ADVANCED TECHNOLOGIES APPLIED TO THE MODERN LOGISTICS OF MILITARY SYSTEMS/EQUIPMENT

Vasile ŞERBĂNESCU*, Atena VIȚĂLUŞ**

*Armaments Department

**Control and Inspection Corps

The nations that achieve cyberpower will command influence in global affairs economically, culturally, militarily, and politically in the decades ahead. Military cyberpower is the application of the domain of cyberspace to operational concepts to accomplish military objectives and missions, and influence operations, as well as warfighting. Infotronics Technologies intertwine advanced information and electronics systems intelligence and enable autonomous business functions and objectives through the use of internet and other tether-free technologies (i.e. wireless, web,…). The modern logistics of military systems/equipment imply core technologies such as Watchdog Agent for Predictive Prognostics, Web-enabled Smart D2B (device to business), Platform and Tools for Data Transformation, Optimization, and Synchronization, Applied Wireless Technologies and Logistics Infotronics Agent (LIA).

The hereby article argues that traceability, predictability and diagnosticability through advanced technologies will lead the armed forces to the life cycle logistics approach for interoperability and optimal cost of military systems/equipment.

Key words: life cycle logistics, cyberspace, robotics, logistics infotronics agent.

The cyber revolution is just the latest in a series of massive waves of "creative destruction" that arise when the convergence of new technologies, organizational models, and process innovations spawns new industries, remakes old economic sectors and in the process, creates new sources of economic, social, political, and military power.

The goal today is **cyberpower**, the ability to master and exploit the revolutionary capabilities of information and communications [3], while simultaneously keeping cyberspace secure. The nations that achieve cyberpower will command influence in global affairs economically, culturally, militarily, and politically in the decades ahead.

Each successive wave of technology constellations (e.g., the convergence of microprocessors, software, and digital networks during the current era) become the engine of economic growth and social change, creating new industries and transforming the underlying political-military systems. Older industries were displaced or transformed in a process that created new sources of competitive advantage and, often, new centers of geopolitical power.

Over the last 250 years, waves of "creative destruction" emerge around the convergence of new technologies and organizational innovations. These waves create new industries, transform the underlying social and political-military systems, and create new sources and centers of power, **Figure 1.**

These new waves included the ages of steam, iron, and railroads; steel, chemicals, and electricity; oil, autos, and electronics; and today, information and computer technologies, with the contours of the next wave around nano-biotechnology and robotics just emerging.

These industry waves follow a predictable sequence [3] that mirrors technology (S-curve) life cycles: incubation, irruption, frenzy, synergy, maturity, and decline, **Figure 2**. Likewise, the role of government follows a predictable pattern as these industries evolve. Incubation occurs when innovations are still in the research and development stage and where use is limited to early adopters.

Cyber is well within the synergy phase and stands ready to enter the maturity phase over the next few years. The recent reinvestment in fiber optic networks and cloud computing infrastructures reflects this transition.

The key questions are where will cyber be by 2020, and what is the appropriate role for government in capitalizing on cyber opportunities while keeping cyberspace secure?

The advent of the Information and Communications Technologies Age has created a new infrastructure - the Internet and a new domain called cyberspace - that has transformed how individuals, businesses and governments interact.

