NATIONAL DEFENCE UNIVERSITY "CAROL I"

REGIONAL DEPARTMENT OF DEFENSE RESOURCES MANAGEMENT STUDIES

NEW TRENDS IN INFORMATION RESOURCES MANAGEMENT

Workshop unfolded during the postgraduate course in Information Resources Management

13- 14.12.2010, Brasov

Coordinator:
LTC Prof. eng. Daniel Sora, PhD

BUCHAREST 2011

Scientific board:

LTC Professor eng. Daniel Sora, PhD

LTC Senior Lecturer Cezar Vasilescu, PhD

Junior lecturer Aura Codreanu, PhD

ISBN: 978-973-663-953-1

CONTENT

THE TWO WINGS OF REVOLUTION IN MILITARY AFFAIRS

MAJ Laurian GHERMAN

INTRODUCTION

The subject of military transformation has expanded to the point that it transcends focused discussion. From a cult phenomenon among military historians, government officials, and policy analysts in the 1980s and 1990s, the concept has morphed into a 21st-century all-purpose explanation for military decision making. It provides a rationale for expanded foreign policy objectives. Further, it has been adopted as a touchstone by the Department of Defense (DOD), especially the civilian leadership, to justify weapons programs and operational approaches. Finally, it has been the object of scholastic attention. Transformation is thus in danger of being the most oversold military-strategic concept since deterrence. A vast academic and military literature and extensive policy-related discussion have raised important questions about U.S. military policy, strategy, and war. Transformation, as understood by Pentagon planners and the political leaders, has the potential to improve military performance in important ways. But it is far from a guarantor of strategic success or sensible policy choices at the margin. This discussion asks pertinent questions about what transformation means and explores its implications for policy and strategy issues that have both immediate and longer-term importance. The most important transformation in the Armed Forces since World War II was the change from a draft to an all-volunteer force (AVF). Related was the deliberate shift in the relationship between the Active and Reserve forces.

The first change, ending the draft and creating the all-volunteer force in the 1970s, really made possible the American military preeminence of the latter Cold War, post–Cold War era (1990s), and early 21st-century. Those who fail to see this have put the cart before the horse, crediting technology with accomplishments that rightly belong to an empowered military with smarter and more motivated people. The all-volunteer force obtained quality personnel who not only enlisted but also reenlisted at unprecedented rates. This improvement was critical for enhancing the quality of the force, for reenlisted provided the nucleus from which the senior sergeants, chief petty officers, and other drivers of combat effectiveness in the field were recruited. Although the AVF recruitment had a rocky beginning in the 1970s, by the end of the Reagan years the military, compared to its 1950s or Vietnam counterparts, was unrecognizable in terms of the motivation, cognitive ability, and leadership skills of its junior officers and enlistees.

Military innovation is both top-down and bottom-up. For technology to find its way into military transformation it must impact on doctrine, organization, and training related to combat. DOD and service leaders must push from the top. Technologies not owned by any service or supported by high-ranking officers have little chance of survival. Joint technology development requires collaboration across services and high-octane promotion from the Office of the Secretary of Defense. DOD and service technology development programs are part of the larger budgetary process, which Congress ultimately controls.

Technology means nothing in war if it is lodged with a general staff that is remote from the field forces and rankers who must apply it for more effective fire and maneuver against an enemy. Soldiers are the best arbiters of mission effectiveness, and the lower the rank, the more ground truth is obtained. The validation of technology effectiveness in terms of mission requires smart soldiers who are empowered to speak frankly. "Zero defects" mentalities or preformatted "lessons learned" are killers of the initiative required for a fast-moving, quick-thinking, and cyber-smart military. Even before the information age, militaries that encouraged lower-level initiative and responsibility were rewarded with superior performances. The German armed forces in the World Wars are examples.

Command was optional prior to the information age. Armies could still prevail under a totally top-down system that treated the enlisted soldier and junior officer as serfs, as the Soviet army did in World War II.

I. INFORMATION MANAGEMENT

I.1 Network centric warfare

DoD transformation seeks to reorient us and focus our attention on emerging and future missions, change the way we fight (operate) to leverage Information Age concepts and technologies, and change our business processes to make us an Information Age organization.

