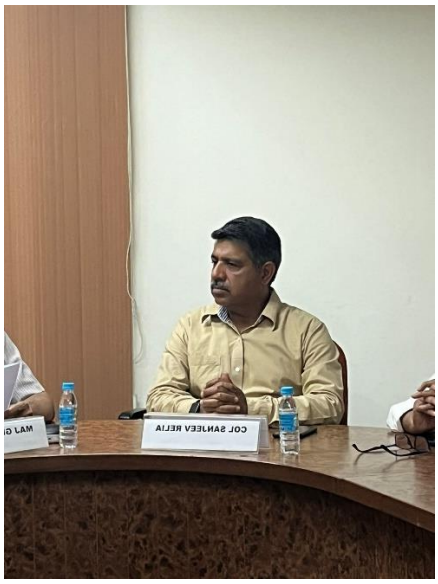
FINAL PRESENTATION BY COL SURAKSH VIR, SENIOR RESEARCH FELLOW, USI

ON "ENHANCING OFFENSIVE CYBER CAPABILITY AT NATIONAL LEVEL"

Time	Topic	Speaker
1400 hours	Welcome Remarks	Maj Gen RS Yadav VSM (Retd), Director, CS3
1405 hours	Guide's Remarks	Col Sanjeev Relia (Retd)
1420 hours	Scholar's Presentation	Col Suraksh Vir, Senior Research Fellow
1505 hours	External Discussant's Remarks	Maj Gen (Dr) Ajeet Bajpai (Retd)
1520 hours	Q&A Session	
1555 hours	Closing Remarks	Maj Gen RS Yadav, VSM (Retd), Director CS3

Key Takeaways:

- A potent offensive cyber capability works on continually collecting vulnerabilities within the systems, networks, or software to reach disruption-causing potential. Since such vulnerabilities are limited in nature, their timely and judicious collation requires a well-planned strategy. Kinetic operations employed in conjunction with cyber offensive attacks can prove to be highly lethal, precise, and efficient, as witnessed in Operation 'Lavendar', Operation 'The Gospel', etc.



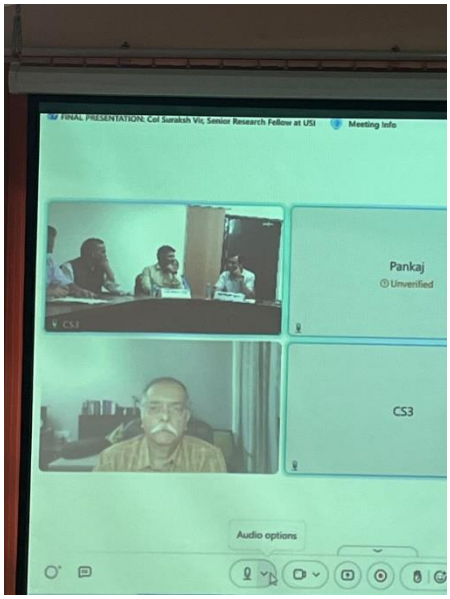
Guide's remarks by Col Sanjeev Relia (Retd)

Presentation by Col Suraksh Vir, Sr. Research fellow USI

- There are five tenets of an effective cyber operation, i.e., cyber defence, cyber deterrence, cyber-enabled influence operations, cyber exploitation, and offensive cyber ops. A strong cyber network defence (CND) forms the foundation for Cyber network exploitation (CNE) and cyber network attack (CNA). Therefore, for strong cyber offensive capabilities, it is advised to invest in CND infrastructure first. In this regard, India should become self-reliant in cyberspace by investing in its own operating system, semiconductor manufacturing facilities, standardisation and testing labs, and National Malware Threat Assessment and Intelligence Repository.

- Cyber operations are more suited to determine strategic interactions rather than tactical outcomes. Hence, developing a cyber network exploitation (CNE) strategy for cyber espionage and propaganda campaigns should be a priority, for which NIST 2.0 is a comprehensive policy framework. Furthermore, a cyber doctrine containing well-defined guidelines for threshold, escalation, and integration with other elements of Intelligence operations is necessary for developing Indian cyber offensive capabilities.

Welcome Remarks by Maj Gen RS Yadav VSM (Retd), Director, CS3



External Discussant's remarks by Maj Gen (Dr) Ajeet Bajpai (Retd)

- India should work on developing a single peacetime and wartime cyber construct by integrating all cyber institutions, both civil and military, under a single umbrella, which in turn would be governed by an Information and cyber doctrine. This body should work on CND, CNE, and CNA simultaneously for optimum cyber offensive capability. This central body should be tasked with capability assessment at regular intervals to keep pace with cyber advancements.

Distinguished Audience

Report by Manah Popli, Research Assistant, CS3, USI