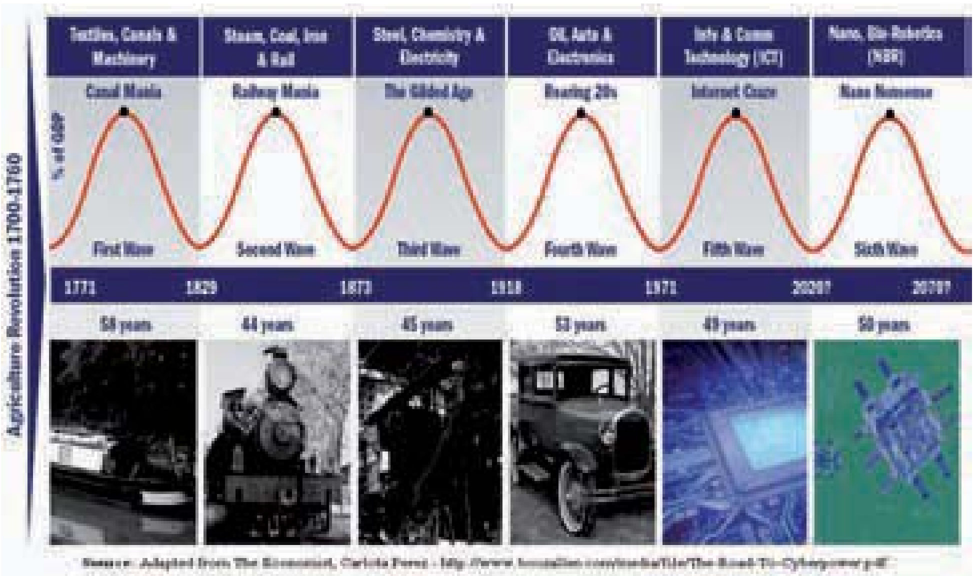

Fig.1. The waves of "Creative Destruction" - Next wave Nano / Bio-Robotics (NBR)

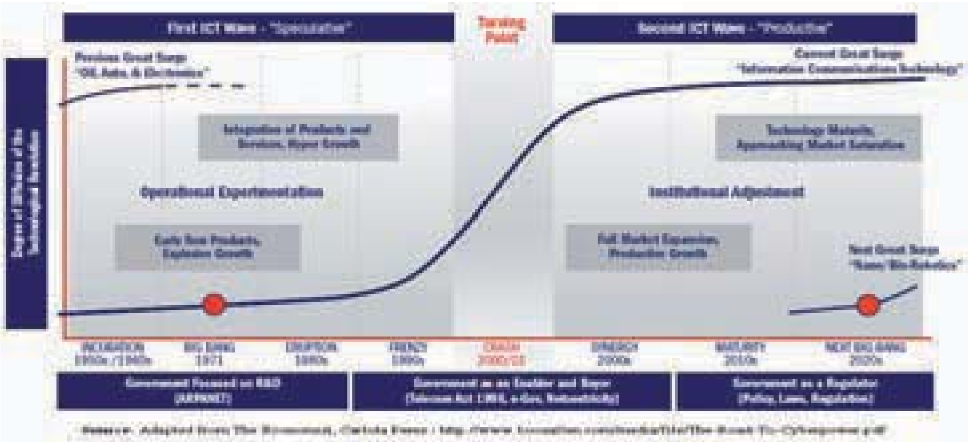

Fig. 2. Information Communication Technology (ICT) Evolution and Role of Government

Cyberspace is comprised of the networks, computers, software, hardware, and other devices (including cell phones and radios) that organizations and people use to store and exchange information across the globe; it includes the information and business processes that power the economy and allow individuals to connect and collaborate across organizational, social, and geographic borders. More importantly, while the Internet is focused on technology and operations, cyberspace is more comprehensive and includes policy and governance, technical standards, operations, human capital, and management.

The number of users and methods used to access cyberspace have grown exponentially in size, scope and complexity. By 2020, there will be almost 3 billion internet users (with most of the growth occurring in India and China), driving massive new investments in infrastructure, technology, and new security architectures, **Figure 3.**

Fig. 3. Cyberspace – Opportunities and Trends

Basic advancement in science and technology [7] come about twice a century and lead to massive wealth creation. **Nanotechnology** is an enabling technology that will impact all the economic sectors, including defence industries, **Figure 4**.

As we are only halfway through the ICT wave, we can expect dramatic changes over the next 10 years as new developments accelerate the growth of cyberspace in size, capabilities, and complexity. Among the expected trends:

- semiconductors will continue to miniaturize through nanoscale manufacturing, resulting in the proliferation of billions of "smart devices" and inexpensive laptops costing $100 or less;

- these new smart devices will collect and process information, accelerating the growth of data from 100 petabytes in 1990 to more than 3,000 exabytes by 2020, growing at a compound annual growth rate of over 50 percent a year and creating a data tsunami in the process;

- ubiquitous high-bandwidth networks - both wired and Wireless - will link mobile users, smart devices, and computing clouds to create an "Internet of things";

- global adoption of Internet Protocol version 6 (IPv6) will expand exponentially the number of IP addresses available for smart devices.

