Last Updated On: July 15, 2021

India's Cyber Security: A look at the Approach and the Preparedness

Dr. Sankalp Gurjar | 15 July 2021

In the last week of June, two interesting developments underscored the need to focus attention on India's cyber security. On 28th June, the International Institute of Strategic Studies (IISS), an influential think-tank based in London, published a report on 'Cyber Capabilities and National Power' which assessed the cyber capabilities of 15 states including India. Unrelated to the launch of the report but linked with the theme of it, on 29th June, India's Foreign Secretary (FS) Harsh Vardhan Shringla addressed the United Nations Security Council (UNSC) Open Debate about 'Maintenance of International Peace and Security: Cyber Security.' Taken together, these two developments provide a good opportunity to throw some light on India's overall approach towards the question of cyber security and the development of its cyber capabilities.

In the last few years, cyber security has attained growing importance in all debates about national security. Cyber capabilities are now considered an essential element of national power. States employ these capabilities for a variety of purposes including to provide essential services to their citizens, launch attacks on the digital infrastructure of adversaries, collect intelligence, and steal trade secrets and technologies for economic benefits.[1] Sophisticated cyber-attacks with the possible involvement and/or support of state actors are carried out to impose costs as well as to send a message to the adversaries. The potential deniability and cheaper costs of launching cyber-attacks make it a particularly attractive tool for security agencies.

The onset of Covid-19 pandemic and the consequent rise in the number of people working from home digitally has resulted in the increase in cyber-attacks and criminal activities in cyberspace. Examples of companies being routinely targeted and being held for ransom as well as attacks on national infrastructure such as power grids and pipelines abound.[2] Security establishments around the world are grappling with questions about the possible use of cyber capabilities by terrorist groups. In the past, Islamic State of Iraq and Syria (ISIS) had used cyberspace to spread its message and attract recruits. To be sure, military application of cyber capabilities and the rise of complex strategic environment with a premium on offensive capabilities to achieve maximum impact by disrupting digital systems has emerged as a serious concern for national security planners. In the coming years, the importance of cyberspace is set to rise even further and hence, issues of internet governance, fixing accountability, setting of norms and building a broad framework to ensure safe and secure cyberspace is necessary. The Foreign Secretary' (FS) address to the UNSC is important in this regard, as it outlines the broad contours of India's approach to the cyber security.

UNSC Open Debate about 'Maintenance of International Peace and Security: Cyber Security'

The address began by acknowledging that the 'nature of conflict and its underlying tools have transformed tremendously over the decades.'[3] The world is now 'witnessing growing security threats to Member States emanating from cyberspace' and therefore, 'this open debate is timely.'[4] FS noted that, the 'borderless nature of cyberspace, and more importantly anonymity of actors involved, has challenged the traditionally accepted concepts of sovereignty, jurisdiction and privacy' and that 'open societies have been particularly vulnerable to cyber-attacks and disinformation campaigns.'[5] Russia's alleged intervention in the American elections is a good example of such attacks and disinformation campaigns.[6] It leads to an emergence of a new set of issues and concerns in the making of national security policy, especially in open societies, where the imperative to find the right balance between privacy, openness and security is not an easy process.

The speech refers to 'some States' who 'are leveraging their expertise in cyberspace to achieve their political and security-related objectives and indulge in contemporary forms of cross-border terrorism.'[7] Besides, cyberspace is being exploited by terrorists 'around the world to broaden their appeal, spread virulent propaganda, incite hatred and violence, recruit youth and raise funds.'[8] Terror networks have also used 'social media for planning and executing their terror attacks and wreaking havoc.'[9] In this context, the Christchurch terror attack of 2019 where the attacker livestreamed it on Facebook is a good example to consider.[10] For a country like India, which has been at the receiving end of terrorism, FS observed that it is important 'to address and tackle the implications of terrorist exploitation of the cyber domain more strategically.'[11]

FS argued that it is 'in the interest of the international community to ensure that all actors abide by their international obligations and commitments and not indulge in practices that could have potentially disruptive effects on global supply chains and trade in ICT [Information and Communication Technology] products.'[12] In the context of the necessity of achieving rapid economic recovery after the Covid-19, ensuring the seamless flow of global supply chains and trade in the case of cyber products is particularly important. India is critically dependent on the exports of services and ICT products play a major role in India's gross domestic product (GDP). Therefore, the issue is of particular relevance for India.