Transformation is about continuous adaptation to the Information Age. A report to Congress on Network Centric Warfare began its executive summary by saying that "Network Centric Warfare is no less than the embodiment of an Information Age transformation of the DoD." This transformation must focus on C2, where information is translated into actionable knowledge. Without a transformation of C2, it is far less likely that we will be able to meet the challenges that lie ahead. A transformation of C2 provides us with the best opportunity to achieve the one organizational characteristic that is sure to stand us in good stead for the foreseeable future– agility. Armed with a general understanding of the concepts of Information Superiority and Network Centric Warfare, enterprising individuals and organizations are developing new ways

of accomplishing their missions by leveraging the power of information and applying network-centric concepts.

Two key realities dominate thinking about *command and control* (C2) in the 21st century. The first is the nature of the 21st century military mission space. This space is characterized by its extreme uncertainty. In addition to the high intensity combat operations that are traditionally associated with military operations, the 21st century mission space has expanded to include a wide spectrum of mission challenges, ranging from providing support to multi-agency disaster relief operations to complex coalition efforts within a political-military environment involving a large variety of military and non-military actors; which we describe as *Complex Endeavors*.

The second reality is the ongoing transformation of 21st century militaries, and for that matter, other 21st century institutions and actors from the Industrial Age to the Information Age. With this transformation comes the ability to leverage new information technologies. This has had, and will continue to have, a profound effect on how institutions manage themselves and how they can work with coalition partners.

These fundamental realities put the emphasis on command and control (C2), interpreted in its broadest sense to include acquiring, managing, sharing and exploiting information, and supporting individual and collective decision-making. In particular, more mature C2 includes the ability to recognize situational change, and to adopt the C2 approach required to meet that change — which we term *C2 Agility*.

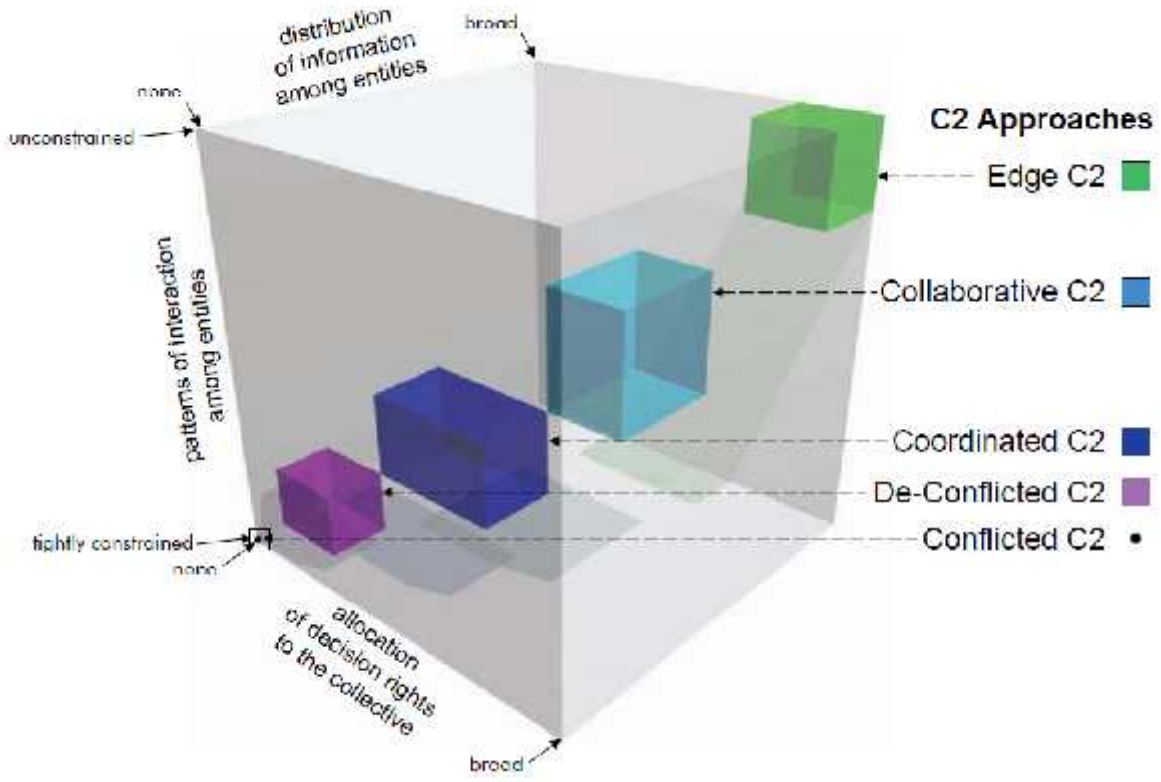


Fig. 2 C2 Approaches as regions in the C2 Approach Space

The C2 approach space contains the different possible approaches to accomplishing the functions that are associated with command and control. This approach space can be viewed from two perspectives. First, it can be used to think about C2 within existing organizations. Second, it can be used to think about how a disparate set of independent (yet inter-dependent) entities, that is, a collective, can achieve focus and convergence.

