# Does India have offensive cyber capabilities? — by Gunjan Chawla

CCG NLU, DELHI *on* JULY 11, 2020

4 MINUTE READ

*By Gunjan Chawla*

While we await the release of the much-anticipated National Cyber Security Strategy 2020 (NCSS), a very significant development in the domestic regulation of foreign trade — by way of an amendment quietly inserted by the Directorate General of Foreign Trade (DGFT) on 11.06.2020, contains an extremely significant indication for the direction we can expect the NCSS document to take.

The Foreign Trade Policy (FTP) is formulated and notified by the DGFT under the statutory authorization provided by Section 5 of the Foreign Trade (Development and Regulation) Act, 1992. The FTP regulates among many other things, the import and export of certain types of technologies. It also enforces in compliance with India's obligations under international export control agreements like the Wassenaar Arrangement.

The latest FTP was formulated for the period of 2015-2020, and last revised in December 2017. The FTP is published in three parts — (i) the Policy Document (ii) Handbook of Procedures and (iii) the ITC-HS Classification.

The Indian Trade Classification based on Harmonized System of Coding, better known as the ITC-HS classification system uses eight digit codes to describe and

categorize items subject to regulation. Schedule I of the ITC-HS deals with import policy, while Schedule II of the ITC-HS describes the rules and regulations related to export policies.

Appendix III to Schedule II contains a descriptive list for the category of SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technology). The SCOMET list itemises goods, services and technologies used for civilian and military applications, including also some 'dual-use items' for export control regulation.

Category 6 of the SCOMET list is the Munitions list, while Category 8 relates to "Special Materials and Related Equipment, Material Processing, Electronics, Computers, Telecommunications, Information Security, Sensors and Lasers, Navigation and Avionics, Marine, Aerospace and Propulsion".

Under 6A021, which falls under the Munitions list, "software" subject to export control regulations is now defined to include,

> ***"Software" specially designed or modified for the conduct of military offensive cyber operations;***
>
> *Note 1 6A021.b.5. includes "software" designed to destroy, damage, degrade or disrupt systems, equipment or "software", specified by Category 6, cyber reconnaissance and cyber command and control "software", therefor.*
>
> *Note 2 6A021.b.5.* ***does not apply*** *to "vulnerability disclosure" or to "cyber incident response", limited to non-military defensive cybersecurity readiness or response.*

Note 2 under 6A021 appears as a welcome relief to the information security research community by keeping vulnerability disclosures beyond the purview of export control regulations. However, it is relevant to mention that "vulnerability

disclosures" and "cyber incident response" had already been excluded from the purview of export control restrictions in an earlier amendment to the SCOMET list on 03.07.2018. However, this exception appears not under category 6, but category 8, as an exception to head 8E401 Computers (Technology). Therefore, the exception carved out under 6A021 by the 11.06.2020 amendment is a mere reiteration of the exception already contained under 8E401, inserted by the amendment of 03.07.2018, which reads as follows:

> *c. "Technology" for the "development" of "intrusion software".*
>
> *Note 1: 8E401.a and 8E401.c* ***do not apply*** *to 'vulnerability disclosure' or 'cyber incident response'.*
>
> *Note 2: Note 1 does not diminish national authorities' rights to ascertain compliance with 8E401.a and 8E401.c.*
>
> *Advertisements*
>
> *Technical Notes:*
>
> *1. 'Vulnerability disclosure' means the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.*
>
> *2. 'Cyber incident response' means the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident.*

Therefore, our export control regulations may have been cognizant of and sensitive to the need for ensuring free flow of data and information with regards to vulnerability disclosures and cyber incident response systems since 2018. It is also

relevant to mention that the previous version of this list dated 24.04.2017 made no references whatsoever to 'cyber incident response' or 'vulnerability disclosure'.

The June 2020 amendment to the SCOMET list is a highly significant development, as this is the first official document that strongly suggests the existence of offensive cyber capabilities specially designed for military use in the broader ecosystem of tech regulation in India.

While MeitY had made a passing reference to "offensive cyber" in a draft report authored by one of four Committees constituted in February 2018, for the promotion of AI and the development of a regulatory framework. The Report of Group D, the Committee on Cyber Security, Safety, Legal and Ethical Issues briefly speaks of "defensive and offensive AI techniques". However, this report contained recommendations that do not carry the force of law. In contrast, the DGFT's latest amendment to the SCOMET list has the effect of subjecting the export of such technologies to strict regulatory control by the Government.

This regulatory development stands in contrast to the response of National Cyber Security Coordinator Lt. Gen. Pant in an interview to Medianama on 2 June 2020, only a few days before the date of this amendment to the SCOMET list:

> ***MediaNama: In terms of follow-up to hardware and software procurement, does India procure any software as cyber weapons? Is there a process to import or export them? There has been a discussion at the Open-ended Working Group [OEWG] at the UN regarding global procurement of cyber weapons. What is India's position, policy on procurement of cyber weapons?***
>
> ***Lt General Pant:*** *No, no. I don't think anyone will be speaking of cyber weapons, sale or anything like that.*

It now remains to be seen whether the National Cyber Security Strategy, yet to be released, will officially acknowledge the existence of 'offensive cyber capabilities', if not 'cyber weapons' within India's cyber ecosystem.