While discussing the solutions to the problems of securing cyberspace, FS noted that the 'interconnectedness of the cyber domain requires that solutions to the complex problems and threats emanating from cyberspace cannot be resolved in isolation.'[13] To do this, the address urged the international community that 'we need to adopt a collaborative rules based approach in cyberspace and work towards ensuring its openness, stability and security.'[14] It is imperative to 'find further common ground and improve upon the already agreed cyber norms and rules.' The rules for the cyberworld 'must strive to ensure collective cyber security through international cooperation.'[15] India believes that 'multi-stakeholder involvement would help in achieving this objective.'[16]

The Covid-19 pandemic and the need to shift a bulk of work and other necessary activities online has highlighted the critical issue of digital divide. The speech underscored that the 'widening "Digital gaps" and "Digital knowledge gaps" amongst countries create an unsustainable environment in the cyber domain.'[17] There is no alternative to focus on capacity building and collective efforts. In the last few years, India has 'successfully leveraged the tremendous potential of cyber technologies in implementing the SDG agenda and improving governance.'[18] FS ended the speech by stressing India's position on the issue of cyber security. The address noted that 'our overarching objective is to harness cyberspace for the growth and empowerment of people, not just of our own country, but for all humanity.'[19] For this objective, 'India is committed to an open, secure, free, accessible and stable cyberspace environment, which will become an engine for innovation, economic growth, sustainable development, ensure free flow of information and respect cultural and linguistic diversity.'[20]

In the context of this stated Indian position on the issue of cyber security, it would be interesting to consider India's cyber capabilities.

IISS Report on Cyber Capabilities and National Power

IISS report assesses 15 countries along the seven verticals. These include Strategy and Doctrine, Governance, Command and Control, Core Cyber-intelligence Capability, Cyber Empowerment and Dependence, Cyber Security and Resilience, Global Leadership in Cyberspace Affairs, Offensive Cyber Capability.[21] Based on these categories, countries are grouped in three tiers: tier one countries are those that have 'world-leading strengths' in all the verticals. United States (US) is the only country which features in Tier One. Tier two countries have 'world-leading strengths' in some categories and include Australia, Canada, China, France, Israel, Russia and the United Kingdom (UK). Finally, tier three countries have strengths in some categories but significant weaknesses in others. India, Indonesia, Iran, Japan, Malaysia, North Korea and Vietnam are part of Tier Three.[22] IISS report notes that these seven countries are at 'much earlier stages in their cyber journeys, each having strengths or potential strengths in some of the categories in the methodology but significant weaknesses in others.'[23]

The report takes note of India's evolving approach to the issue of cyber security. It notes that although the first national cyber security policy was released in 2013, 'India's thinking on cyber policy for the civil sector continues to develop.'[24] The overarching and updated national cyber security strategy was intended to be released in 2020 'to address developments in 5G, ransomware and the Internet of Things.'[25] However, Covid-19 and other challenges seem to have stalled that effort. Nonetheless, India is 'actively reframing all areas of cybersecurity policy, including education, skills, import controls and national security' and after the border clashes with China last year, concerns have been heightened about Chinese cyber-attacks and security of Chinese-made digital systems.[26]

India is an interesting case study for cyber power assessment. It has a large digital economy estimated to be worth $190 billion, a vibrant start-up culture and a vast talent pool to build national cyber power. Yet, India's cyber capabilities are decentred and multiple agencies play a role in cyber security related functions. National Technical Research Organisation (NTRO), which was set up in 2004, is a 'main cyber agency' and reports to the National Security Advisor (NSA).[27] Defence Cyber Agency, created in 2019, 'is central to the command and control of India's military cyber capabilities.' The intended function of DCA is 'to integrate and coordinate the cyber, space and special- forces capabilities of the three armed services.' Besides, the Intelligence Bureau (IB), Research and Analysis Wing (RAW) and Defence Intelligence Agency (DIA) are integral parts of India's cyber intelligence capabilities.[28]

The report notes that 'beyond the domestic threats, India's cyber-intelligence capabilities have unsurprisingly been focused on its near abroad, particularly Pakistan.'[29] In fact, 'India's cyber-intelligence reach appears weak' and therefore, 'it tends to rely on partnerships such as those with the US, the United Kingdom and France for a higher level of cyber situational awareness and to help it develop a greater reach of its own in future.'[30] Interestingly, the report recognises that 'in the field of artificial intelligence (AI), India's research capability has been placed quite highly in global rankings.' India's 'AI research and development (about 85%) is conducted by universities rather than industry.'[31] IISS report believes that 'the most distinctive feature of India's cybersecurity infrastructure is the importance of the private sector, which has led the way in developing strong policies and standards.'[32] As the internet integrates with everyday lives and sectors such as e-commerce take off, the necessity of developing ever greater cyber capabilities will increase on an unprecedented scale.

India has often been targeted by Chinese and Pakistani cyber-attacks. North Korea has also been launching cyber-attacks on India using the Chinese networks. In 2020, India faced the second-highest number of incidents of ransomware in the world. The attacks on financial institutions have been of particular concern for India. However, India's overall preparedness to deal with the growing threats in the cyber domain has left much to be desired. In 2018, India was ranked 47th out

of 175 countries in a Global Cybersecurity Index prepared by the International Telecommunications Union. In the same index, China stood at the 27th position, much ahead of India.[33] IISS report notes that India understands that 'its defensive capabilities are relatively weak.' As a result, 'it pursues diplomatic efforts to bring the governance of cyberspace within the rules-based international order, while maintaining a realistic approach to dealing with the states that are targeting its networks.'[34] India has well-developed cyber partnerships with the US and UK and can perhaps augment its capabilities with the help of close strategic partners such as Israel and France.

