Indian armed forces approach to managing ISR big data

Kulshrestha, Sanatan

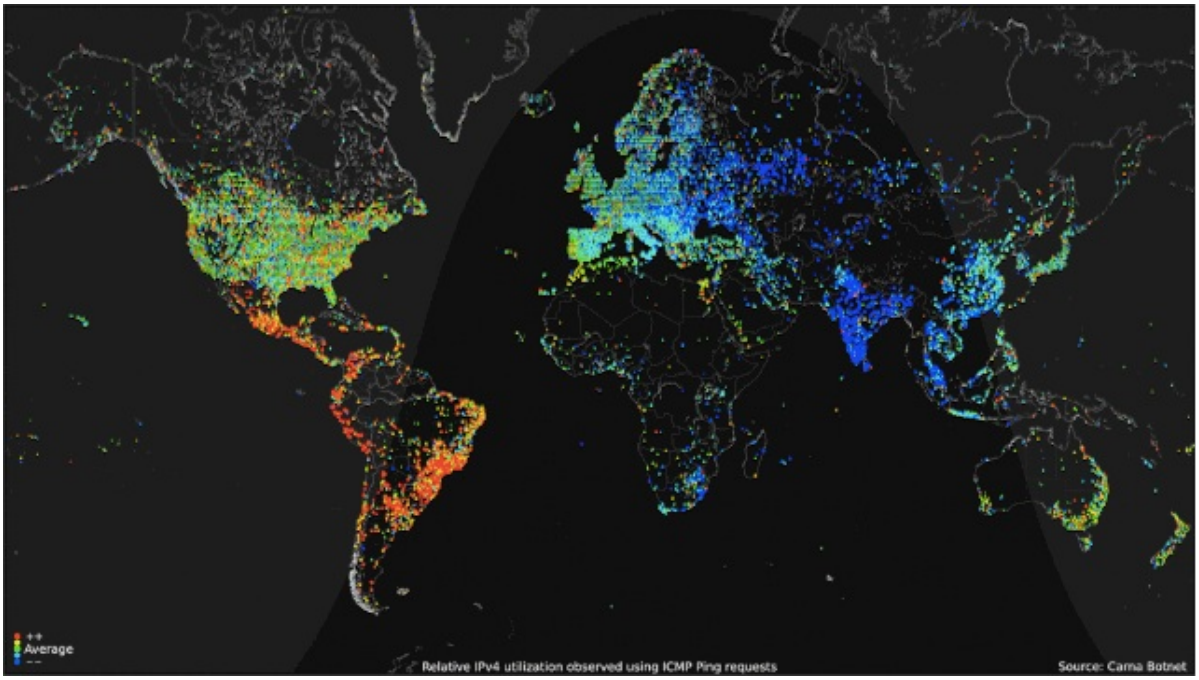
Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

TRANSCRIPT | Indian Armed Forces Approach to Managing ISR Big Data

indrastra.com/2016/10/TRANSCRIPT-Indian-Armed-Forces-Approach-to-Managing-ISR-Big-Data-002-10-2016-0050.html

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

Senior Fellow New Westminster College, Canada



GIF Attribute: Carma Botext

"Data really powers everything that we do." - Jeff Weiner, CEO, LinkedIn

Distinguished guests, serving and retired defense personnel, industry professionals, friends from the media, Ladies, and Gentleman, At the outset, I wish to thank The Royal Armed Forces of Malaysia, Tangent Link, and Association of Old Crows for providing me the opportunity to present this talk today.

My talk would touch upon aspects of

-Big Data- Definitions, scope, ambit

-Military Information and Intelligence

- National Security, ISR,

-Big Data and ISR

-Synergies with Digital Industry

-Security of Big Data

-& the Indian Context

Since, we have an enlightened audience here; I would go directly to the topic assigned to me and skip the general aspects of Big Data, which you all are aware of.