We define NCW as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battle space.

I.2 Information warfare

Information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology, such as networks and computer databases, which enable the military to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power. The current DOD term for military information warfare is “Information Operations” (IO).

DOD information operations are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives. The focus of IO is on disrupting or influencing an adversary’s decision-making processes.

DOD identifies five core capabilities for conduct of information operations; (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare. These capabilities are interdependent, and increasingly are integrated to achieve desired effects.

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Deception guides an enemy into making mistakes by presenting false information, images, or statements. MILDEC is defined as actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to take (or fail to take) specific actions that will contribute to the success of the friendly military operation.

OPSEC is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities.

CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications.

EW is defined by DOD as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring. Directed energy weapons amplify, or disrupt, the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems. DOD now emphasizes maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future communication systems, sensors, and weapons systems.

This may include: (1) navigation warfare, including methods for offensive space operations where global positioning satellites may be disrupted; or, (2) methods to control adversary radio systems; and, (3) methods to place false images onto radar systems, block directed energy weapons, and misdirect unmanned aerial vehicles (UAVs) or robots operated by adversaries.

I.3 Electronic warfare

Electronic Warfare (EW) is the struggle for control of the electromagnetic spectrum to assure that friendly forces can use the spectrum to their full potential in wartime, while denying that use to enemies. Military operations are executed in an information environment increasingly complicated by the electromagnetic (EM) spectrum. The electromagnetic spectrum portion of the information environment is referred to as the electromagnetic environment (EME). The recognized need for military forces to have unimpeded access to and use of the EME creates vulnerabilities and opportunities for electronic warfare (EW) in support of military operations.

EW includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

EA involves the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

ES is the subdivision of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. ES is differentiated from signal intelligence (SIGINT) [which comprises communications intelligence (COMINT) and electronic intelligence (ELINT)], even though all of these fields involve the receiving of enemy transmissions.

The differences, which are becoming increasingly vague as the complexity of signals increases, are in the purposes for which transmissions are received.

- COMINT receives enemy communications signals for the purpose of extracting intelligence from the information carried by those signals.
- ELINT receives enemy noncommunication signals for the purpose of determining the details of the enemy's electromagnetic systems so we can develop countermeasures. Thus, ELINT systems normally collect lots of data over a long period of time to support detailed analysis.
- ES, on the other hand, collects enemy signals (either communication or noncommunication) with the object of immediately doing something about the signals or the weapons associated with those signals. The received signal might be jammed or its information handed off to a lethal response capability. The received signals can also be used for situation awareness that is, identifying the types and location of the enemy's forces, weapons, or electronic capability. ES typically gathers lots of signal data to support less extensive processing with a high throughput rate. ES typically determines only *which* of the known emitter types is present and where they are located.

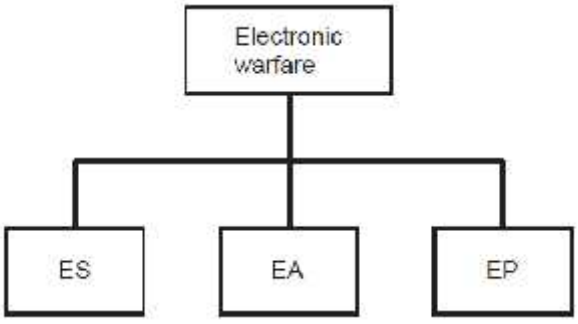


Fig. 3 EW subdivisions

The basic principles of the electromagnetic spectrum are fairly simple. Scientists have identified four fundamental forces that define the universe. Three of them — the strong force that binds atoms, the weak force that decays atoms, and gravity — are not readily manipulated by humans.

The fourth, electromagnetism, is the one fundamental force that humans have found relatively easy to channel, store, modify and apply for various purposes.

