STATEMENT OF CASE

PROJECT 'SARVAGYA' : GENERATIVE AI MODULE FOR REAL-TIME CYBER-SECURITY QUERY RESOLUTION AND CYBER THREAT AWARENESS TO BE DEPLOYED ON ACG WEBSITE (IN-HOUSE DEVELOPMENT)

1. **General**. In the dynamic and ever-evolving landscape of cyber-security, ensuring robust protection of critical infrastructure demands advanced real-time solutions that can swiftly adapt to emerging threats. Project 'SARVAGYA' an innovative generative AI-driven interactive module, has been developed by ACG, to revolutionize the Indian Army's cyber-security framework by providing immediate, precise responses to complex queries related to Indian Army cyber policies, guidelines, and adversarial open source intelligence. This cutting-edge solution leverages Natural Language Processing (NLP) to generate highly accurate, context-aware insights, enabling users at all levels to efficiently navigate through extensive, constantly updated database. By incorporating OSINT into its architecture, Project 'SARVAGYA' not only delivers comprehensive guidance on compliance but also offers a real-time view of the adversarial cyber threat landscape, enhancing operational readiness. Its secure offline deployment on ACG website ensures data integrity, while its intuitive interface empowers users to access actionable intelligence seamlessly. This tool will serve as a force multiplier, reinforcing the Indian Army cyber defenses and ensuring proactive, informed decision-making in an increasingly complex digital cyber-space. Approval of Project 'SARVAGYA' will fortify the Indian Army's cyber defense posture, making it a valuable asset in maintaining superiority in the cyber domain.

2. **Aim**. The aim of Project 'SARVAGYA' is to enhance the Indian Army's cyber-security capabilities by integrating a generative AI-driven interactive module with the ACG website. This module will deliver real-time, precise responses to queries related to cyber-security policies and adversarial intelligence. The In-House developed tool is an initiative to streamline access to vital information, improve policy compliance, and bolster operational readiness in an increasingly complex cyber landscape, ultimately reinforcing the Army's cyber defense posture against emerging threats.

3. **Deployment**. This module is designed to be integrated into ACG website, facilitating immediate access to cyber-security policies and guidelines.

4. **Proposal**. It is proposed to integrate an advanced AI-driven interactive module, Project 'SARVAGYA' with ACG website. This in-house developed system, trained on the comprehensive database of Indian Army cyber-security policies and guidelines, will deliver real-time, accurate solutions to user queries. Regular updates will ensure the module remains current. Operating securely in an offline environment with restricted access, this AI solution will enhance the Indian Army cyber-security posture and will boost policy compliance standards.

5. **Description** : **Project 'SARVAGYA'**

(a) **Model Overview**. Project 'SARVAGYA' is an advanced AI-driven interactive module designed to enhance cyber security management within the Indian Army. The system leverages a Large Language Model (LLM) trained on an extensive and continually updated dataset comprising Indian Army's cyber security policies, advisories, and guidelines. Additionally by incorporating an cyber OSINT database, the module will also provide a real-time picture of the cyber threat landscape and adversarial cyber intelligence. Hosted securely on ACG website, the module functions offline, ensuring secure access and protection of sensitive data. Its core purpose is to deliver real-time, precise solutions to user queries, streamline information retrieval, and promote better compliance with cyber security protocols.

(b) **Architecture and Operation**. The model architecture is built around the following key components:-

(i) **Large Language Model (LLM)**. The AI module utilizes a generative LLM optimized for natural language processing (NLP), enabling it to interpret and respond to queries in a human-like manner. The LLM is trained on a vast corpus of IA-specific data, including cyber policies, threat advisories, and procedural guidelines.

(ii) **Vectored Database**. Integrated with a vectored database, the LLM can search for contextually relevant information across multiple documents, ensuring comprehensive responses. The database will also include Open Source Intelligence (OSINT) updates, capturing adversarial cyber capabilities, latest trends, and vulnerabilities to provide a holistic threat landscape.

