IN FOCUS

06 May 2014

ROADMAP FOR UNITED STATES CYBER COMMAND AND ITS APPLICABILITY FROM INDIAN PERSPECTIVE

Ashish Gupta
Research Fellow, CAPS

United States Cyber Command (USCYBERCOM) reached full operational capability on 31 October 2010, with following mission statement : 'USCYBERCOM plans, coordinates, integrates, synchronises and conducts activities to direct the operations and defense of specified Department of Defense information networks and prepare to and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensuring US/Allied freedom of action in cyberspace and deny the same to our adversaries'[i]. On his confirmation hearing, when slated to head the newly created US Cyber Command in 2010, General Keith Alexander avoided publically answering all or part of 29 questions. His responses to these questions were classified, out of the close scrutiny in public domain.

Vice Admiral Michael S. Rogers, President Obama's nominee to run the National Security Agency (NSA), as well as to succeed Gen Alexander as the head of USCYBERCOM, on appearing before the Senate Armed Services Committee (SASC) on 07 Mar 14responded in writing to a similar set of questions very differently. He never once invokes the need to answer the questions put up to him in classified format. This is indicative of the change in the mindset of strategists to take a pathuntraversed rather than going down the beaten path for cyberspace operations. "The U.S. possesses superior military might across all war fighting domains, cyberspace included," Vice AdmiralRogers wrote. "In truth, however, there has been no large scale cyber conflict yet in history, and the state of strategy and execution of cyber warfare is evolving as we speak."Vice AdmiralMichael Rogers envisioned that, "All of the major combat commands in the United States military will soon have dedicated forces to conduct cyber attacks alongside their air, naval and ground capabilities The activation of these combat units would help counter the perception around the world that the United States is "an easier mark" for cyber attacks because it did not "have the will to respond."[ii]

Admiral Rogers assumed command of U.S. Cyber Command and became director of the NSA and the Central Security Service during a ceremony in Fort Meade on 04 Apr 14. He took the reins at tumultuous time, an offshoot of grave concerns in the intelligence community, a result of release of thousands of documents on Wikileaks by former NSA employee Edward Snowden related to highly classified NSA surveillance operations. Admiral Rogers reiterated that the key to success in the future would be synergeticpartnerships between USCYBERCOM and the NSA, the FBI, the Homeland Security and Justice Departments. From the inception of USCYBERCOM, there are certain issues which are still ambiguous. This ambiguity stems, not from the lack of clarity of mission or thought, but due to unconventional nature of expected warfare in cyber space. These are:

- *Use of offensive tools after commencement of an identified/ perceived attack.* Both, Gen Alexander and Admiral Rogers were guarded in their response on the use of offensive tools against an attacker after commencement of an attack. In Defence parlance, any such activity by its nature is defensive.
- *Use "offensive cyber weapons" in response to an attack without conclusively establishing identity of true perpetrators.* In response to this, Admiral Rogerswrote that, "If the 'attack' met the criteria approved by the President in our Standing Rules of Engagement, the military would exercise its obligation of self-defense. However, operationally, it is difficult to develop an effective response when we do not know who is responsible for an 'attack'."
- *Initiation of mitigating actions when the responsibility of an 'attack' cannot be attributed to a particular nation, group or individual.*
- *Developing a direct cyber deterrence policy*.There is an inherentdichotomy deeply embedded in this approach. For being effective, cyber weapons need to be secretly developed, evaluated and checked for efficacy. In response, Admiral Rogers wrote that, "The establishment of U.S. Cyber Command is an element of a deterrence strategy, but

more work and planning will be required to evolve a solid national strategy. Classic deterrence theory is based on the concepts of threat and cost; either there is a fear of reprisal or a belief that an attack is too hard or too expensive. Cyber warfare is still evolving and much work remains to establish agreed upon norms of behavior, thresholds for action, and other dynamics." Admiral Rogers further wrote, "A broad understanding of cyber capability, both defensive and offensive, along with an understanding of thresholds and intentions would seem to be logical elements of a deterrence strategy, both for our allies and our adversaries, and as they are in other war fighting domains."[iii]

