.

From Coordination to Integration

Since the appointment of Rear Admiral Gupta as the head of the DCA, the Government has made only one announcement that has a significant bearing on its role and functioning. The Prime Minister's announcement in August about the creation of a new position of a Chief of Defence Staff (CDS) is a welcome step and is expected to catalyse the move from coordination to integration in the operations of the Army, Navy and Air Force and the operationalization of the three tri-services agencies. The burden of this herculean task entrusted to Admiral Gupta will now presumably, be shared by the CDS.

Unlike the Chairman of the Chiefs of Staff Committee (COSC), which is an additional position occupied by the senior-most officer among the three Chiefs, who serves as *primus inter pares*, or the first among equals – the CDS will be above the three chiefs, and act as a single-point military advisor to the Government and coordinate long term planning, procurements and logistics of the three service. However, there is long way to go between the announcement of this reform and its actual implementation.

Each of these two announcements – the setting up of the DCA, as well as creation of the CDS post necessitates certain changes in the legislated structure of the three wings of the armed forces for two distinct, but related reasons.

First, because the present legislations that govern the composition and structure of the three wings do not offer sufficient guidance for routine operations conducted jointly by the three wings, nor do they envision an officer superior in rank to the Chiefs of the three services.

The Central Government has the power to make rules under S. 191(2)(l) of the Army Act, 1950 to provide for the relative rank of the officers, junior commissioned

officers, petty officers and non-commissioned officers of the regular Army, Navy and Air Force when acting together. S. 189(2)(l) of the Air Force Act, 1950 also confers the same power with respect to the Air Force. However, such a provision to make rules is conspicuous by its absence in the Navy Act, 1957. S. 184(2) of the Navy Act, 1957 confers upon the Central Government, the power to make regulations to provide for the relative rank, precedence, powers of command and authority of officers and sailors in the naval service in relation to members of the regular Army and the Air Force, but this makes no specific reference to the situation when members of three forces are acting together. Instead, S. 7 of the Navy Act provides that

> *"When members of the regular Army and the Air Force are serving with the Indian Navy or the Indian Naval Reserve Forces under prescribed conditions, then those members of the Army or the Air Force shall exercise such command, if any, and be subjected to such discipline as may be prescribed [under this Act]."*

Additionally, the provision states that it cannot be deemed to authorise members of the regular Army or the Air Force to exercise powers of punishment over members of the Indian Navy. This provision is rooted in the colonial history of our naval laws, as it was felt that as the conditions of service at sea differed from that on land and because the erstwhile Navy (Discipline) Act, 1934 differed in many respects to the law relating to the Army and the Air Force, no attempt should be made to assimilate the revised Navy Act in other respects to the law relating to the Army and Air Force. Oddly enough, such unique demands of the sea as a theatre of war that prevented assimilation of the three wings are amplified in the case of cyberspace as a distinct, but connected theatre of war and deserve appropriate recognition in law – in a manner that encourages integration.

The existence of such disparate provisions on the conditions of service of members of the three forces when acting together could foreseeably, prove to be a hurdle in implementing integration for the creation of tri-services agencies. Additionally, the

rank, powers and office of a Chief of Defence Staff is not defined or recognized in either of the three Acts. Should such a post be created by the issuing of rules or regulations by the Central Government, they would have to be laid before Parliament, pursuant to S. 185 of the Navy Act, S. 193A of the Army Act and S. 191A of the Air Force Act. In the current state of the law, it is unclear which of these three Acts could be invoked to formulate rules to create such a post in a manner that facilitates such integration.

The second reason is that the advent of cyberwarfare has brought nation-states into what can be described to as the fourth dimension of warfare—military operations that were until recently restricted to the physical domains of land, sea and air have now entered the virtual realm. The growing risk of cyber espionage and breaches of information security of Government agencies, like the ones in 2008 highlight the urgent need for such coordination to ensure prompt, proportionate responses. Thus, we need to prepare a framework not only because the conduct of hostilities now requires unprecedented, seamless integration between the three forces, but also because these hostilities will be conducted in an entirely new dimension, which possesses certain unique characteristics and limitations as a distinct operational theatre for military action.