(iii) **User-Friendly Interface**. The module features an intuitive user interface, allowing users to input their queries easily. The generative AI will process these queries and generate relevant, context-aware responses, enhancing user engagement and accessibility.

(iv) **Query Processing and Response Generation**. Upon receiving a user query, the AI processes it using NLP techniques and retrieves information from the database, generating thorough responses that draw from all relevant sections. This ensures users receive comprehensive answers rather than isolated pieces of information.

(c) **Functions and Use Cases**. The AI module will serve various levels of users within the Indian Army:-

(i) **Policy Queries**. Immediate responses to queries related to Indian Army's cyber-security policy, guidelines and numerous advisories without referring large volume of pages physically.

(ii) **Cyber Threat Intelligence**. The users can get responses to their queries related to cyber threat landscape and adversarial cyber activities.

(iii) **Predictive Analysis**. The module will be able to carry out predictive analysis on relevant topics based on the database.

(d) **Secure Offline Operation**. Project 'SARVAGYA' operates in a completely offline environment, without any internet dependency, maximizing security by isolating the system from external networks. Controlled database access restricted to administrators only ensures only authorized personnel interact with the module database, further protecting data.

(e) **Application and Impact**. Project 'SARVAGYA' will revolutionize cyber security management within the Indian Army by providing a robust, AI-driven solution accessible to all levels of users. From junior personnel seeking clarification on policies to higher authorities requiring detailed guidance, the module will deliver precise and comprehensive solutions in real-time. By offering actionable responses and simplifying complex information, the system will foster better decision-making and operational readiness. The incorporation of cyber OSINT data will ensure a well-rounded understanding of adversarial capabilities, enhancing the Army's cyber defense strategies. In summary, Project 'SARVAGYA' is an essential tool for fortifying the Indian Army's cyber defense capabilities, supporting users at all levels in maintaining a secure and resilient cyber environment.

6. **Justification**. Project 'SARVAGYA' represents a pivotal advancement in the Indian Army's cyber-security arsenal, designed to meet the urgent need for rapid, precise access to cyber policies and intelligence. Leveraging advanced AI, including Natural Language Processing (NLP) and generative algorithms, the system delivers real-time, context-aware solutions from an extensive, ever-evolving database of cyber-security protocols. This ensures that both junior personnel and higher authorities can swiftly access actionable, comprehensive information to enhance decision-making in high-tempo, operational settings. Its secure, offline architecture safeguards sensitive military data, while the integration of cyber OSINT provides real-time insights into adversarial cyber capabilities, thus bolstering proactive threat anticipation and

mitigation. The intuitive user interface and seamless query processing foster rapid compliance with cyber-security protocols, mitigating vulnerabilities and improving the Army's overall digital resilience. The module is developed in-house; hence there is no development cost. Approval of Project 'SARVAGYA' will solidify Indian Army's cyber defense posture, ensuring operational superiority in the evolving cyber battle space.

7. **Financial Implication**. There are no financial implications as the module has been developed in-house, utilizing existing resources and infrastructure.

8. **Conclusion**. Project 'SARVAGYA' represents a cutting-edge application of Artificial Intelligence tailored to the Indian Army's cyber security needs. By providing real-time, comprehensive answers to queries related to cyber policies and adversarial intelligence, it significantly enhances the Army's cyber security posture. The incorporation of this AI-driven module will not only streamline access to vital information but also strengthen the Army's ability to respond to and anticipate cyber threats. In the dynamic cyber domain, where rapid response is critical, this project is a decisive step towards fortifying our defenses and ensuring operational readiness.

(Abhishek Lal)
Lt Col

Stn : C/o 56 APO

Dated : 25 Sep 2024

COUNTERSIGNED

Stn : C/o 56 APO

Date : 25 Sep 2024

ARMY CYBER GROUP
IHQ of MoD (Army)

Lt Col/ले. कर्नल
Sys Mgr
प्रणाली प्रबन्धक
Army Cyber Group
सेना साइबर समूह
Integrated HQ of MoD (Army)
एकीकृत मुख्यालय (सेना)