Big Data Analytics in Indian Navy

Kulshrestha, Sanatan

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Big Data Analytics in Indian Navy

indrastra.com/2017/08/Big-Data-Analytics-in-Indian-Navy-003-008-2017-0027.html

By Rear Admiral Dr. S. Kulshrestha (Retd.)
Indian Navy

Image Attribute: INS Vikramaditya in Baltic Sea / Source: Indian Navy

"The single most effective thing you can do right now to improve the security of your computer is to unplug it from the Internet. Pull out that Ethernet cable; throw the wireless router in the microwave. The vast, vast majority of infections that plague your machine will arrive via the Web ." - Omar El Akkad

Today, stand-alone computers and devices can be injected by viruses using drones and aircraft to cripple a nation's cyber capability. Air Gaps placed at critical points in cyber infrastructure does not provide protection against a cyber-attack anymore. U.S. has been flying **EC-130H *"Compass Call"*** on daily missions to deny ISIS military leaders and fighters the ability to communicate and coordinate defensive actions by shutting down their cell phones, radios, IEDs and very likely their new weapon of choice, drones.

Big Data management (Storage, Handling, Analysis, Transmission) is directly linked to its security. Big Data security involves, infrastructure security, data management, data privacy, and integrity & reactive security. The Government of India (GoI) has appreciated the all-pervasive nature of the cyber space domain and has therefore structured a holistic approach to the issues of Cyber Security and Big Data.

Cyber Security

The **Indian IT Act, 2000** defines *"Cyber Security"* as means for protecting information, equipment, devices, computer, computer resource, communication devices and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Also, the GoI recognizes that Cyberspace is vulnerable to a wide variety of incidents, where in targets could be the infrastructure or underlying economic well-being of a nation state. A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the

information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting the functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy, and national security.

On July 2, 2013, GoI released the **National Cyber Security Policy 2013** with the Vision *"To build a secure and resilient cyberspace for citizens, businesses and Government"*. The stated Mission is *"To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation".*

Some of the objectives of the policy are to; create a secure cyber ecosystem in the country, create an assurance framework for design of security policies, strengthen the Regulatory framework,enhance and create National and Sectoral level 24×7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, enhance the protection and resilience of Nation's critical information infrastructure by operating a 24×7 **National Critical Information Infrastructure Protection Centre (NCIIPC)** and mandating security practices, develop suitable indigenous security technologies through frontier technology research, improve visibility of the integrity of ICT products and services, create a workforce of 500,000 professionals skilled in cyber security in the next 5 years, create a culture of cyber security and privacy, develop effective public private partnerships, enhance global cooperation by promoting shared understanding.

Important agencies dealing with cyberspace include - **National Information Board (NIB)** which is an apex agency with representatives from relevant departments and agencies that form part of the critical minimum information infrastructure in the country. **National Cyber Response Centre – Indian Computer Emergency Response Team (CERT-In)** which monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. It maintains 24×7 operations center and has working relations/collaborations and contacts with various CERTs, across the globe. Within this infrastructure, NCIIPC act as a designated agency to protect the critical information infrastructure in the country.

Big Data Analytics

In India, **Department of Science and Technology (DST)**, under the **Ministry of Science and Technology and Earth Sciences** has been tasked to develop Big Data Analytics (BDA) ecosystem. DST has identified important areas for development of BDA ecosystem in India. Creation of the HR talent pool is the first requirement. This will require the creation of industry academia partnership to groom the talent pool in universities as well as the development of strong internal training curriculum to advance analytical depth. The Big Data Analytics program has five steps:-

- to promote and foster big data science, technology, and applications in the country and to develop core generic technologies, tools, and algorithms for wider applications in Government-owned or driven services.

- to understand the present status of the industry in terms of market size, different players providing services across sectors, SWOT of industry, policy framework and present skill levels available.

- to carry out market landscape survey for assessing the future opportunities and demand for skill levels in next ten years.

- to bridge the skill level and policy framework gaps.

- to evolve a strategic road map and micro level action plan clearly defining roles of various stakeholders such as government, industry, academia, and others with clear timelines and outcome for the next ten years.

National Data Sharing and Accessibility Policy (NDSAP) 2012 of DST is designed to promote data sharing and enable access to government owned data.