IISS report notes that 'India has developed relatively advanced offensive cyber capabilities focused on Pakistan. It is now in the process of expanding these capabilities for wider effect.'[35] In fact, in the wake of the November 2008 terror attacks, India considered a cyber response.[36] The report candidly admits that 'it is difficult to gauge the extent or orientation of India's current investment in offensive capabilities but there are some indications that the focus may have shifted more to countering China, given its growing economy and regional power.'[37] There have been suggestions to build India's offensive cyber capabilities by think-tanks. The section on India ends by making an observation that 'India's focus on Pakistan will have given it useful operational experience and some viable regional offensive cyber capabilities.'[38] Moving further, India 'will need to expand its cyber-intelligence reach to be able to deliver sophisticated offensive effect further afield.' To do this, 'close collaboration with international partners, especially the US, will help.'[39]

Concluding Remarks

In the context of the FS' address and IISS report, we can discern three broad trends: *first*, India is actively thinking about the issue of cyber security and is advocating a multi-stakeholder approach as opposed to countries like China which favour greater state control over the cyberspace. *Second*, cyber security is relevant not only for securing India's digital infrastructure but also for the larger transformation of India as could be seen in the development of the Co-Win application which has been developed and deployed for Covid-19 vaccination. Bridging the digital divide by providing easy, cheap and reliable access remains however key in this regard. The expansion of cyber activities and the effort to bring millions of Indians into the digital domain will necessitate the growing salience of pursuing defensive as well as offensive cyber capabilities. *Third*, India has been taking steps, as could be seen in the creation of multiple agencies and pursuing diplomatic collaborations with strategic partners, to ensure that deficiencies in the cyber security domain could be addressed. But a lot more needs to be done to secure its cyber infrastructure. The world is entering an era where national security will hinge increasingly on cyber security. Therefore, there is no option but to build defensive and more importantly, offensive cyber capabilities while pushing for the creation of governing norms and frameworks for the use of cyberspace.

*****

**Dr. Sankalp Gurjar, Research Fellow, Indian Council of World Affairs, New Delhi.*
Discalimer: Views expressed are personal.

References:

[1] International Institute of Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment", June 28, 2021. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (Accessed on July 10, 2021).

[2]Ibid

[3]Ministry of External Affairs, "Foreign Secretary's Statement at the UN Security Council Open Debate on "Maintenance of International Peace and Security: Cyber Security", June 29, 2021. Available at: https://www.mea.gov.in/Speeches-Statements.htm?dtl/33963/Foreign_Secretarys_Statement_at_the_UN_Security_Council_Open_Debate_on_Maintenance_of_International_Peace_and_Security_Cyber_Security_June_29_2021Accessed on?

[4]Ibid

[5]Ibid

[6]Patrick Howell O'Neill, "The Russian hackers who interfered in 2016 were spotted targeting the 2020 US election", *MIT Technology Review*, September, 10, 2020. Available at: https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spotted-targeting-the-2020-us-election/(Accessed on July 10, 2021)

[7]Ministry of External Affairs, No. 3

[8]Ibid

[9]Ibid

[10]BBC News, "Christchurch shootings: 49 dead in New Zealand mosque attacks", March 15, 2019. Available at: https://www.bbc.com/news/world-asia-47578798 (Accessed on July 10, 2021)

[11]Ministry of External Affairs, No. 3

[12]Ibid

[13]Ibid

[14]Ibid

[15]Ibid

[16]Ibid

[17]Ibid

[18]Ibid

[19]Ibid

[20]Ibid

[21] International Institute of Strategic Studies, No. 1, pp. 3

[22]Ibid, pp. 9-12

[23]Ibid, pp. 11

[24]Ibid, pp. 133

[25]Ibid, pp. 133-134

[26]Ibid, pp. 134

[27]Ibid, pp. 134

[28]Ibid, pp. 135

[29] Ibid, pp. 135

[30]Ibid, pp. 135-136

[31]Ibid, pp. 136

[32] Ibid, pp. 137

[33]Ibid, pp. 137

[34]Ibid, pp. 138

[35]Ibid, pp. 139

[36]Raj Chengappa and Sandeep Unnithan, "How to Punish Pakistan", *India Today*, September 22, 2016. Available at: https://www.indiatoday.in/magazine/cover-story/story/20161003-uri-attack-narendra-modi-pakistan-terror-kashmir-nawaz-sharif-india-vajpayee-829603-2016-09-22 (Accessed on July 12, 2021)

[37] International Institute of Strategic Studies, No. 1, pp. 139

[38]Ibid, pp. 139

[39]Ibid, pp. 139