Scientists generally divide the spectrum up into seven segments. Radio waves are in the lowest-frequency, longest-wavelength segments of the spectrum. Other, higher frequencies can transmit more information in a given space of time, but they degrade quickly in the atmosphere and therefore require a dedicated conduit, such as an optical cable, to maintain their integrity. The radio-frequency segment of the spectrum has traditionally been the principal battleground within which electronic warfare is waged. However, many of today's advanced military systems are utilizing other segments of the spectrum.

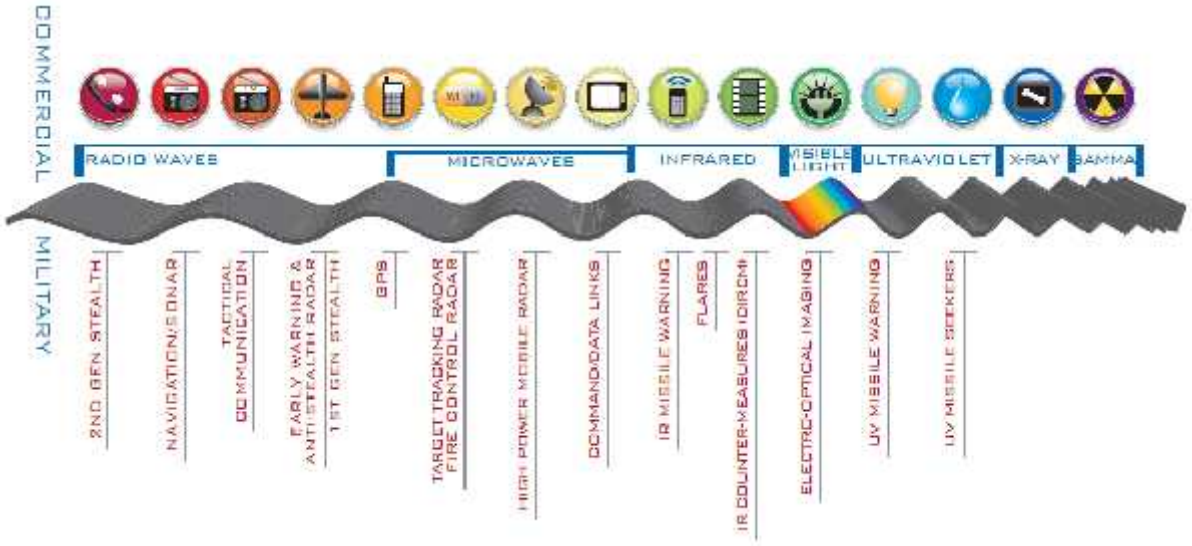


Fig. 4 The electromagnetic spectrum

Control of the spectrum is a strategic capability that confers great power and will be necessary for every conflict in the foreseeable future.

II. ELECTRICAL WEAPONS

II.1 Weapons platform digitization

From a broad perspective the introduction of networking techniques into war fighting systems is the military equivalent of the digitization and networking drive we observed in Western economies between 1985 and 1995. Military networking, especially between platforms, is far more challenging than industry networking due to the heavy reliance on wireless communications, high demand for security, and the need for resistance to hostile jamming. The demanding environmental requirements for military networking hardware are an issue in their own right. It should come thus as no surprise that the introduction of networking into military environments has proven more painful and more protracted than the industry experience of over

a decade ago. At the most fundamental level networking aims to accelerate engagement cycles and operational tempo at all levels of a war fighting system. This is achieved by providing a mechanism to rapidly gather and distribute targeting information, and rapidly issue directives. A high speed network permits error free transmission in a fraction of the time required for voice transmission, and permits transfer of a wide range of data formats. In a more technical sense, networking improves operational tempo (optempo) by accelerating the Observation-Orientation phases of Boyd's Observation-Orientation-Decision-Action (OODA) loop. The four components of the OODA loop can be split into three which are associated with processing information, and one which is associated with movement and application of firepower. Observation-Orientation-Decision is information centric while Action is kinematic or centered in movement, position and firepower. If we aim to accelerate our OODA loops to achieve higher operational tempo than an enemy, we have to accelerate all four components of the loop. Much of twentieth century war fighting technique and technology dealt with accelerating the kinetic portion of the OODA loop. Mobility, precision and firepower increases were the result of this evolution. There are practical limits as to how far we can push the kinetic aspect of the OODA loop - more destructive weapons produce collateral damage, faster platforms and weapons incur ever increasing costs. Accordingly we have seen evolution slowdown in this domain since the 1960s. Many weapons and platforms widely used today were designed in the 1950s may remain in use for decades to come, the B-52 being a good case study. The ultimate limit on the combat effect produced by a war fighting system, and thus is capability, is bounded by the Action or 'kinetic' phase of the loop. Bombs or missiles delivered are the bottom line, and networking is a tool to facilitate this effect, it is not a substitute for bombs and missiles on target as some proponents of NCW publicly advocate.

