Centre for Air Power Studies (CAPS)

Forum for National Security Studies (FNSS)

**Title:** **THE ART OF PHREAKING, HACKING, CRACKING…**

**Chairperson:** Gp Capt **Ashish Gupta**, Senior Fellow, CAPS

**Speaker:** Mr **E.Dilipraj**, Associate Fellow, CAPS

**Discussant:** Wg Cdr **BS Nijjar**, Research Fellow, CAPS

**Rapporteur:** Dr **Temjenmeren Ao**, Associate Fellow, CAPS

**Date:** 08 April 2016

- Phreaking, Hacking and Cracking involves retrieving confidential documents and information through unconventional – and at times unethical – means. These are the offsets that came along with the telecommunication network revolution.
- Phreaking evolved in the US in the 1960s as a fun endeavour undertaken by groups called "phone freaks"; by middling with the telephone networks that enabled them to make free calls. The techniques adopted by these phone freaks were whistling and the loop method.
- The golden age of phone phreaking began with the invention of the 'Blue Box' that was used for making long distance calls. These phone freaks were hired by many underground organisations for helping them carry out their covert missions.
- The evolution of the data processing technology – modern day computer – in the 1970s attracted a new form of curiosity amongst the existing techno freaks and this resulted in the evolution of the 'computer freaks' and the formation of various clubs such as 'computer freaking club', that has led to the development of today's software and hardware companies. The founding members of these companies, such as Apple, are members of these clubs.

- This also lead to the evolution of a counter group know as hackers, who unlike the computer freaks, didn't have the resources to develop new software but had the curiosity in order to enable them to learn computer systems, programmes, hardware and hence, developed the techniques to discover the vulnerabilities in the existing systems.
- By the 1980s hackers were considered as the true inhabitants of the cyber world, as they helped in the development of newer technologies in the data software and hardware.
- However, a hacker, from a positive connotation is a person who enjoys exploring the details of programmable systems and finds methods to stretch their capabilities. It began to have a negative connotation as an inquisitive malicious meddler of computers who tries to discover information by poking around.
- In 1985 a new connotation was also incorporated known as 'Crackers', defined as one who breaks the security of a system.
- A loose set of regulations was put in place known as 'Hackers Ethics', in order to regulate hackers operations and ensure that their operations do not destroy any operating systems.
- Ethical cracking done for securing systems and networks in order to fix the existing vulnerabilities became acceptable. However, with the growth and spread of computers, a new breed of hackers and crackers has emerged who are driven by self interests and monetary gains, by carrying out illicit activities.
- Based on their activities', hackers can be divided into three categories; white hat hackers that carry out cyber security at one end and the black hat hackers involved in illicit activities on the other extreme end. In between, there are the grey hat hackers, whose activities come in the grey area, using illicit means for catching punishable offences.
- India's first major jostle from the impact of a cyber-attack was felt when BARC's website was breached in 1998 following India's nuclear test. This was followed by numerous cyber-attacks – showcasing various existing vulnerabilities in the system.
- Pakistan based hackers have been launching cyber attacks on India and these occur during important dates such as Independence Day, Republic Day, War victory anniversaries, and so on. There are Indian hacking groups as well such as Team Nuts that hacked into various Pakistani Commercial sites. A group of hackers in India who operate under the sobriquet "India Cyber Army" (ICA) also carried out numerous cyber-attacks

on Pakistan following the 26/11 attacks, with Pakistan's Cyber Army launching a counter offensive against India.

- The presence of cyber threat from India's external as well as internal adversaries has necessitated beefing up of its cyber security mechanism. However, a lot of bottlenecks remain pertaining to the identification and recruitment of existing talent and providing them with the technical know-how. These shortcomings need to be addressed and necessary measures need to be undertaken to strengthen the nation's critical infrastructure against cyber-attacks.