Testimony of Admiral Michael S. Rogers and Implications for India

#1901 713 April 29, 2018 By P K Mallick

Admiral Michael S. Rogers is the Director of the National Security Agency (NSA), Commander of the U.S. Cyber Command (USCYBERCOM) and Chief of the Central Security Service (CSS) since April 3, 2014. He is going to be replaced by US Army's Army Cyber Command Chief Lt. Gen. Paul Nakasone. On 27 February 2018 Admiral Michael Rogers testified before the Senate Committee on Armed Services. In his prepared speech the Admiral explained the various progress made by the USCYBERCOM. This was his last testimony to the Senate.

In the USA the top officials of the Government are madae to undergo hearings before taking over, during the tenure and while handing over the responsibilities. They are grilled by the Senators and often asked very searching and sometime uncomfortable questions. The top official has to answer on his own without any support from his staff.

These hearings/testimonies give out lot of details about the US Government's policies and plan for future actions. This particular testimony has lot of relevance for us as at throws up number of questions which we should also consider.

Some of the highlights of his testimony are given in succeeding paragraphs.

The Cyberspace Environment. USCYBERCOM is providing support to the U.S. Central Command (USCENTCOM), U.S. Special Operations Command (USSOCOM), in Afghanistan, Iraq, Syria and other places in Africa and Asia.

Threat From Violent Extremist Elements.USCYBERCOM along with law enforcement agencies, intelligence and liaison partners tries to find and destroy the key nodes in ISIS and other violent extremist groups' online infrastructure and media operations.

Integrate Cyberspace Operations With Traditional Military Capabilities. China and Russia integrate cyberspace operations with the plans and capabilities of their traditional military capabilities. These two nations also count as peer or near-peer competitors in cyberspace.

Iran and North Korea. Iran and North Korea have growing capabilities in cyberspace. Though they have fewer technical tools, they employ aggressive methods to carry out malicious cyberspace activities.

Three Milestones. USCYBERCOM has achieved the following milestones :

Elevated to unified combatant command status.

The Cyber Mission Force(CMF), specifically of the 133 CMF teams, all of them will be attaining full operational capability by September.

USCYBERCOM will open its new Integrated Cyber Center and Joint Operations Center (ICC/JOC) at Fort Meade very soon.

US Cyber Command's Missions and Performance. The following was highlighted:

Ensured that no harm was done by the WannaCry and NotPetya malwares outbreaks.

The Cyber Protection Teams were engaged with testing own systems.It necessitated the Department of Defense to review the cybersecurity of critical defense capabilities like nuclear command and control, sensitive information systems and long-range strike assets.

Defended the United States against cyber threats to U.S. interests and infrastructure. Cyber capabilities can also disrupt and potentially deter non-cyber threats as well.

Cyber capabilities integrated with plans and operations across all domains to influence and shape adversary behaviour, during preparation as well as joint operations in a conflict.

The Joint Task Force has given important supporting fires to USCENTCOM and USSOCOM in the campaign. The right processes were built to integrate cyberspace operations as one piece of a complex and coordinated multi-domain military campaign.

Cyber Operations - Integrated Planning Elements (CO-IPEs) at each Combatant Command are being established at full operational capability within the next five years to plan, synchronize, integrate and de-conflict cyberspace operations with Combatant Command plans and operations.

The new Cyber Excepted Service helps to recruit, manage and retain cyber expertise in a highly competitive talent market.

USCYBERCOM personnel, hone their skills and their teamwork through increasingly realistic exercise scenarios and simulated network environments.

Awarded a contract for IT executive research services in September 2017 valued at over $500,000 to developedcapabilities required to equip the Cyber Mission Force.

Q&A Session

During the Question and answer session the Senators grilled Admiral Michael S. Rogers hard. Not surprisingly most of the questions were on Russian interference in the USA's electoral process in 2016.

Russian Influence Operations. Some of the searching questions were**:**

Russian President Vladimir Putin has reached a conclusion: There is little price to pay for his actions and they can therefore continue.

Whether Moscow was trying to obtain a strategic objective by influencing U.S. public opinion on elections.

"Have you been directed to go after the Russian attacks at their origin, given this strategic threat that faces the United States and the significant consequences you recognize already?"

Why he had not done more to counter Russian hacking and leaking in the runup to, and after, the 2016 election? It was time for the head of Cyber Command to request more authorities.

Russia defeated and humiliated USA in the cyber war.The US Government failed to protect US democracy. Where is the source of failure – imagination, policy, structure, personnel, leadership and investment?

Admiral Rogers defended deftly with the consummate skills of a lawyer. Many a times he said, "I'm an operational commander, I'm not going to tell the President what to do." Some of his answers were :

Be mindful of falling in the trap that just because someone comes at us in cyber that we have to default to immediately going back and doing the exact same thing. I've always believed we need to step back and think a little bit more broadly about it and just don't default — it's because of that, you know, that I have not done that to date".

Asked by Democratic Sen. Jack Reed if he has been directed by the President, through the defense secretary, to confront Russian cyber operators at the source, Rogers said "no I have not" but noted that he has tried to work within the authority he maintains as a commander.I think, in fairness, you can't say nothing's been done. But the point would be, it hasn't been enough.

They haven't paid a price at least that is sufficient to get them to change their behavior.I believe that President Putin has clearly come to the conclusion there's little price to pay here, and that therefore I can continue this activity.