Big Data Analytics infrastructure development in India is being steered by the C-DAC (Centre for Development of Advanced Computing), Ministry of Electronics and Information Technology. State of the art hardware system and networking environment has already been created by the C-DAC at its various facilities. C-DAC's research focus in cloud computing includes design and development of open source cloud middleware; virtualization and management tools; and the end to end security solution for the cloud. A number of applications in C-DAC are being migrated to cloud computing technology.C-DAC regularly conducts Training on *"Hadoop for Big Data Analytics"* and *"Analytics using Apache Spark"* for various agencies including Defence.

Big Data Analytics with Hadoop from **Philippe Julio**

Indian Navy & Big Data Analytics

The Big Data Analytics infrastructure for the Indian Navy operates under the holistic approach of the Government of India with respect to Big Data Analytics ecosystem and cyber security.

Indian Navy has a robust naval network with thousands of computers connected to it. This naval network ensures information availability/ processing, communication services, service facilitation platforms, multi-computing platforms, resources/information sharing, data warehousing, and so on. However, Cyber Security and Network Integrity is crucial to protect the naval network from data theft, denial of service, malicious viruses/ trojans attacks, single point failure, data & network integrity loss, and active/ passive monitoring.

Indian Navy has **Naval Unified Domain (NUD)** or Enterprise Intranet, which is back bone of Indian Navy. All communications, internal to enterprises, are through NUD only. It offers secure, isolated, fast and reliable connectivity across navy. NUD network operates only on controlled data (no unknown data from other applications is permitted) which can be easily segregated and analyzed.

Vulnerabilities arise as personnel working on NUD may need to transfer data from the internet to NUD and vice-versa, which may lead to security breaches of NUD. Further, physical guarding of NUD network lines against Men-in-the-Middle Attack is a complex task since Naval units are located at different geographical locations. There is also a possibility of attacks carried out by sophisticated software and hardware technologies such as via a mirror port or via a network tap to undertake passive monitoring, active monitoring, and certificates replications and so on.

The applicability of big data analytics in the context of Indian Navy is very much in line with the developed forces in the world. There exists a requirement of efficient big data analytics in the fields of intelligence, operations, logistics, mobilization, medical, human resources, cyber security and counter insurgency/ counter terrorism for the Indian Navy. There is also the associated requirement to acquire the predictive capability to anticipate specific incidents and suggest measures by analyzing historical events.

However, due to nascent nature of big data analytics, its awareness is limited to a small number of involved agencies in the Navy. The benefits of big data in operational scenario decision making while safe guarding accuracy and reliability have not yet been internalized. Big data projects even at pilot scales may not be available currently. In the present situation, decision makers are not clear about the capability of big data, costs, benefits, applicability or the perils if any of not adopting big data.

Big data holds enormous potential in Naval Context to make the operations of Navy more efficient across the entire spectrum of its activity. The research and development necessary for the analysis of big data is not restricted to a single discipline and requires an interdisciplinary approach. Computer scientists need to tackle issues pertaining to inferences, statisticians have to deal with algorithms, scalability and near real time decision making. Involvement of mathematicians, visualizers, social scientists, psychologists, domain experts and most important of all the final users, the Navy, is paramount for optimal utilization of big data analytics. The involvement and active participation of national agencies, the private sector, public sector, and armed forces would ensure full exploitation of the potential of big data for the Indian Navy.

The need for today is to start feasibility studies and research programs in select fields in order of desired priorities, followed by pilot studies and thereafter adopting commercial off-the-shelf (COTS) hardware and make available big data analytic software suites.

About the Author:

RADM Dr. S. Kulshrestha (Retd.), INDIAN NAVY, holds expertise in quality assurance of naval armament and ammunition. He is an alumnus of the NDC and a Ph.D. from Jawaharlal Nehru University, New Delhi. He superannuated from the post of Director-General, Naval Armament Inspection in 2011. He is unaffiliated and writes in defense journals on issues related to Armament technology and indigenisation.

Cite this Article:

Kulshrestha, S. "Big Data Analytics in Indian Navy" IndraStra Global Vol. 03, Issue No:08 (2017) 0027
| **http://www.indrastra.com/2017/08/Big-Data-Analytics-in-Indian-Navy-003-008-2017-0027.html** | ISSN 2381-3652

AIDN0030820170026 / INDRASTRA / ISSN 2381-3652