These and other developments are leading to what's commonly called the Web 3.0 stage of Internet development. Web 1.0 was about digitizing data and connecting people to information via the Internet. Web 2.0 saw the deployment of social – networking applications such as MySpace, Facebook, wikis, and Twitter, which connected people

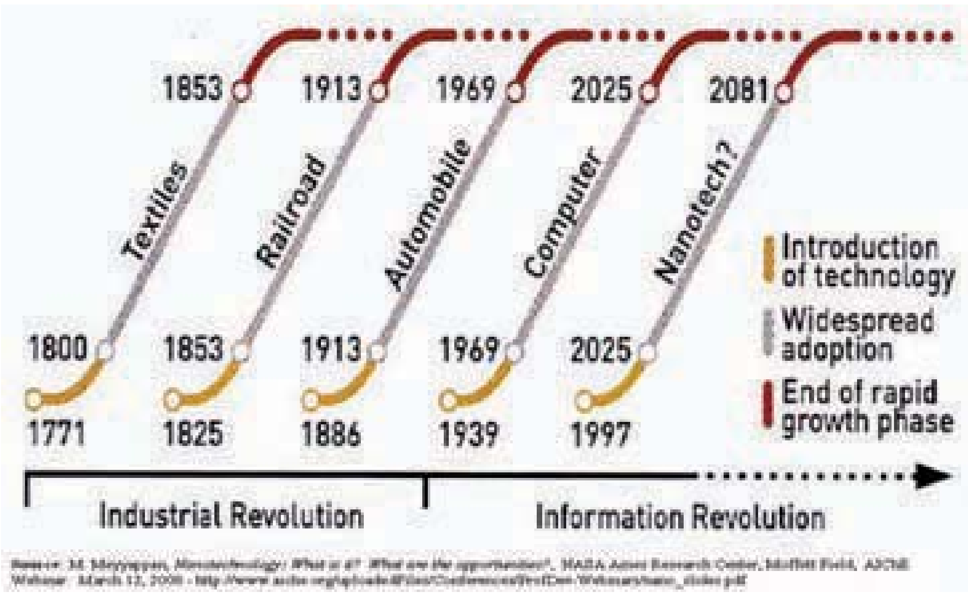

Fig. 4. Advancement in science and technology

to people, improving collaboration and creating new social ecosystems. Enabled by distributed clouds, the semantic Web technologies and other emerging applications, Web 3.0 will connect information to information in ways that significantly increase the amount and usefulness of the data collected.

Military cyberpower [6] is the application of the domain of cyberspace to operational concepts to accomplish military objectives and missions, and influence operations, as well as warfighting. Military administration, personnel management, medical care, and logistics are also enhanced by cyber tools. The growth in information technology and use of cyberspace has given the military new capabilities, but has also new challenges.

Military robots are used increasingly in wartime situations to reduce human casualties, being used for a mix of both combat against the enemy and non-combat roles [1].

The range of available military robots is huge, but a successfully one is **Multifunction Utility / Logistics and Equipment Vehicle (MULE)**. MULE [8] is an unmanned platform that provides transport of equipment and/or supplies in support of dismounted maneuver forces. The vehicle is designed to carry the load of two infantry squads, totaling about 2,000 pounds (907 kg), and support troops with water and power sources for extended operations, **Figure 5**.

Fig. 5. Multifunction Utility/Logistics and Equipment (MULE) - Unmanned Ground Vehicles (UGVs)

The MULE will be a "follower" to the human team. Each of the team members will be able to order the MULE to come forward, to support the operation. Otherwise, the vehicle will maintain a safe distance behind the team, waiting for orders. The MULE can communicate with and sometime, deploy unmanned aerial and ground vehicles (UAV/UGV) to give the squad members a true 360 degree image of the battlefield.

In 2008 LOCKHEED MARTIN displayed the latest configuration of the MULE which recently received new wheels, utilizing springs made of composite materials, instead of inflatable tires. Currently at an engineering evaluation phase, MULE is expected to mature into a full scale development system and be ready for deployment with the first Future Combat Systems (FCS) units of action, around 2013-1014. The company expects a requirement for 1,530 vehicles, based on current Army plans.