AdmiralRogers's answers to the Senate Armed Services Committeebrought fore one of the most detailed public descriptions of how the United States is developing an offensive military capability to use cyber weapons.As per the statement of AdmiralRogers, the US Cyber Command priorities include:

- *Secure, "cyber robust" and "defensible" telecommunications architecture*. The limited capability of legacy information systems and some weapons systems, to withstand a dedicated and determined cyber-attackfrom an adversary determined to undertake operations detrimental to US interest, is still a matter of concern. There is a need to upgrade and incorporate "cyber robust" technologies in these systems.
- *Training cyber warfare personnel.* U.S. military personnel are not fully reared up to confront advance cyber threats. This is attributableto the lack requisite training and confidence in waging cyber war across its full spectrum. They also are not able to comprehend the levels of risk acceptable in the cyber domain and lack "reliable cyber situational awareness".
- *Intelligence on global cyber threats.* Admittance in cyber domain is easy costing only a pittance as compared to other war fighting domains. This has led to emanation of cyber threats from state-sponsored military operations and espionage activities, to extremist organizations, to cyber criminals and recreational hackers seeking financial gain and notoriety. Though it would be a herculean task to compile and collate data of all the individuals and groups capable of compromising US interest by acts committed in cyberspace, the availability of such data would ensure monitoring, tagging and confronting potential perpetrators.

- *Delegation of authority for conducting cyber attacks.*The authority for defending networks and conducting cyber-attacksis vested with many military and government, having different origins, objectives and orientations. This may result in failure to undertake concerted and collaborative efforts. Additionally, cyber warfare operating concepts are "undefined and not wholly realistic."
- *Defending government and private networks*. In recent past, cyber threats have transformed in their severities, complexities and rationality, shifting from temporarily disruptive attacks to extremely damaging cyber strikes capable of destroying data, threatening the economy and possibly endangering lives. Cyber Command also needs to proactively defend the networks from adversaries intending to stealing data, money, and other property.

The thoughts that echoed during the hearing might have emanated from the U.S.cyber threatperspective, but a closer scrutiny reflects its indelible universal applicability. Cyber attacks may occur with little or no warning and will allow onlya small window of opportunity to mount a defensive action seeking to prevent or deflect potentially significant harm to critical infrastructure. Any delay in seeking authority to act in response to such emergency actions could obviate the initiation any meaningful action. In India, the thought process for establishing an independent Cyber Command is underway, having persistent proponents in top military echelons. During his address on 22 Nov 13, Prime Minister Manmohan Singh highlighted the need for developing capacities to counter what he described as "global surveillance operation." The Prime Minister said:

> "*While globalization has induced growing and complex inter-dependencies among states and multinationals on the economic and trade front, it has also nurtured intense competition and rivalries in the security domain. Managing this contradictory tenor, which has been highlighted by the global surveillance operation mounted by the US National Security Agency, is also a policy imperative for us.*"[iv]

Cyber has enmeshed so intricately in military operations that it warrants elevating it to a unified command.To counter any threat, perceived or real, emanating from state-sponsored military operations and espionage activities or extremist organizations and cyber criminals, theobjective must be to acquire tangible national capacity, or what the lexicon now refers to as comprehensive national power. This needs to be aneffectuated by leveraging technological and industrial prowess at our disposal, bolstered by the appropriate military sinews.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies CAPS)

End Notes

[i] U.S. Department of Defense, Cyber Command Fact Sheet, available at: "http://www.stratcom.mil/factsheets/Cyber_Command/, 21 May 2010, accessed on 20 February 2014

[ii] "N.S.A. Nominee Promotes Cyber war Units", By Sanger 11 Mar 2014 available at: " http://www.washingtontimes.com, 11 March 2014, accessed on 13 March 2014

[iii] Ibid.

[iv] "India Debates Establishing Cyber Command", By VivekRaghuvanshi 22 Nov 2013, in "http://www.defensenews.com/article/20131122/DEFREG03/311220008/India-Debates-Establishing-Cyber-Command, 22 Nov 2013, accessed on 15 Apr 2014