Military Information and Intelligence

National Security. Friends, Volume of data has expanded exponentially with the internet, especially in areas affecting national security like counterterrorism, network security, and counter-proliferation. There is a rapid influx of unstructured data relating to national security issues, as cyber defense requires both real-time and offline analysis. The handling of this data needs quick advances from system architecture to innovations in statistics. Large scale and in-depth querying of big data, visualization of big data in various forms like maps, graphs & timelines, and near real-time analyses of streaming data are some of the essential requirements for national security issues. Currently, Intelligence, Surveillance, and Reconnaissance programs, ISR in short, fall into three major categories of National Level, Joint Military Intelligence Level, and the Tactical Level. The Tactical ISR effort provides direct support to the military operations. However, in the recent years the consumers of ISR realize that the distinction between three types of ISR effort is blurring, this has been succinctly brought out in the Intelligence Resource Manager's Guide that, "As systems grow in complexity and capability and methods become more sophisticated, increasing numbers of intelligence assets are capable of simultaneously serving both national and tactical purposes."

The importance of information and intelligence for the military is apparent from the fact that it is fundamental to the planning of any military operation in peace or war. It forms the core component of the military kill chain. The Military uses a term Kill Chain to describe the sequence of events leading to the destruction of the target. It includes the steps of target detection and identification, dispatch of force or weapon to track it, decision making, and final command to destroy it. It is also known as F2T2EA cycle or the Find, Fix, Track, Target, Engage and Assess cycle. ISR is the key determinant of detection and identification of the target.

Reconnaissance and surveillance tasks have been carried out by militaries prior to mounting any assault on the enemy. The

success of the mission depends on upon the correct analysis of the available information during the planning stage. The collection of information, its analysis, and further dissemination is of prime importance for any military. Today the methods of collecting information have changed due to quick availability of combat information of high quality and reliability from a varied array of sensors and sources.

A definition of Intelligence, Surveillance and Reconnaissance (ISR) components taken from US Army manuals lists Intelligence as firstly, the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; and secondly, as information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. Surveillance is defined as the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. Reconnaissance is a mission undertaken to obtain by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. An optimal ISR plan is formulated by integrating the ISR missions based upon capabilities of various assets available. The information is thereafter collated and analyzed for feeding into the planning of operations.

Big Data and ISR

The basic information that is required by any commander in today's networked warfare is the accurate position of his own units, the location of the enemy and his reserves, the location of supporting units and placing of other miscellaneous assets. With this knowledge, a commander today can effectively carry out his mission by optimally utilizing the available firepower and resources. Thus crucial to any mission is 'situational awareness', which comprises tasking, collection, processing, exploitation, and dissemination. Embedded in the ISR is Communication without which no mission can be accomplished. Digital communication systems, the internet, and mobile devices have revolutionized the amount of data generation. The term Big Data in the military thus refers to a whole gamut of information available from sensors, video imagery, mobile phone, signals intelligence, and electronic warfare interceptions to satellite images. Data is being collected at unprecedented levels.

Rapid technological advances in sensor based, smart, and networked combat systems is pushing the military to adopt commercially available emerging technologies and adapt them for its use. The advent of big data is driving the armed forces to shift the integrated decision-making support systems to architecture and analytics of big data. The financial crunch faced by militaries in leading countries implies even more dependence upon technology by the reduced manpower. This, in turn, has led other nations to adopt a wait and watch strategy by which they would go in for the best available solution adopted by leading armies.

To understand and react to real-time tactical situations commanders have to manage and control big data environment comprising of, historical or point-in-time data, transactional [1] and ad-hoc use of the system. The military has been collecting data at humongous levels since the induction of unmanned vehicles with sensors. The data heaps cannot be analyzed in the traditional manner. They require dedicated data scientists and development of different software tools to exploit extracted information for mission planning. It is understood that in Afghanistan, the Defense Advanced Research Projects Agency (DARPA) had sent in data scientists and visualizers under a program called Nexus 7. They operated directly with military units and assisted commanders in solving specific operational challenges. In some cases surveillance and satellite, data was fused to visualize traffic flow through road networks to detect and destroy improvised explosive devices. Major issues faced by the military today involve the availability of ever-increasing volumes of sensor data from integral sources like UAVs and other national assets. The **US ARGUS-IS ground surveillance system** collects more than 40 Gigabytes of information per second. Spy satellites deployed by countries also generate gigabytes of geospatial data. It has become increasingly important for military officials to make sense of the vast amount of data that they are producing. A simple full day UAV mission can provide upwards of 10 terabytes of data of which only about 5% is analyzed and the rest stored.