In the last 30 years, evolution in product, manufacturing and quality (**Figure 6**) implied some important „steps" from intelligent mechatronics (data & control intelligence) to product that thinks and links (information & computer intelligence) and products that learn, grow, reconfigure, and sustain (knowledge & distributed intelligence), or from factory automation (flexibility) to enterprise integration (agility) and e-logistics & e-manufacturing (velocity) with near-zero-downtime & sustainability and asset optimization [5].

The characteristics in the evolution [4] of product and service value imply for infotronics systems IT - embedded autonomous service, smart and predictive systems and zero-breakdown productivity (**Figure 7**).

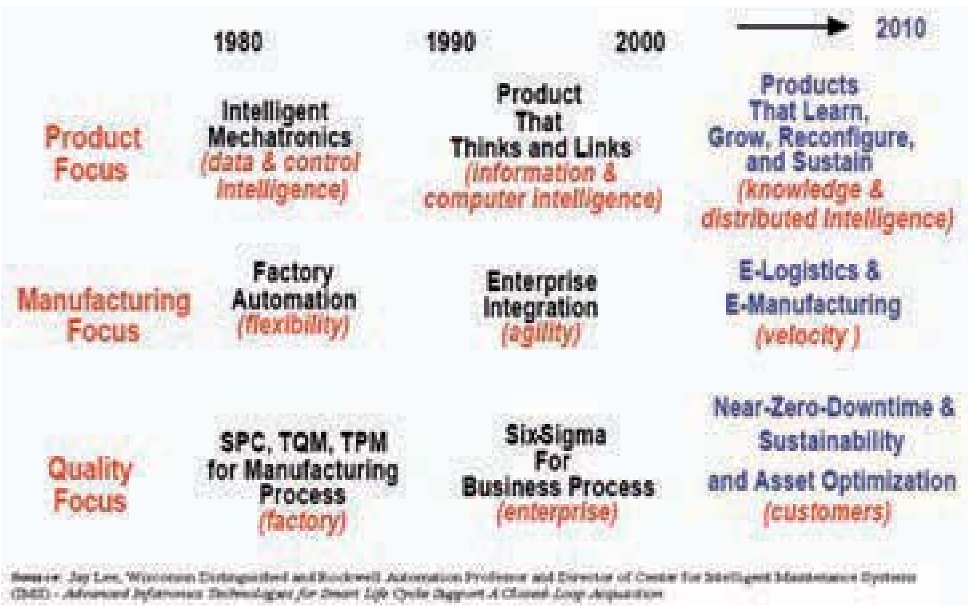

Fig. 6. Evolution in Product, Manufacturing and Quality

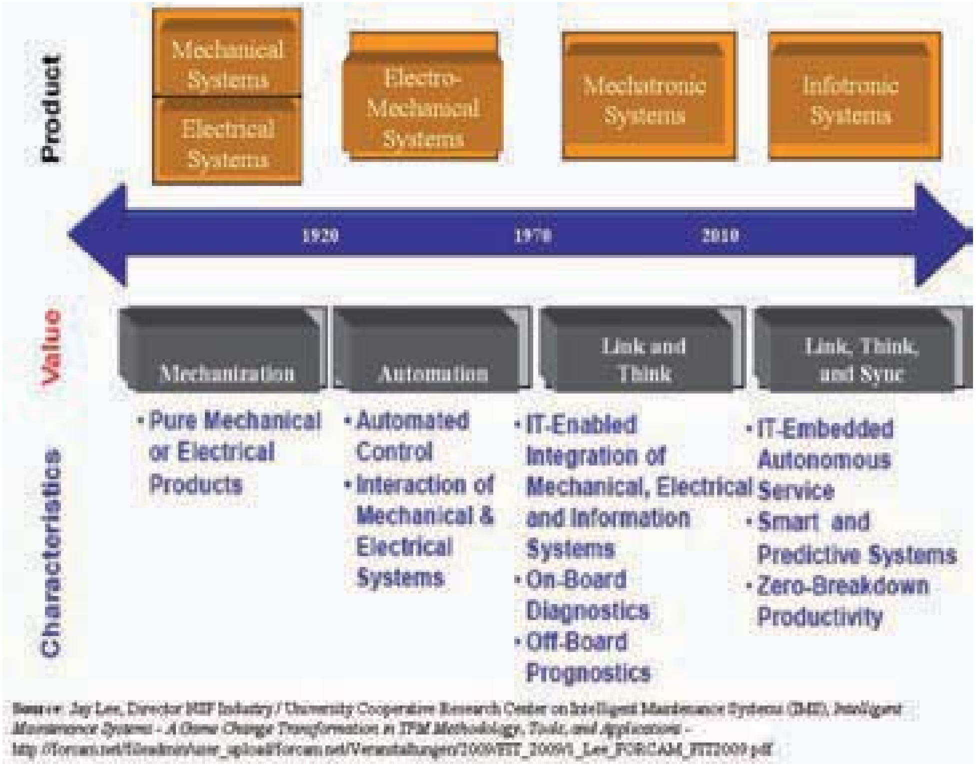

Fig. 7. Evolution of Product and Service Value

Autonomous logistics processes are an approach to face the current challenges in logistics by use of modern information and communication technologies (ICT) and novel decision-preparing and decision-making tools. Risk management is needed to make the autonomous logistic processes reliable and robust against suddenly appearing events which were not considered during the planning phase of the logistic processes. The ongoing development of modern ICT, e.g., telematics, mobile data transfer, and transponder technology