

Cyber Security: The New Phase of National Security

by Sagar Kumar Paswan

“National Security necessarily denotes a nation's determination to preserve certain interests at all costs. Foremost among these national interests are the nation's territorial integrity, political independence and fundamental governmental institutions. It embraces not only survival of the nation but also its ability to survive.” - Rober E. Osgood Jr.

This definition of National Security still stands to some accounts, but in this ever-changing environment where (especially with the advent of COVID-19) everything is going online, cyber warfare and security are among some of the most important concerns which our nation faces right now.

Today's definition acknowledges economic, environmental, human political and social factors among other strands that impact the concept of security. With the advancement of technology, nuclear weapons came into being. However, they cause widespread mass-destruction; nations now have started fighting indirect wars with the use of technology and software.

Cyber-attacks have been developing for a while across the globe and their potential is increasing everyday. These concerns become clearer with the reports from the Washington Post on the “Pegasus Software” owned by NSO Group from Israel. This software has been said to hack into an individual phone through a bug and then track all their activities including their conversations, text messages etc. Reports about the sale of the software suggest how governments across the globe had purchased it and the report from the Washington Post suggests that the cellphones of various leaders across the globe and in India had also been compromised through the software, the likes of which include French President Emmanuel Macron and former German Chancellor Angel Merkel among various others. This development sent shock waves across the globe. To add to this, the influence of Cyber Hackers in the 2016

US elections has been said to be enormous, which was won by Republican Donald Trump. There are many similar instances, which can be recalled in the recent past from India also. One example could be the Blackout in Mumbai which happened in October 2020 during which a later report suggested that the blackout happened because of

some Chinese hackers attacking the Control System of the city. This suggests how susceptible our cyber-surveillance system is to hackers. In recent years, there have been many reports also suggesting how Aadhar Data could be hacked and the personal information of many of our country's people has been prone to data fishing.

Way Forward

Indian authorities have so far been spending most of their resources tackling localised cybercrime while responding to major attacks on a case-by-case basis. Recognising these strategic dimensions of cyberspace, the PMO (Prime Minister's Office) created the position of National Cyber Security Coordinator in 2014, a

welcome first step. Indian civil institutions have their fire-fighting agencies while the armed forces have their insulated platforms to counter cyber-attacks.

Thus, the government among various other aspects of national security shall consider these factors as well, and bring in modern technology to tackle this situation as the issue of national-security failure now transcends boundaries in the age of the Internet.

