Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
29/16

WHY INDIA NEEDS TO BUILD INDIGENOUS CYBER CAPABILITIES?

E.Dilipraj
Associate Fellow, CAPS

There is an ongoing legal turf war between FBI and the tech giant Apple over unlocking of the iphone of an accused condemned in a mass shooting case. This act of the accused was described as an act of terrorism, in which 14 people died and 22 people were seriously injured. What one needs to realise here is that the tussle between FBI and Apple could be seen as the starting point of realization regarding the wide gap existing between technology and legislature. Highlighting similar consensus, James Comey, Director of Federal Bureau of Investigation (FBI), once stated that

> *"…technology has become the tool of choice for some very dangerous people. Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem…."*[1]

This FBI v/s Apple case is keenly being observed by countries around the world as the US, which is otherwise considered as the cradle of computer and internet technology is legally fighting against Apple—an internet based technology giant and a powerful non-state actor, over the issue of privacy, state control, national security and public safety. The outcome of this case will be a benchmark to many similar cases in the future not only in the US but also in other parts of the world. Nevertheless, while this scuffle is still on, the actions of legal agencies in few countries on such similar cases is worth mentioning.

To begin with, France is in the process of pushing a bill in the parliament that would impose penalties including a jail term on technology executives who deny access to encrypted data during a terrorism investigation. The lower house of the chamber of parliament has already passed this bill with a majority rating of 474 accepting the bill while 32 members opposed it.[2] It is being speculated that once this bill becomes a law, for every act of non-

compliance to the government's request, the technology companies have to pay 1 million Euros as fine to the French government.

In another case in São Paulo, Brazil, on March 1, 2016, the Brazilian law enforcement authorities held Facebook's Vice-President for Latin American region Diego Dzodan, under custody for allegedly failing to provide information requested for criminal investigation and non-compliance of court-order. For more than a month prior to the arrest, Facebook's subsidiary— WhatsApp - had been ordered to reveal messages relating to a suspected drug-trafficking ring. After the company denied three related requests by federal police, the judge first imposed a daily fine on the US Company of 50,000 reais (£9,000), then a daily penalty of 1 million reais (£180,000), and finally ordered the arrest of the Vice President.[3] Although Mr Dzodan was released the next day by another judge from a higher court stating that he [Dzodan] cannot be blamed responsible for the inaction of the company, the case is much similar to that of the ongoing FBI – Apple case. Also in a similar case, on December 16, 2015, a judge in Sao Bernardo do Campo, an industrial suburb of Sao Paulo ordered the suspension of WhatsApp service for a time period of 48 hours due to the company's non-compliance to requests for information by the country's investigating agencies.[4] Although the suspension was lifted by another judge in a higher court after around 12 hours, this incident is another case of conflict of interest between the legislature and an advanced cyber technology company.

Russia, on the other hand, is taking much bolder steps in restricting the operations of the US IT giants like Google, Microsoft and Apple from operating in Russia. German Klimenko, the newly appointed first Internet Advisor to President Putin, is in the process of introducing a bill in the parliament for increasing the taxes on the applications that are bought from Google Play Store or the App Store within Russia. The proposed bill if cleared would charge VAT of 18% on the revenue of 300 billion Rubles ($3.9 billion) made together by the companies like Google, Apple, Microsoft and other foreign companies in Russia every year.[5] Klimenko is also determined to switch the state networks operating on the Windows operating system to open-source operating system-Linux, that according to him will secure Russia's networks to an extent from the US surveillance and snooping programmes.[6] His steps in containing the operations of US IT giants in Russia can also be perceived as an effort to promote Russian IT companies like mail.ru, VK and Yandex in the domestic market which claim to have similar technological capabilities like Google and Facebook.

Furthermore, China, which is popular for its high level internet censorship, has cleared a stringent cyber security law which was brought into effect from January 01, 2016. One of the

sections under this law states that all the telecommunications and Internet companies operating in China are required to provide technical assistance, including decryption of sensitive user data, to the law enforcement agencies in any probe meant "to avert and investigate terrorist activities".[7]

Moving on, in India, the gap between legislature and cyber technologies is much bigger in comparison to the situation in the countries discussed above. Section 69 of Information Technology Act 2000 is the only available legal supplement for the country to demand for decryption of data for the purpose of investigation and national security. However, it should be noted that this act may not be binding on companies which are not registered under Indian legal jurisdictions. In simple terms, Facebook, Google, Twitter or any other foreign country based IT giant need not necessarily respond to all requests from the Indian government regarding data or information for some ongoing investigation related to a crime or national security threat.

