THE DIPLOMAT

Can Offensive Cyber and Information Control Capabilities Be Simultaneously Measured?

A recent case in India suggests complications in measuring a country's cyber power through open-source intelligence.

By **Gunjan Chawla**

September 16, 2020

Credit: Flickr/Blogtrepreneur

The Belfer Center for Science and International Affairs at the Harvard Kennedy School recently published a detailed report on a National Cyber Power Index 2020 (NCPI), which creates a ranking system for the "cyber power" of 30 countries. The NCPI defines cyber power as a function of the country's intent and capability using a set of 32 intent indicators and 27 capability indicators developed by the researchers. The indicators are grouped under seven broad objectives that countries pursue using cyber means, including surveillance, defense, offensive capability, manipulation of the information environment, intelligence, commercial and industrial growth, and norms.

India ranks 21st in the overall NCPI ranking. It did not make it to the top 10 in *any* of these categories and is classified as a "low-intent, low capability" cyber power — certainly not good news for strategists in the most cyber-attacked nation in the world. Additionally, faced with an ongoing uncertain environment at India's borders, with aggressive Chinese posturing turned into an occupation of territory Beijing has not disputed before, China's ranking as a top contender to displace the United States'

technological superiority should undoubtedly be the most worrying for India.

Before policymakers tasked with formulation of India's much-awaited National Cyber Security Strategy rush back to the drafting table in dismay, let us take heart in the observation that Israel too is suspiciously low in the rankings for cyber capability. This is despite Israel's formidable prowess in the cyber and intelligence domains, now (in)famous in India, courtesy the NSO Group's Pegasus spyware controversy. The Belfer Center report acknowledges that Israel's low ranking on cyber capability is an anomaly and points to the use of only publicly available open-source information, which does not reveal much about covertly conducted cyber operations. This anomaly opens up the analysis and rankings to broader criticism.

In this article, I identify certain points of tension within the chosen criteria, to illustrate the inherent difficulties in measuring cyber power accurately in a context where information controls deployed by the state to hide capabilities function effectively.

As a preliminary objection, technologists would very likely point to the difficulty of separating cyber defense from cyber offense and intelligence in practice as an inherent weakness in considering these separately in any analysis. Further, if we deconstruct the rankings across objectives studied to deduce which elements of the cyber power playbook are being prioritized by a particular country, the logic of the indicia adopted starts to break down.

India ranks relatively high on norms, intelligence, commerce, and defense (in descending order) but lowest on information control, offense, and surveillance (in ascending order). Defense appears to sit in the middle of India's cyber power priority list. India's overall ranking on the NCPI suggests that India has low cyber capability weighed down by even lower intent.

With respect to India's cyber capabilities, it is very surprising to see India ranked the *lowest* in the Cyber Capability Index on both information control and surveillance. For rankings on these two objectives under intent, India ranks significantly higher for surveillance, but is at the bottom of the ladder in information control. This appears to be starkly at odds with the on-ground reality of surveillance and information control in India.

It seems intuitive, even simplistic, to state that publicly available information is extremely limited, especially on strategically sensitive matters like cyber defense, cyber offense, and especially information control. But the effectiveness of information control measures to prevent leakages of such sensitive information, especially covert operations in many of the jurisdictions studied, could introduce distortions in perceptions of power and its analyses. These distortions would, in theory, be proportionate to the degree to which information control measures prove effective in preventing leakage of sensitive information into the public domain. The challenge thus lies in the near-total non-observability of the effectiveness of information control measures. In this manner, the inclusion of information control as an objective of a cyber power appears to militate against accurate readings of data gathered with respect to indicators for other objectives.

A recent blink-and-miss regulatory development in India's export control regulations, for instance, suggests that there is a lot more to cyber policy and cyber power than meets the eye.

On June 11, India's Directorate General of Foreign Trade (DGFT) amended certain items listed in a Schedule appended to the "Indian Trade Classification based on Harmonized System of Coding," better known as the ITC-HS classification system. One of the insertions made by this amendment in the Schedule falls under Category 6 (Munitions) of the Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET) export-control list. One item, numbered as 6A021 in this list,

explicitly referred to software “specially designed or modified for use in military offensive cyber operations.” Voilà! India’s first official acknowledgement of offensive cyber capabilities. Given that the executive documents that vest legal authority in India’s external intelligence agency, the Research and Analysis Wing (R&AW) as well as India’s technical intelligence agency, the National Technical Research Organization (NTRO). remain classified, chancing upon this little piece of OSINT seemed too good to be true.

On July 10, we published a brief update about this regulatory development, juxtaposing it with a quote from an interview of India’s National Cyber Security Coordinator, where he asserted that India has no plans to procure “cyber weapons or anything like that.” A few days, perhaps weeks later, an updated and sanitized version of the same regulations was uploaded on the DGFT website, which erased this terminology from the text altogether. The text of the original amendment can be accessed at the end of this piece.

When attempting to answer the question whether India has offensive cyber capabilities based solely on publicly available information, there are several plausible explanations and interpretations of this chain of events.

Depending on one’s perspective and distortions in perception at play, one may believe this to be clear evidence of India’s acquisition of offensive cyber technologies (whether indigenously developed or imported remains unclear) that are now restricted for export outside India. If this is the case, the change signals a failure of intra-government information controls followed by a rather clumsy restoration of those controls. On the other end of the spectrum, one could attribute the initial reference to “offensive cyber” simply to bureaucratic lethargy — made evident by the use of terminology imported from another jurisdiction’s export control regulation — as an inadvertent error that was later corrected.

For researchers of cyber policy, this necessitates a finer dissection and critical analysis of the constituent elements of cyber power, its indicators, and their prioritization in relation to one another, as well as the publicly available information relied on in the construction of the NCPI.

Gunjan Chawla is the Technology and National Security Programme Manager at the Centre or Communication Governance at National Law University Delhi.

TAGS

Asia Defense Security South Asia India cyber capabilities India cyber strategy information control Offensive cyber weapons