Accordingly, the question of whether the Government would treat the breach of 'India's cyberspace' by foreign actors, at par with violations of our sovereign territory, airspace or territorial waters must be answered in the affirmative.

At the minimum, this should include, (1) defence communications and operational networks, (2) security of the Government communication networks (3) security of classified and privileged information and (4) critical information infrastructure (CII) should be considered constituent components of our sovereign-protected cyberspace. Since the promulgation and notification of the Information Technology (Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2014, CII falls within the purview of the NCIIPC. Rule 3(4) excludes systems notified by the Ministry of Defence (MoD) as critical information infrastructure. To enable this legally, (1), (2) and (3) ought to be

notified by the MoD as such, and explicitly entrusted to the DCA for appropriate action for their protection with appropriate directions.

Constitutional Constraints on Waging War in Cyberspace

Indeed, our cyber forces have been fashioned as an 'agency' and not a 'service' unto themselves, but contemporary research indicates that with appropriate training and experience, the agency is expected to provide the base for, and grow into a full-fledged Cyber Command. However, we cannot rely solely on emergency powers under Article 352 of the Constitution as the starting point of our analysis of the legal framework that applies to India's defensive operations in the cyber realm. Such an analysis leads us to arguments in favour of invoking the fundamental duties of citizens Article 51A for boosting the recruitment of cyber warriors. Such a system can only remain functional, if at all, on an *ad-hoc* basis. The domain of Parliamentary action cannot reasonably be restricted on the premise that cyberattacks against Government agencies are the 'new normal'. The State must prepare for the eventuality that *ad hoc* arrangements set up as necessary reactions to security breaches need to be institutionalized in law. It is not sufficient to assert that the exigencies of cyberwarfare make it inefficient to seek Parliamentary sanction. And so, the military establishment that engages in hostilities with foreign actors in cyberspace, whether fashioned as an agency, service or command, should be read into the phrase 'any other armed forces' of Entry 2 of Schedule VII.

When it comes to the defence of India, the Constitution is unambiguous.

Article 53(2) of the Constitution declares that the supreme command of the armed forces of the Union shall be vested in the President and the exercise thereof *shall* be regulated by law. (emphasis added) Article 53(3)(b) also states that nothing in this Article shall "prevent Parliament from conferring by law functions on authorities other than the President".

Article 246(1) of the Constitution vests legislative powers in the Parliament. The provision refers to Schedule VII, which identifies specific areas upon which Parliament is entitled to legislate in the national security domain. These areas include the following:

1. Entry 1 refers to "the Defence of India and every part thereof including preparation for defence and all such acts as may be conducive in times of war to its prosecution and after its termination to effective demobilization."
2. Entry 2 places "naval, military and air forces; and any other armed forces of the Union" within the legislative competence of Parliament. To this effect, The Army Act and Air Force Act were adopted by the Parliament in 1950 and the Navy Act in 1957.
3. Entry 7 refers to "Industries declared by Parliament by law to be necessary for the purpose of defence or for the prosecution of war". Although the IT sector is treated as a strategic sector by the Government, no such law has been enacted by Parliament.

The language of Article 246 indicates that Parliament is competent to legislate on these issues. However, the use of the word 'shall' in the language Article 53 suggests that Parliament is duty-bound to enact such a law. This can also be inferred from the language of Article 73(1) of the Constitution, which states that "The Executive power of the Union shall extend –(a) to matters with respect to which Parliament has the power to make laws". This makes it clear that the exercise of the Executive power is made conditional on the legislative competence of the Parliament, and not *vice versa*.

So far, no specific legislation has been forthcoming from Parliament to approve or regulate the exercise of the executive power to engage in cyberwarfare, nor has the Government proposed any. However, the promulgation of a Cybersecurity Act that would cover not only various cyber-related crimes, offences, forensic and policing, but also, have enabling provisions for cyber war and defences against cyber war has been proposed by other think tanks, and even Admiral Gupta himself.

