Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
20/18

'Do Not Buy' List of DoD: Escalating Cyber concerns between the US and Russia-China

Dr. E.Dilipraj
Research Fellow, CAPS

Keywords: Department of Defence, Cyber threats, Software ban, Do Not Buy List, US, Russia-China

The US has recently admitted preparing a 'Do Not Buy' list of companies that use Russian and Chinese origin software in their products. The acceptance for this came from Ellen Lord, the Under Secretary in charge of procurement in the Department of Defence (DoD), who further stated that the DoD was in preparation of this list for the past six months.

It should be noted here that way back in June 2017, President Donald Trump administration had banned the use of Russian company - Kaspersky Lab Products - within the US government organisations. President Trump had in fact signed a separate law in this regard.[1]

The US authorities claim that this effort is to secure their government organizations free from Russian and Chinese cyber meddling through software. Also, it can be seen as a growing insecurity within the US government agencies due the increasing cyber capabilities of Russian and Chinese companies especially in the defence sector.

There are also concerns existing within the US Congress regarding the use of two Chinese Telecom company products: ZTE Corp. and Huawei;[2] which might have also made it to the current list. Although the names of companies in the 'Do Not Buy' list was not openly revealed, the US DoD is believed to have started circulating the list to defence contractors, large and small, via a number of defence industry trade associations.[3]

The information about preparation and circulation of such a list cannot be seen in isolation as countries around the world are getting sensitive about components of their defence products: both hardware and software. For instance, the US and other Western companies such as Cisco, IBM, SAP, Hewlett Packard Enterprise Co and McAfee have allowed Russia to conduct source code reviews of their products before entering into the lucrative Russian market. The Federal Security Service

(FSB) and Federal Service for Technical and Export Control (FSTEC) are two agencies that are tasked for reviewing products especially from Western companies. It is estimated that Russia's Information Technology market is worth more than $18.4 billion which the Western companies do not want to miss out by denying review on their products.[4] Although the US has advised its country's companies against submitting their source codes for Russian Review, many companies take this risk in order to gain profit from the Russian Market.

In a similar case, the Chinese cyber law which came into effect in-mid 2017 also requires foreign companies to submit their products for review with the Country's authorities. According to the law, foreign companies that seek to be active on the Chinese market are required to provide access to their software source code.[5] China Information Technology Evaluation Center is designated as the agency responsible for the review of the source codes of foreign companies. US companies like IBM, Microsoft and more have heeded to the Chinese law and have submitted their source codes for review.

The US government authorities claim that when Russia and China ask for review of source codes, they also look for vulnerabilities which can be exploited in later stages. Also, the preparation of the recent 'Do Not Buy' list is hailed within the DoD as an attempt to subvert Russian and Chinese cyber operations by hiding vulnerabilities into the products.

However, the answer given to the first concern at least from the Russian side states that all the reviews take place in a secured environment which is known as "Clean Room", where no software data can be altered, copied or transferred.[6] Once again, regarding the 'Do Not Buy' list, it can only be stated that the insecurity of the US is reflecting in their actions. The US intelligence agency's infamous efforts in global digital surveillance has the country (US) worried about its own security as many more countries, especially Russia and China, are developing their own cyber operations.

Moreover, these developments add more levels of complexity to the existing trade-war geopolitical scenario boiling between the US-led West and Russia-China. The US wants to project Russia-China as the negative powers of the world and on the other hand, Russia-China are working towards bypassing the West dictated international order and establishing an alternate order for themselves; something that reflected in the recently concluded BRICS Summit in Johannesburg.

In this scenario, India should be a keen observer of the developments taking place globally with regard to cyber products. With a multi-billion dollar IT market, the country is a lucrative destination for companies around the world. India is also a key importer of many defence equipments, most of which are heavily dependent on cyber technology. Therefore, there arises a natural concern for the country to be wary of its supplier's intent as well, since these products are destined for national security purposes. India may also work towards attaining more cyber sovereignty in terms of regulating its cyberspace and bringing more stringent laws which will ensure the country's security in the virtual domain.

(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] Roxana Tiron, "Pentagon's 'Do Not Buy' List Targets Russian, Chinese Software", Bloomberg, July 27, 2018, https://www.bloomberg.com/news/articles/2018-07-27/pentagon-s-do-not-buy-list-targets-russian-chinese-software, accessed on July 31, 2018.

[2] Ibid.

[3] Graeme Burton, "US gov's 'do not buy' list shuts out software from China and Russia", The Inquirer, July 30, 2018, https://www.theinquirer.net/inquirer/news/3036757/us-govs-do-not-buy-list-shuts-out-software-from-china-and-russia, accessed on July 31, 2018.

[4] Joel Schectman, Dustin Volz, Jack Stubbs, "Under pressure, Western tech firms bow to Russian demands to share cyber secrets", Reuters, June 23, 2017, https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB, accessed on July 31, 2018.

[5] Boris, "Foreign companies' source code reviewed by a Chinese agency linked to online espionage", Malware Complaints, 01 September 2017, https://malwarecomplaints.info/foreign-companies-source-code-reviewed-chinese-agency-linked-online-espionage/, accessed on July 31, 2018.

[6] No. 4