open new opportunities for the development and emergence of intelligent logistic systems which can satisfy the requirements of autonomous logistic processes. The main technical challenge of autonomous logistic processes is the realisation of autonomous decision taking in logistic entities that have no reliable connection to a central control system.

However, in order to maintain a controllable dynamic logistic system, the technological development needs not only to provide autonomous replacements in the short-run for standard logistic operations, but it must also take into account that introducing autonomy will impact the operational and strategic management of logistic services. In this respect, the vision [5] on smart life cycle support for military systems/equipment is presented in **Figure 8**.

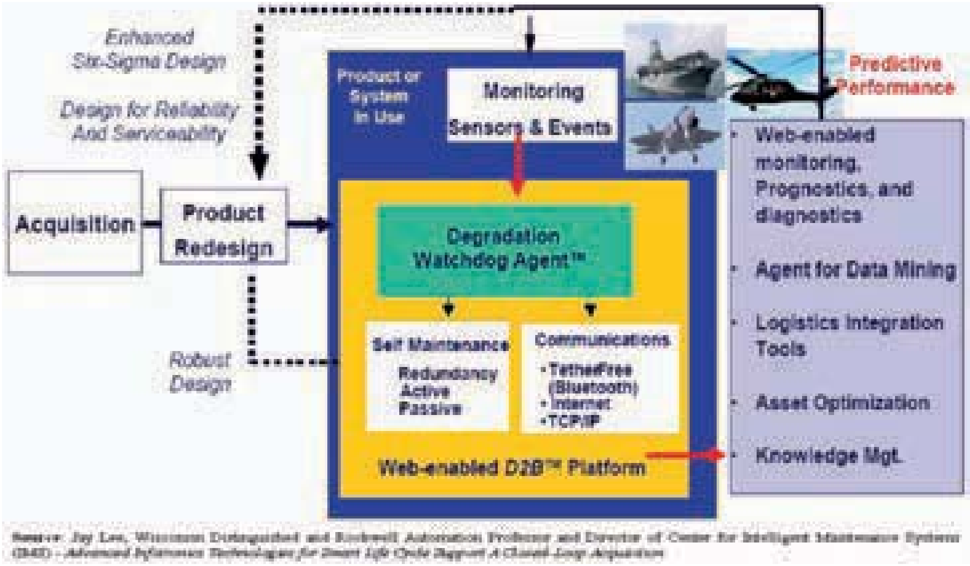

Fig. 8. Vision on smart life cycle support for military systems / equipment

The Watchdog Agent is a toolbox of algorithms that can autonomously asses and predict the performance degradation and remaining life of machines and components. This information can be fed to a closed-loop product life-cycle management system, **Figure 9**. The Watchdog Agent provides machine level intelligence and is synchronized with the operation and synchronization level intelligence. It includes signal processing and feature extraction, diagnoses, performance prediction, and performance assessment modules.