Thus, the power to make preparations for prosecution of war in cyberspace should be backed by Parliamentary sanction. Such an enactment would also help clarify many other questions and streamline the contours of India's cybersecurity infrastructure and institutions. For example, the domain of authority of the DCA and its relationship with its civilian counterparts including the National Cyber Security Coordinator (NCSC) and the Indian Computer Emergency Response Team (CERT-In) remain unclear. With proper consideration and consultations, the setting up of the DCA could potentially open the doors to enhanced, perhaps even institutionalised civilian-military cooperation that begins in cyber operations and permeates into conventional operations as well.

Two new domains—space and cyber—enabled by high technology, offer unprecedented opportunities for enhanced communication and coordination among wings of the armed forces in all theaters of war, and be used as force multipliers for intelligence analysis, mission planning and control.[i] Given their crucial role in intelligence analysis, foreseeably, the Government could model the agency as one that 'cyber-supports' military operations, but with a greater emphasis on covert operations rather than conventional warfare. In such a scenario, we may expect that its structure and functioning would be shrouded in secrecy, analogous to the Research and Analysis Wing (R&AW) or the Intelligence Bureau (IB). This means that the DCA would work closely with the Defence Intelligence Agency (DIA). While structures analogous to existing intelligence agencies could potentially allow greater freedom of action for cyber operations, it could also compromise the DCA's potential to draw upon civilian expertise.

In the interest of widening the pool from which the DCA recruits and trains its cyber-warriors, a proper legislative mandate would go a long way in establishing and strengthening strategic partnerships with the private sector, where most of the country's tech talent is currently employed.

[i] As an aside, it is pertinent to mention that India's entry into the fifth dimension i.e. space remains debatable— even after carrying out the first successful test of anti-satellite (ASAT) weapon and being in the process of setting up a Defense Space Agency, our policies still espouse the principle of peaceful uses of outer space.

*

This article was first published on CCG-NLUD's blog, its been cross-posted with prior permission.

Support our journalism:

For You

- Sign up for our Daily Newsletter to receive regular updates
- Stay informed about MediaNama events
- Have something to tell us? Leave an Anonymous Tip
- Ask us to File an RTI
- Sponsor a MediaNama Event

DISCOVER MORE

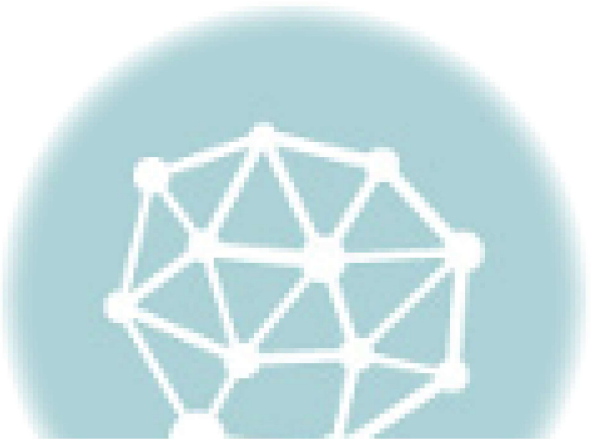
cybersecurity | cybersecurity policy | defence cyber agency

Related Posts:

India's Cybersecurity Strategy Policy in 2020, says National Cybersecurity Coordinator Rajesh Pant

Why Maj. Gen. Vombatkere has challenged Aadhaar Amendment Act in the Supreme Court; On WhatsApp and Traceability

How India should deal with cyber attacks on critical infrastructure



National Security Council invites comments on National Cyber Security Strategy 2020 until Dec 31

Google Chrome to gradually block all 'mixed content downloads'

Google Nest makes two-factor authentication mandatory starting spring

MEDIANAMA

MediaNama is the premier source of information and analysis on Technology Policy in India. More about MediaNama, and contact information, here.