



RAJEEV CHANDRASEKHAR
MEMBER OF PARLIAMENT
RAJYA SABHA

Member of Standing Committee on Finance
Member of Consultative Committee on Finance
Member of Parliamentary Forum on Youth
Co-Chairman, Vigilance & Monitoring Committee, Bangalore Urban District
Vice Chairman, National Military Memorial Management Trust, Bangalore

Dear Shri Donal,

14 July, 2014

Sub.: Cyber Security

I refer to the large number of cyber attacks on Indian Assets over the last few years and the threat it poses to our national security.

With over a billion citizens and the ease of online banking and transactions coupled with the increase in the number of users of smartphones – there has been a significant increase in malicious attacks on digital devices and software systems. According to media reports, there has been a 136% increase in cyber threats and attacks against government organizations, and a 126% increase in attacks targeting financial services organizations in India. As many as 34% of Indian financial companies and 43% Government organizations reported cyber threats and attacks in 2013 — up from 15% and 19%, respectively, in 2012. According to Symantec's 2013 Norton Report, by July 2013, sophisticated cyber assaults like ransomware and spear-phishing has cost Indian individuals and companies approx. US\$4 billion.

Recently, there have been several instances and attempts to attack the Defence systems in India, as well as the civilian departments. This calls for an urgent need to counter cyber crime and secure the country from it. I have raised this issue earlier in Parliament and also through letters to the previous Government, emphasizing the need for a policy, strategy and body to address the issue of cyber protection.

Though the previous Government had announced a National Cyber Security Policy (NCSP), in July 2013, it does not have any accompanying action plan and specific strategies to counter this threat. It fails to detail specific parameters for effective implementation and also does not mention the Information Technology Act of 2000 which is significant in the event of a conflict. The policy also has no details about the parameters of privacy in the context of cyber security. Cyber security, privacy and civil rights or liberties constitute the three components of the triangle that is integral to the subject at hand.



Further, the policy does not give clarity about how the data will be collected, where and under what conditions it would be stored, and how it will be used. It has no checks and balances to ensure that activities meant for protecting online information are not abused, and does not explain how the Government will safeguard the civil liberties of the citizens.

Other developing countries like Malaysia are implementing their cyber security apparatus at a rapid pace. For example, the government of Malaysia has introduced strict new compliance requirements in the form of Malaysia's Personal Data Protection Act 2013.

Cyber espionage is a very clear and real threat to our nation and will only grow in terms of the threat it represents. As technology more and more pervasive in the country and various organizations, we become more vulnerable to this threat of cyber espionage and cyber attacks. Therefore, I urge you to make this an important priority, and an effective capacity and solution to manage the same be created within the Government, so that we are a cyber secure nation.

I look forward to meeting with you and discussing this further at your convenience.

Yours Sincerely,

RAJEEV CHANDRASEKHAR

Shri Ajit Doval
National Security Advisor
Prime Minister's Office
South Block
New Delhi 110 001