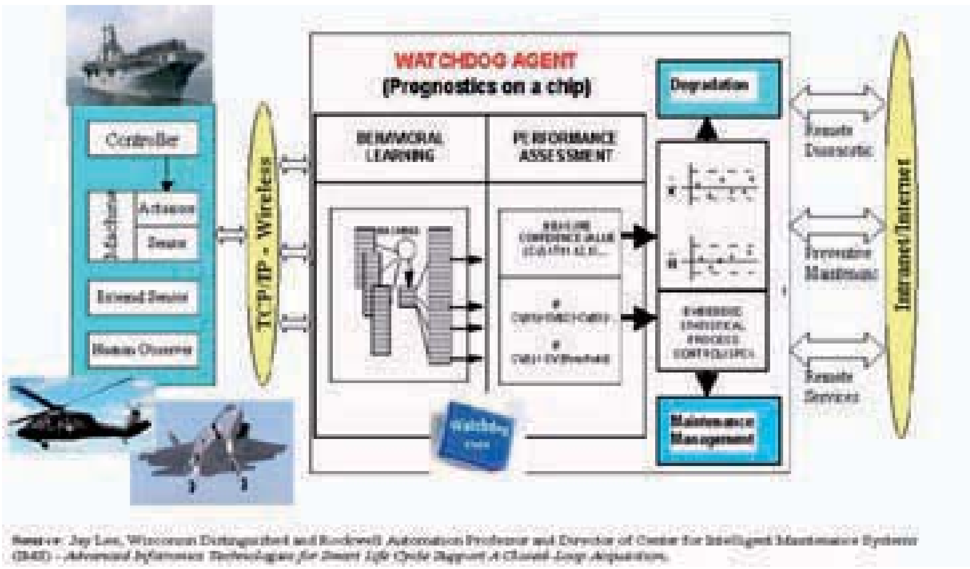

Fig. 9. Watchdog Agent – Prognostics on a chip

The toolbox consists of tools such as Neural Networks, Fourier Transform, Support Vector Machine, Self-organizing Maps, Fuzzy Logic, Logistic Regression, Hidden Markov Models, Bayesian Belief Networks, Match Matrix, Autoregressive Moving Average, Time-Frequency Analysis, in addition to others.

The Next Step: Self-Maintenance. The ability of a machine to adjust its own functionality according to its health status is an integral part of a self-maintenance paradigm. Self-maintenance requires both functional intelligence and health intelligence. This information can be fed into a functional intelligence module – e.g. controller – and the machine's operation can be adjusted accordingly. The purpose of self-maintenance is to provide enough time for maintenance personnel to become available and proper downtime to be scheduled.

Infotronics Technologies intertwine advanced information and electronics systems intelligence and enable autonomous business functions and objectives through the use of internet and other tether-free technologies (i.e. wireless, web,…). The modern logistics of military systems/equipment implies core technologies such as Watchdog Agent for Predictive Prognostics, Web-enabled Smart D2B (device to business), Platform and Tools for Data Transformation, Optimization, and Synchronization, Applied Wireless Technologies and Logistics Infotronics Agent (LIA), **Figure 10**.