Analysts are restricted by the download speeds of data depending upon their locations. Untagged data leads to downloading of similar data from other sources by the analyst to firm up their conclusions. Many times the communication lines are shared or may not be continuously available thereby increasing delays in the analysis. Providing a comprehensive situational awareness is dependent upon the accuracy and integration of data received from multiple types of sensors as well as intelligence sources. The screens and software tools do not have interoperability as of now. Due to security considerations, ISR data from different sources is stored in different locations with varying access levels, this leads to incomplete analysis. Single network domain providing access to data at multiple levels of security classification is not yet available. Analysts currently spend only 20 percent of their time looking at correct data, whereas 80 percent of the time is spent looking for the correct data.

Synergies with Digital Industry

This has led to a synergetic relationship with digital industry where in the military no longer develops its own hardware and software de Novo, but harnesses and modifies the 'commercial of the shelf' (COTS) items. Some common technologies in the big data ecosystem are, Apache Hadoop, Apache Hive / Apache Pig, Apache Sqoop, In-memory Databases, NoSQL Databases and MPP Platforms. Some of the companies working in this field which provide a common operational picture or COP for the military are :

Modus Operandi, which takes big data, infuses it with expert knowledge and creates a common framework for easy identification of patterns. Palantir Technologies, which is known for its software **Palantir Gotham** that is used by counter-terrorism analysts at offices in the United States Intelligence Community and United States Department of Defense.

SAP's Hana platform, provides a real-time analytics and applications platform for real-time big data that offers varying layers of security. It offers predictive, forecasting and calculation solutions and stitches together maintenance failure codes and document notes. To tackle the problem and analyze data in real time, Oracle has created a newly engineered system to handle big data operations. The company brought together its hardware with Cloudera's Hadoop, enabling patching of multiple layers of the big data architecture. United Data Architecture of Teradata is a comprehensive big data solution, which aims to bring data needed for analytics across the entire organization into one place to create a single version of enterprise data. DigitalEdge by Leidos is a scalable, pre-integrated, flexible, and pluggable data management platform that allows rapid creation and management of near real-time big data applications. Leidos's Scale2Insight (S2i) is a solution that supports large complex data environments with multiple disparate sensors collecting information on different parts of the data ecosystem.

SYNTASA delivers analytical applications focused on the behavior of visitors to internal government websites. The analytics, which is built on an open source big data platform, determine the behavioral trends of visitors in order to improve the use of information by government analysts.

Security of Big Data

Today all the Critical Networks whether in the Government Sector or Large Enterprises are being overwhelmed by new sophisticated attacks that blend malicious techniques. These attacks are aimed to steal critical confidential data and sensitive information, intellectual property, and can cost millions of dollars in remediation.

An advanced persistent threat, APT is a set of stealthy and continuous computer hacking processes, often orchestrated to target a specific entity. An APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over long periods. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

Unfortunately, Legacy Firewalls and Stand-Alone Threat Detection products fall short in addressing these challenges because they are not architecturally designed to effectively coordinate across threat disciplines or deliver the advanced protection and performance needed at the right place in today's modern computing environments. The most effective security solutions include powerful threat analysis capabilities that can collect data from all sources and automatically cut through the noise of terabytes of data to present the most relevant data. Integration of technologies and automated correlation capabilities of data is the key in this aspect.

One effective way of addressing the data security problem could be that,

-The sensors (e.g. NGFW[2]) are installed at all the data points to cover the distributed nature of big data. -The Security should be an end to end approach covering the perimeter as well as the end points for known as well as unknown threats.

-It should have unprecedented visibility into unknown threats, with the collective insight of thousands of global enterprises, service providers, and governments feeding the service.

- The Solution should be able to correlate and gain intelligence not only from the sandbox [3] and URL (Uniform Resource Locator) DB(Data Base) but also from third-party feeds, including closed and open source intelligence.

-Lastly, it should have a common point of management to control distributed network of sensors. Ability to view all sensor traffic, manage all aspects of device configuration, and generate reports on traffic patterns or security incidents.