I don't think we anticipated the level of aggressive behaviour we would see over time from Russian actors. Nor did the government appreciate how Russia would see information and influence warfare as a strategic imperative over time.

Everything, both as the director of NSA and what I see on the cyber command side, leads me to believe that if we don't change the dynamic here, this is going to continue and 2016 won't be viewed as something isolated. This is something that will be sustained over time.

There should be no doubt that Russia perceives its past efforts as successful and views the 2018 US midterm elections as a potential target for Russian influence operations.

Of Russia's strategic objective I believe they're attempting to undermine our institutions.The US is smart enough and strong enough to prevent Russian election hacking but not enough is being done.

As the head of the NSA, he has authority to collect signals intelligence on foreign adversaries and their activities. That's altogether different from attacking a hostile government. As the head of Cyber Command, he could execute offensive operations. But the commander in that job just can't start a hacking-and-leaking war against Kremlin without approval from above.Such operations would play a role in a broader military strategy requiring Presidential approval.

Elections are a state process. As far as Cyber capability is concernedthat is the responsibility of DOD, Department of Justice (DOJ) and Department of Homeland Security (DHS). That's the Executive Branch,that's federal, that's not state.

Other Issues

Some other cyber related issues which came up during the Q&A Session are:

Deterrence. Regarding US capability the questions asked were: what are the specific steps taken in the past to develop full range of these capabilities and how do they utilize the best minds in niche technology areas like Artificial Intelligence, Robotics. It was replied that USCYBERCOM had no direct role. Deterrence has multiple components in the form of Economic, political, diplomatic tools etc. Cyber is part of various options.

Nature of relationship between DoD and other agencies responsible for protection of critical infrastructure. Should USCYBERCOM have the responsibility for protecting critical infrastructures given the expertise and capability it has and the requirement of prioritization, resources and interagency cooperation.

Who is in charge in case of a catastrophy? DoD, Department of Home Land Security, FBI or the affected sector?

Lack of effective cyber doctrine at national level.

How to respond to data manipulation.

Need to rethink what is critical infrastructure. The election process was not a critical infrastructure.

Areas Needing Improvement

Capability Development. Tools, who will do what, what is the role of services.

Acquisition. Acquisition of technologies in cyber domain will have to be done outside the rigid existing acquisition framework.

Recruitment of Personnel. In the military side recruitment of talent exceeds expectation. For civilians, recruitment and retention are problem areas.Recruitment is now for people of military of today and not for military of tomorrow.

Number and Nature of Threat. State actors are becoming aggressive, the capabilities are growing, significant innovations are taking place.

Adversaries may buy foreign companies legally. This may have military applications.

USCYBERCOM is designed to carry out tactical operations.USCYBERCOM is not built to deal with content in information domain. For psychological operations and deception operations there are different branches. For conducting own information operations there is need for integration.

Implications for India

The testimony by Admiral Rogers is a source of some searching questions for us. Some of them couldbe :

Who Will Cary Out Cyber War. Intelligence agencies cannot fight war. The Rules of Engagement are different. That is why US CYBERCOM is responsible for cyber war. They take help of the expertise of NSA. In our case who will wageCyber War?

Cyber Command. There is no debate on the need of establishment of Cyber Command. Previous and present Governments have announced the raising of Cyber Command. Are we serious? What is the delay?

Adversary Capabilities. What are the cyber warfare capabilities of China and Pakistan? Has there been any collusion?

Offensive Capabilities. Do the India Armed Forces have the capability to wage cyber war against the adversaries?

Who is in Charge. If one of the critical infrastructures, say financial System, goes down in a cyber attack: who will be in charge to mitigate and take offensive actions.

Private Sector. If a big IT Industry is taken down by a cyber attack and that industry is able to retaliate against the attacking agency, what is the rule position? Does he attack? If he attacks what happens?

Responsibility. Who is responsible for cyber security of increasingly important Defence Industrial Bases including OFB, DPSUs and the concerned private sectors? Who audits DRDO networks and establishments? Who keeps a check on Cyber Security of Nuclear installations? Who is responsible?

Doctrine. What is our cyber warfare doctrine?

Critical Infrastructures. Is there any requirement to revisit the sectors designated as Critical Information Infrastructure? In today's networked digital world everybody is vulnerable. Do we consider health or election system critical?

Conclusion

This hearing gives a fair idea about functioning of USCYBERCOM. There are host of such issues which come out from this testimonial.All democratic countries grapple with similar problems in cyber domain. India is no exception. We needto introspect where we stand in organization, capability, development of tools in niche technology areas, innovation and R&D and host of other such issues in cyber domain.We should be able to take note of these and hopefully take appropriate measures.

[Maj Gen PK Mallick, VSM (Retd) has been a Senior Directing Staff(SDS) at National Defence College, New Delhi. He is an expert in Cyber Warfare, SIGINT and Electronic Warfare].

References

1. Statement of Admiral Michael S. Rogers Commander United States Cyber Command before the Senate Committee on Armed Services, 27 february 2018, available at :https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf

2. Maj Gen P K Mallick, Cyber Security in India- Present Status, Vivekananda International Foundation, Issue Brief – October 2017 available at : https://drive.google.com/file/d/1wnTK_0h6bQuKb9pBTCE5CdtMFvP7ZYnV/view