Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 557-558, DOI : 10.14429/dsj.66.10804

GUEST EDITORIAL

Special Issue on Cyber Security

Indivar Gupta* and P.R. Mishra
Scientific Analysis Group, Delhi - 110 054, India
**E-mail: indivargupta@sag.drdo.in*

In the present cyber age, public services are getting more and more dependent on use of information and communication technologies (ICT) day-by-day. A number of applications viz., Internet of Things (IoT), cloud computing and virtualisation and machine to machine (M2M) system usage are sneaking deeply into our everyday life. The more we depend on ICT, the more deepens our concern about informationtechnology security or cyber security.

Cyber security protects the data and integrity of assets that belong to or connect to anetwork. It is meant to defend those assets against all sorts of threat actors throughout the life cycle of a cyber attack. It is quite unsurprising that cyber security industry is growing at the same pace as ICT is doing. A cyber security expert has not only to deal with cyber attack but has to develop solution so as to suit budgetary constraints. A cyber security expert therefore needs to have a deeper understanding of these topics and many others, to be able to confront those challenges more effectively.

The theft of information from a government or a defence sector is seen as the most serious threat to national security. These thefts often go unnoticed for a long time as they are perpetrated in a secret and silent manner. The risk of a disastrous active attack on vital national infrastructure is yet another matter of concern. Such an attack may harm the backbone of a country. Stuxnet episode is the best example of such attack.

The government must protect its assets from cyber threats especially those belong to the military domain. The more sophisticated information systems emerge; the more challenges are created for the government. This is because cyber threats do not fit into the legacy security frameworks that exist in the government setup. Two major challenges in this context are to keep itself updated at the same pace as the technology advances and to ensure a smooth transition during the updation. A state-of-the-art R&D is needed to effectively meet such challenges.

Special issue of the *Defence Science Journal* is being published with the aim to include innovative works, relevant surveys and expositions, especially related to defence sector. Considering the broad spectrum of cyber security, an extensive and diverse list of topics was included into the scope. These topics included cyber threat mitigation techniques, cyber threat modeling and risk management, hacking and countermeasures, privacy, design and analysis of crypto-algorithms, authentication and authorisation, key exchange protocols, content protection (integrity), digital signature and certification, firewalls, intrusion detection system, and intrusion prevention system, secure operating systems, database security, network security, security infrastructure and security evaluation, malware and protection, software protection (tamper resistant software), etc. The composition of topics is expected to cater something for everyone and everything for someone.

We hope that special issue of the *Defence Science Journal* will address to a wide audience. We invite critical reviews, suggestions from our learned readers so as to make any issue of *Defence Science Journal* coming in this area better and more purposeful.