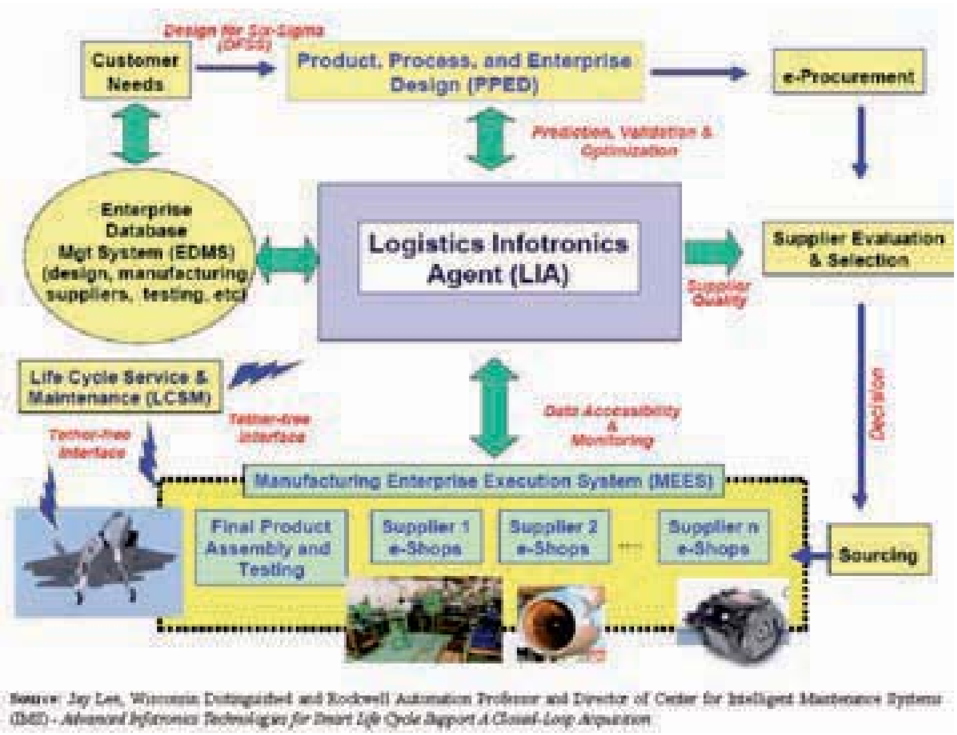

Fig. 10. Logistics Infotronics Agent

Advanced infotronics technologies for smart life cycle support (**Figure 11**) means firstly the utilization of tether-free interface.

Advanced technologies applied through the life cycle logistics of the major military equipment (**Figure 12**) involves the approach in terms of programme management, systems engineering, supportability analysis, integrated logistic support elements, logistics engineering and reliability, availability, maintainability, testability, predictability and diagnosticability for the interoperability and optimal cost of major military equipment.

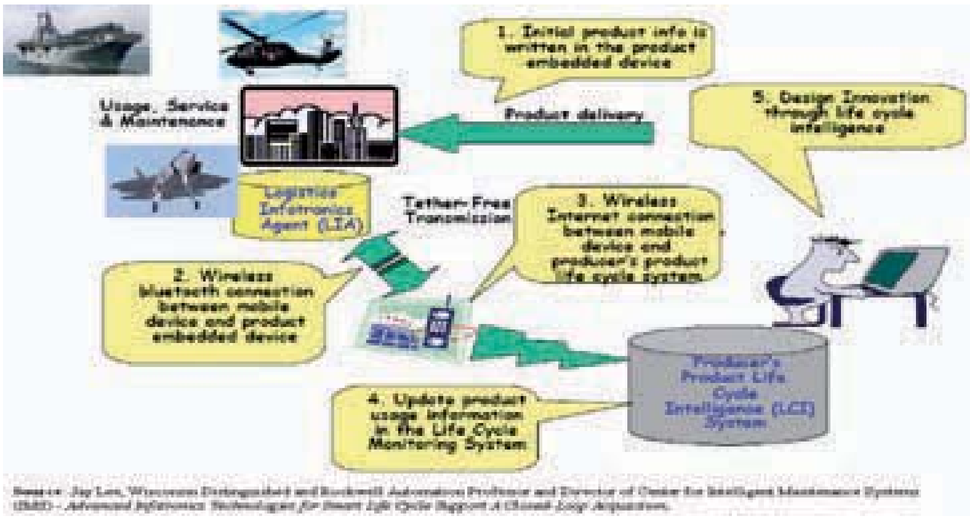

Fig. 11. Advanced Infotronics Technologies for Smart Life Cycle Support

Fig. 12. Life cycle logistics of major military systems

For the near future traceability, predictability and diagnosticability through the advanced technologies will lead the armed forces to establish a guidance on the life cycle logistics of the military systems/equipment, **Figure 13**.

