INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

IDSA COMMENT

The US' Surveillance Review Panel Report: An Assessment

Cherian Samuel

January 9, 2014

The Snowden revelations occupied the mind space through much of the past year, and more of the same may be expected over the coming year. Even if much of the focus of the Snowden revelations have been on issues ranging from civil liberties to espionage to how the US treats its allies, the biggest impact has been felt on cyber security, which has been shown to be all but non-existent in the face of a well-funded organisation like the National Security Agency (NSA) determined to exploit and even create vulnerabilities in pursuit of the narrow ends of espionage. The coming months would see the crystallisation of responses to these revelations both within the US and internationally. Much will depend on the Administration's response to the 300-page report issued by the 5-member review panel appointed by the President in August and which was released in December.[1] The members of the review group included a former cyber security advisor (Richard Clarke), a former deputy Director of the CIA, and three law professors.

The President's mandate to the review group was to assess "**whether**, in light of advancements in communications technologies, the United States employs its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while appropriately accounting for other policy considerations, such as the risk of unauthorized disclosure and our need to maintain the public trust."[2] Subsequently, this weak mandate was modified to consider "**how** in light of advancements in communications technologies, the United States **can** employ its technical collection capabilities…"[3]

The 46 recommendations in the report pull no punches in offering drastic solutions while addressing many of the issues that have come to the fore in the wake of the Snowden revelations.

[1] Available online at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[2] Presidential Memorandum -- Reviewing Our Global Signals Intelligence Collection and Communications Technologies, 12 August 2013. The White House, Available online at http://www.whitehouse.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec
[3] Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology, 27 August 2013. The White House, Office of the Press Secretary. Available online at http://www.whitehouse.gov/the-press-office/2013/08/27/statement-press-secretary-review-group-intelligence-and-communications-t

Inasmuch as balancing liberty and security is a dilemma for all democratic governments, the content of the report is relevant to discussions on similar issues elsewhere including India. It is another issue that no other intelligence agency would match up to the scale of the NSA's activities, aided substantially by the dominance of US companies in the domain of internet and communication technologies.

The Report provides a historical backdrop to the current controversy, quoting chapter and verse from the report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (more commonly known as the Church Committee) set up in 1976 after the excesses of the Watergate Affair. The CIA was prohibited from spying on Americans and the NSA and FBI were allowed to do so only under strict oversight. Despite the edifice of over-sight and control by a combination of high-level officials, rapid changes in technology have meant that the over-seers were way behind in comprehending the changes in laws and protocols. The committee notes that "Senior policymakers should determine the activities of intelligence agencies; senior policymakers are the only participants with the breadth of experience to make such decisions…" The fact remains that senior policy makers were the consumers of the content produced by the NSA and would perforce have had some inkling of where the information was coming from.

In the absence of sufficient political oversight, the NSA engaged in many acts, which, had they been done by other countries, would no doubt have resulted in punitive actions on the part of the US. It has placed the US in the uncomfortable position of undertaking the same actions that it has been accusing other countries of doing and weakening the very foundations of the open, global and secure cyberspace it has been propounding. Among the more egregious of these has been the deliberate weakening of security standards that underpin the integrity of data flows through cyberspace, and the forcible and voluntary co-option of US information security and data services companies in this exercise. With the credibility of all these companies in tatters, the NSA's actions will impact US companies for a long time to come.

The recommendations in the Report range from specific steps for re-structuring the NSA to ending mass surveillance as well as ways and means of making oversight more meaningful and transparent. It must be mentioned that even though the report is ostensibly about reforms and corrections to the way the NSA collects intelligence, it seems the Group could not resist the opportunity to take a swipe at its cyber adversaries as well. Recommendation 31 says, "The United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications." It then goes on to say that "Among those measures to be considered are: (1) Governments should not use surveillance to steal industry secrets to advantage their domestic industry; (2) Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise

manipulate the financial systems; (3) Governments should promote transparency about the number and type of law enforcement and other requests made to communications providers; (4) Absent a specific and compelling reason, governments should avoid localization requirements that (a) mandate location of servers and other information technology facilities or (b) prevent trans-border data flows." The last of these is what exercises US businesses the most, with emerging services such as cloud computing in jeopardy following efforts by governments across the world to ensure data protection and privacy.

While the Executive is at liberty to accept or reject the recommendations, the large number makes it easier for the government to pick and choose. The Obama Administration has already rejected a key recommendation; that since both the NSA and US Cyber Command have conflicting functions and conflict of interest, the NSA should be placed under civilian control and should be split from the US Cyber Command. In all probability, those recommendations relating to the privacy of non-US persons, such as extending the application of the Privacy Act of 1974 to foreigners, would be given short shrift. The Administration would be throwing out the baby with the bathwater if it were not to consider practical recommendations like streamlining the process for law enforcement authorities (LEAs) to obtain cooperation through the Mutual Legal Assistance Treaty (MLAT) process (Recommendation 34). Though the MLAT process is an improvement on Letters Rogatory in that it imposes an obligation on the US to respond to an LEA request, it is still, as the report notes, a slow and cumbersome process, with an average response time of 10 months. Practical and long overdue steps suggested include, a) creating an online submission form for MLATs, b) streamlining the number of steps in the process, and c) streamlining provision of the records back to the foreign country.

While global opinion still largely is in favour of an open and global cyberspace, fears of its fragmentation could well become a self-fulfilling prophecy if the issues brought out in the report are not addressed adequately and in a timely fashion.

Views expressed are of the author and do not necessarily reflect the views of the IDSA or of the Government of India.