CNS Address at Cyber Security Seminar on 17 November 2017

1. Dr Gulshan Rai, the National Cyber Security Coordinator, Shri Alok Joshi, Chairman NTRO, Principal Staff Officers, Flag Officers, Officers, distinguished guests, members of the media, ladies and gentlemen.

2. It is indeed an honour and a privilege to deliver the Keynote Address at this seminar on a topic that is both contemporary to each one of us as well as increasingly relevant to the Armed Forces. At the outset, I would like to thank Dr Gulshan Rai for participating in this seminar on 'Cyber Security in the Context of the Indian Navy'.

3. I would also like to take this opportunity to congratulate the organisers, the Directorate of Information Warfare, for hosting this event. The theme for this Seminar is very topical and reflects institutional resolve to harden our cyber-systems and networks against emerging threats.

4. Regardless of where we are, in harbour or at sea, on routine patrol or forward deployed on an operational mission, we are never away from the all-pervasive nature of information connectivity. We are constantly connected to the grid, to receive or to transmit information. In such a situation, *Information Assurance* becomes paramount. We often tend to take this for granted. We do not have the luxury of being ignorant of or accepting lapses in 'information assurance', since shortfalls will invariably compromise the entire network and can even translate into real and immediate risks to the individual or the deployed platforms.

5. It would be an understatement if I say that the cyber-domain is one big, ever expanding, intriguing labyrinth. As the whole edifice has

numerous linkages, it makes it that much more difficult to have control and monitoring mechanisms.

6. Moreover, dependence on cyberspace is virtually absolute. This naturally creates proportional vulnerabilities. Therefore, both ‘security in cyberspace’ and ‘security of cyberspace’ have assumed increased importance. At the national level, there is a deep understanding of the threats, as well as our vulnerabilities. A number of measures have been initiated or are in the process of being implemented to specifically address the issue of cyber security. Let me share some of my thoughts on cyber security and the challenges for the Indian Navy.

7. Whilst a few countries have tried to impose controls in order to assert their sovereignty over the cyber space, such restrictions have proven to be largely symbolic. Cyber space is a breeding ground where new challenges manifest at an alarming pace. Moreover, cyber-attacks can be almost impossible to trace. As a result, attribution of the responsibility becomes very difficult, and this in turn limits the options that can be initiated.

8. We, in the Indian Navy, are progressing our capability and expertise to be able to identify the source of the attacks, assess the offensive capabilities of the adversary, and be capable of rapidly countering them. Our quest for capabilities towards identification of potential threats and offensive action against enemy’s information infrastructure, in pursuit of ensuring protection of own systems are essential to prepare for, and support military operations. While a lot has been achieved, there is more that can be done and this requires our

urgent attention especially when we consider the rapid advances that our adversaries are making in this domain.

9. Networked computer applications have shaped the way economies of the world function. The management of critical national infrastructures are increasingly being undertaken via the cyber-domain. In fact, the cyber-domain has also begun shaping the way the State interacts with its citizens. Militaries too are increasingly dependent on Information and Communications Technology (ICT) networks for conduct of operations, situational awareness and Network Centric Warfare.

10. We in the Indian Navy also use a large number of networks which can be subjected to cyber-attacks. While we have safeguards in place including maintaining air-gapped networks, we must be fully mindful that these air gaps are only notional, and can be bridged using a variety of technical means. It is, therefore, important that we keep up our guard to maintain the integrity of our networks, and remain constantly ahead of the curve.

11. Devices, hardware as well as software are being developed at a feverish pace. Vulnerabilities and tacit agreements between private developers only come to light when ‘system weaknesses’ lead to a major security breech. The exponentially expanding ‘Internet of Things’ ecosystem is further complicating the scene. Many of these, owing to their easy availability and utility find applicability within the Navy. We have laided down guidelines for vulnerability assessment of networks and systems prior to their introduction, so that we do not land up unknowingly as victims. While we can consider incorporation of suitable

security features in custom-made solutions, commercially available resources would need to be holistically examined for their integrity.

12. Social Media and easy availability of smart devices is facilitating communications between individuals, often in encrypted form, without government involvement, thereby giving them a sense of security to share anything and everything. Any compromise of operational information can inflict disproportionate and debilitating impacton our abilities. Therefore, we have processes in place to constantly educate and sensitise our personnel on the responsible use of social media, as also smart devices. Notwithstanding, there is aneed to evolve regulatory frameworks and monitoring mechanisms to ensure that the advantages of technology can be safely harnessed without it becoming an anathema.

13. There have been several instances of cyber-attacks targeting national infrastructure – some reported and countless others left in the realm of conjectures and imagination. Who can ever forget the famous STUXNET attack!

14. Cyber-warfare has emerged as one of the most viable options to cause disruptions without applying visible, physical force and even without the formal declaration of hostilities. The point I wish to make here is that, cyber security has become so important in the national security arena world over, that it has emerged as the fifth domain of warfare itself, after land, sea, air and space.

15. We in the Indian Navy are fully seized of the importance of cyber security. We need to continuously explore innovative means to continuously fortify our part of the cyber-space. More importantly, cyber security requires a top-down approach because security procedures of any kind, including cyber security are essentially inconvenient. Having said that, it is also important that from the organisational perspective, we accord the required thrust and commit human and material resources appropriately to bolster our capabilities.

16. In my view, there are five key aspects which will decisively influence cyber security.

(a) First and foremost would remain the adherence to laid down SOPs by all personnel. Awareness programmes will need to be continued at all levels, from Seminars such as these, down to the unit level, to reinforce the importance of cyber security.

(b) Secondly, we must accept that smart devices and widespread use of social media creates vulnerabilities that the individual is either unaware of or chooses to ignore. It is important for us as an organisation where security of information is paramount to constantly sensitise personnel on these aspects and create architectures to enable their safe use.

(c) Thirdly, security features need to be included right from the design stage for all custom made IT and networked solutions. This is critical, considering the fact that in future we will see increasingly networked operations.

(d) Fourth, we will need to invest in acquiring and honing skill sets to be able to achieve information superiority, especially in a net-centric battlefield.

(e) And finally, as cyber gets more integrated with security strategies, thresholds and countermeasures would need to be redefined.

17. Ladies and gentlemen, it is impossible to isolate ourselves from the cyber domain, either as individuals or as an organisation. The dangers of an insecure cyber domain can put all of us in peril. We, therefore have to create structures to leverage it in a secure manner. Success can only be achieved through consistent adherence to security standards by each one of us and a culture of accountability at every level.

18. In our continued efforts at cyber security, we need to target both the organisational procedures as well as personnel. After all, we are as strong as our weakest link!

19. I wish everyone fruitful and positive deliberations and once again congratulate the Directorate of Information Warfare for hosting this seminar. I look forward to reading your deliberation and the suggestions that emerge.

20. Jai Hind. *Śaṁ No Varuṇaḥ*.