Palo Alto Networks is a company working in the cyber-security domain and has become a leading APT provider, so much so that its Chairman & CEO Mark McLaughlin has been appointed as the 'Chairman' of the US NSTAC {National Security Telecommunications Advisory Committee}.

Indian Context

"Knowledge of the mechanics and details of big data analytics are not only important to exploit it but also to collapse the distances between policy, planning, and operations." - Lt Gen Anil Bhalla, DGDIA, and DCIDS (Int), in 2015

The applicability of big data analytics in the context of Indian defense forces is very much in line with the developed forces in the world. This has been brought out during the deliberations of various national level seminars organized by military think tanks. Center for Land Warfare Studies CLAWS, for instance, conducted a seminar titled Big Data–Applicability in the Defense Forces.

The outcome of the seminar resulted in highlighting the requirement of big data analytics in the fields of intelligence, operations, logistics, mobilization, medical, human resources, cyber security and counter-insurgency/ counter-terrorism for the Indian armed forces. It was highlighted that in the arena of intelligence examples of inputs likely to be received and analyzed during peace are related to terrorism, proxy war, left-wing extremism, the conduct of training by opponents, deployment of forces, and sponsoring of non-state actors. The seminar brought out the need for the development of algorithms to analyze millions of open-source documents generated and compare them with the gathered human intelligence. There is a requirement to acquire the predictive capability to anticipate specific incidents and suggest measures by analyzing historical events.

However, fact remains that due to nascent nature of big data analytics its awareness is limited to a small number of involved agencies. The benefits of big data in operational scenario decision making while safeguarding 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.

In June 2016, Comptroller and Auditor General who also overlooks various financial aspects of the Indian Armed Forces announced setting up a data analytics center — first of its kind by any auditor — for analyzing 'big data' in the government domain.

Conclusion

It is apparent that the era of Big Data is already here and its impact is being felt in all aspects of modern day life. The challenges at all stages of the data analysis include scaling, heterogeneity, lack of structure, privacy, error handling, timeliness, origins, visualization and data security. Big data holds enormous potential in India to make the operations of armed forces more efficient across the entire spectrum of their 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 military, 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 country.

The need today is to start feasibility studies and research programs in select fields in order of desired priorities, followed by pilot studies and thereafter adopting COTS hardware and available big data analytic software suites. With this, Friends I have finished what I had to say. Thank you all for being such a wonderful audience!

“Without big data, you are blind and deaf and in the middle of a freeway.” - Geoffrey Moore, author, and consultant

Thank you and Jai Hind!

About the Author:

REAR ADMIRAL DR. S. KULSHRESTHA (RETD.)
INDIAN NAVY

RADM Dr. S Kulshrestha retd. is a post grad in Physics. After joining the Indian Navy he specialized in Quality Assurance of Naval Armament and adorned various key appointments at Naval Command Headquarters, Defence R & D establishments, and Ordnance Factories.

He held the coveted position of the Director General of Naval Armament Inspection, Govt of India.

He holds a Doctorate from 'School of International Studies' at the Jawaharlal National University (JNU) New Delhi.

IndraStra™
www.indrastra.com

Publication Details:

This transcript is derived from a conference talk on Indian Armed Forces Approach to Managing ISR Big Data" by Rear Admiral Dr. Sanatan Kulshrestha,retd, Former Director General Naval Armament Inspection, Indian at Electronic Warfare Asia 2016, Kula Lumpur, Malaysia [Sep 20, 2016]

Kulshrestha, Sanatan. "TRANSCRIPT | Indian Armed Forces Approach to Managing ISR Big Data" IndraStra Global 02, no. 10 (2016) 0050 http://www.indrastra.com/2016/10/TRANSCRIPT-Indian-Armed-Forces-Approach-to-Managing-ISR-Big-Data-002-10-2016-0050.html. |ISSN 2381-3652|

Endnotes:

[1]. Transactional data, in the context of data management, is the information recorded from transactions. A transaction, in this context, is a sequence of information exchange and related work (such as database updating) that is treated as a unit for the purposes of satisfying a request.

[2] A Next-Generation Firewall is an integrated network platform that combines a traditional firewall with other network device filtering functionalities such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS).

[3] A sandbox is a testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control.

AIDN0021020160050 / INDRASTRA / ISSN 2381-3652

About IndraStra Global