*This article was first published on CCG-NLUD's blog. It has been cross-posted with the author's permission.*

**Support our journalism:**



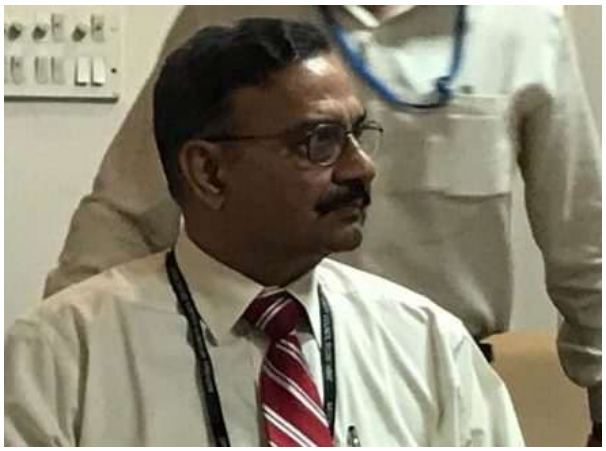
## For You



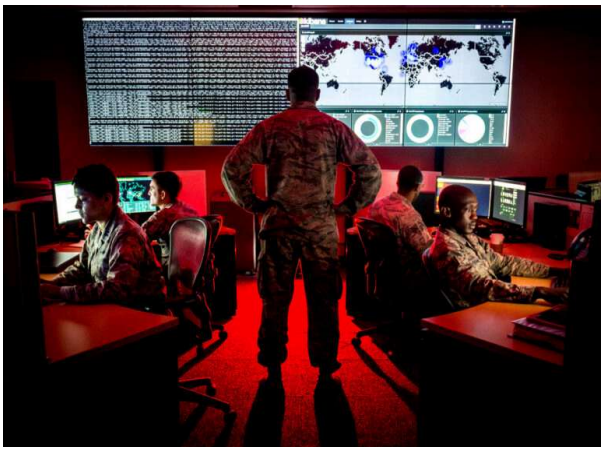
DISCOVER MORE

cyber security | cybersecurity | national cyber security strategy 2020

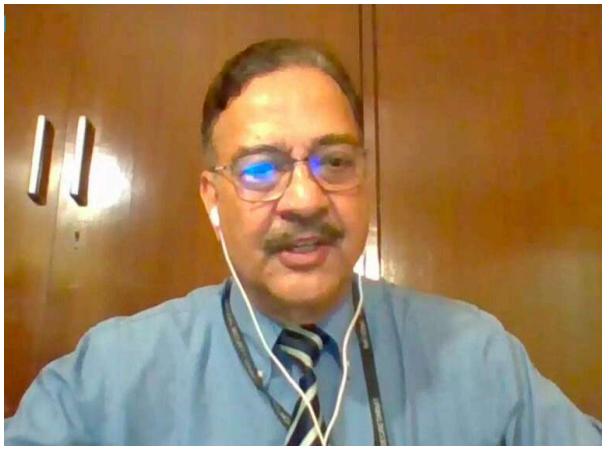
**Related Posts:**



## Lt Gen. (Dr) Rajesh Pant on India's National Cyber Security Strategy, Indo-US cooperation, end-to-end encryption and more

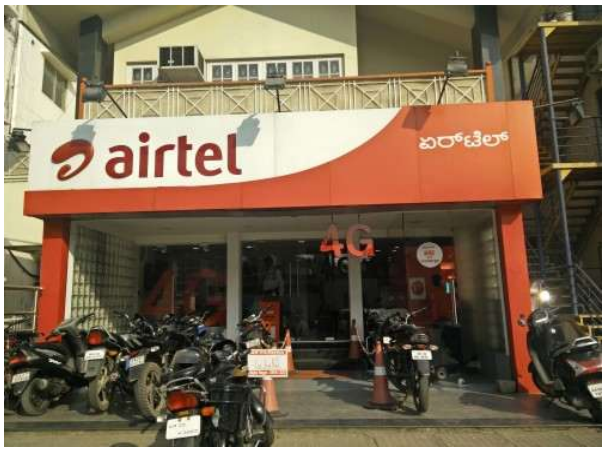


## What are 'offensive cyber capabilities'? — by Gunjan Chawla and Vagisha Srivastava



## 'National Cyber Security Strategy awaiting cabinet nod, will hopefully be released in October': Rajesh Pant

## Exponential growth in number of cyber incidents reported to CERT-In during pandemic: MEITY




## Airtel partners Symantec to distribute B2B cyber security solutions in India

## Promoting encryption should be 'primary focus area' of National Cyber Security Strategy 2020: Internet Freedom Foundation

MEDIANAMA

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