Moreover, in spite of the exisitng number of talents in IT and ITeS sector, the country suffers from lack of indigenous development of software and hardware products for domestic purpose. While the country's GDP gains revenues worth more than 100 billion ever year from exporting software products, it remains unclear if the nation is thinking towards creating an indigenous operating system. Such an effort, if carried out, would help to an extent to curtail the mass surveillence and espionage programmes of foreign countries that exploit foreign built OS and would also help to reduce the country's dependency on foreign technology companies for general operation of computers. China and Russia have built their own versions of open-source Linux based operating systems which are in the process of implementing it in their respective countries and a similar effort in India would be fruitful in the longer term though it may have to face certain resistance in the early stages. Again, taking a cue from Russia and China, Indian government should encourage and promote home grown 'desi' Internet based companies like Google, Facebook, Twitter, which when successful, could help retain domestic data within the country.

Similarly, on the hardware front, the country's efforts are barely scratching the surface. The country's semiconductor manufacturing industry which forms the basics for the cyber world is yet to come out of the research labs of Universities like IITs and IISCs and set up commercial production. The government's plan for setting up two semiconducter plants with an investment of Rs 63,000 crore is yet to see the light of day as the proposals are still under consideration. [8] Nevertheless, it is believed that the first plant would be established by 2017 in Prantij of Sabarkantha district, Gujarat which would

employ over 25,000 people including 4,000 direct employees.[9] The country also lacks manufacturing capability of IT hardware especially the networking equipments which are the sensitive equipments when used in national critical infrastructures.

Based on the existing cyber environment, India could adopt a three pronged strategy as follows:

- Indigenous development of software and hardware products for domestic use,
- Promotion of indigenously built IT products even if it has to be through import substitution,
- Enhancing the country's cyber security laws and passing of the pending privacy protection laws.

The countries around the world would keep debating for a long time over the issues of Internet governance, cyber governance, privacy, data protection, state control, etc in the cyber domain, which should not stop any state from pursuing its actions in order to regulate and secure its domestic cyberspace. Therefore, India should focus on enhancing its capabilities in the cyber realm in order to be self dependent in this highly virtual world and to avoid becoming a cyber slave nation.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] James B.Comey, "Going Dark-Are Technology Privacy and Public Safety on a collision course", Speech at Brookings Institution, Washington D.C, October 16, 2014, https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course, Accessed on March 15, 2016.

[2] Helene Fouquet and Marie Mawad, "France clears Bill that could force Apple to unlock terror data", *Bloomberg Business*, March 08, 2016, http://www.bloomberg.com/news/articles/2016-03-08/france-votes-on-bill-that-could-make-apple-unlock-terrorist-data, Accessed on March 15, 2016.

[3] Jonathan Watts, "Brazilian Police Arrest Facebook's Latin American vice-president", T*he Guardian*, March 01, 2016, http://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan, Accessed on March 15, 2016.

[4] "Brazil court orders WhatsApp messaging to be suspended", BBC, December 17, 2015, http://www.bbc.com/news/world-latin-america-35119235, Accessed on March 15, 2016.

[5] Ilya Khrennikov and Stepan Kravchenko, "Russia's New Internet Czar Wants Apple and Google to Pay More Taxes", Bloomberg, February 09, 2016, http://www.bloomberg.com/news/articles/2016-02-09/putin-s-new-internet-czar-joins-hunt-for-google-apple-taxes, Accessed on March 15, 2016.

[6] Ibid.

[7] Bruce Einhorn, "A Cybersecurity Law in China Squeezes Foreign Tech Companies", Bloomberg Business, January 22, 2016, http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies, Accessed on March 15, 2016.

[8] Pankaj Doval, "Make in India: Plan for Rs 63,000 crore semiconductor wafer plants hits hurdle", Economic Times, May 29, 2015, http://economictimes.indiatimes.com/tech/hardware/make-in-india-plan-for-rs-63000-crore-semiconductor-wafer-plants-hits-hurdle/articleshow/47466506.cms, accessed on March 16, 2016.

[9] "Semiconductor Industry in India", http://www.ibef.org/industry/semiconductors.aspx, Accessed on March 16, 2016.