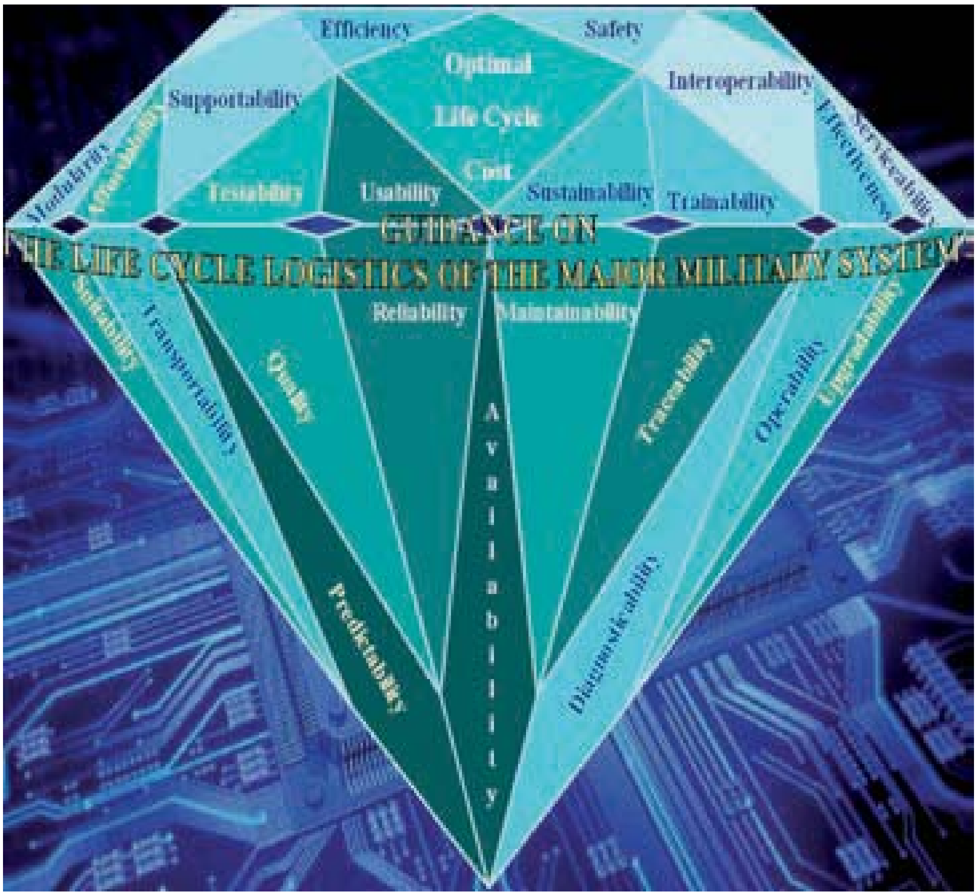

Fig. 13. Guidance on the life cycle logistics of the major military systems

REFERENCES

[1] *An Introduction to Military Robots*, http://www.robotmatrix.org/military-robot.htm

[2] Booz, Allen, Hamilton, *The Road to Cyber Power – Cyber Age , Cyberspace, Cyberpower, Cybersecurity, Commercial / Goverment Action*, Christopher Newport University, October 28, 2009.

[3] Booz, Allen, Hamilton, *The Road to Cyber Power – Seizing Opportunity While Managing Risk in the Digital Age*, 2010.

[4] Jay Lee, Director NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), *Intelligent Maintenance Systems - A Game Change Transformation in TPM Methodology, Tools, and Applications*.

[5] Jay Lee, Wisconsin Distinguished and Rockwell Automation Professor and Director of IMS - *Advanced Infotronics Technologies for Smart Life Cycle Support A Closed-Loop Acquisition.*

[6] Larry K. Wentz, Charles L. Barry, Stuart H. Starr - *Military Perspectives on Cyberpower* - Center for Technology and National Security Policy at The National Defense University Washington, DC, July 2009.

[7] M. Meyyappan, *Nanotechnology: What is it? What are the opportunities?*, NASA Ames Research Center, Moffett Field, AIChE Webinar, March 12, 2008.

[8] Multifunction Utility/Logistics and Equipment, http://defense-update.com/products/m/mule-load-carrier.htm.