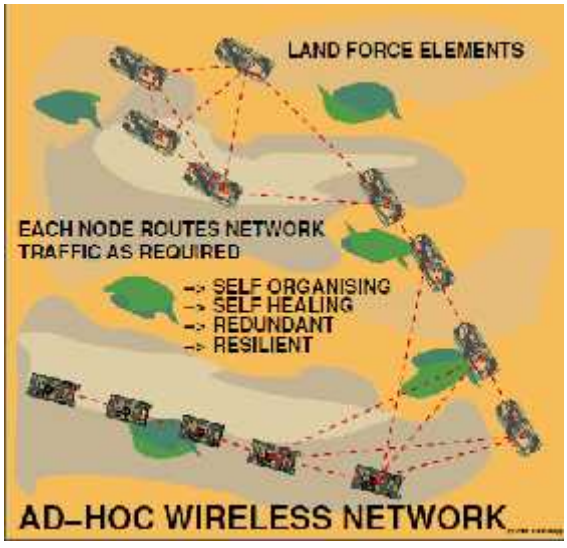


Fig. 5 Classical platforms with data communication abilities

II.2 Mobility

Warship designers until now have used hydraulics, pressurized air, and steam to move large masses, such as aircraft catapults, aircraft elevators, and ship propulsion systems, yet new advances in high-power electronic devices may lead to all-electric power aboard surface vessels. The latter half of the past century saw nuclear power, computers, and precision-guided rocketry greatly increase the capabilities and killing power of naval warships. While those technologies improved through the decades, the next evolution in ship design is expected to alter naval maritime architectures so dramatically that it has been compared to the transition from sail — to steam — to nuclear power.

This next evolution, called advanced electrical power systems (AEPS), involves the conversion of virtually all shipboard systems to electric power — even the most demanding systems, such as propulsion and catapults aboard aircraft carriers.

AEPS, in short, will provide the foundation upon which to build fleets of all-electric ships — otherwise known as AESs. Ship designers are already working on all-electric ship concepts in programs such as:

- the U.S. Navy's next-generation destroyer, known as DDG 1000 Zumwalt;
- the British Royal Navy's Daring-class Type 45 destroyer;
- the French navy's Forbin-class Horizon future anti-air warfare frigate;
- the Italian navy's Bergamini-class Horizon frigate.

Also planned as an all-electric ship is the CVN-21 (CVN-X) next-generation U.S. Navy carrier, currently in Phase II design and scheduled for launch around 2011 to 2013 to replace the then half-century-old USS Enterprise (CVN 65). The CVN-21's new nuclear reactor not only will provide three times the electrical output of current carrier power plants, but also will use its integrated power system to run an electromagnetic aircraft launch system (EMALS) to replace the current steam-driven catapults. Combined with an electromagnetic aircraft recovery system (EARS), EMALS will enable the new carrier to conduct high-intensity aircraft launch and recovery operations consistently with minimal recovery or maintenance downtime.

The amount of power that an electric motor generates, stores and distributes throughout a vessel, in tandem with an integrated "fight-through" power (IFTP) system designed to function despite combat damage, is essential to the operation of the next generation of warships, due to the enormous amount of electrically powered components they will carry. These include computing systems for functions such as network-centric warfare and onboard automation; powerful surface and underwater sensors and dual-band radar units; "plug-and-play" modules that upgrade operational capabilities during the life of a ship; launch and guidance of conventional armaments such as the 155mm. Advanced Gun System and Tomahawk cruise missile; and new armaments

such as directed-energy weapons and rail guns, which are still on the drawing board. An electric motor and the IFTP system also will manage energy more efficiently than the gas-turbine power plants, gearboxes and related mechanical components they replace. This is because software developed for use with the IFTP system regulates energy distribution to the propellers and elsewhere in the ship. Rather than having conventional turbine engines dedicated to propulsion and configured to deliver maximum power in anticipation of a rare command for flanking speed, energy will be channeled as needed to the propellers, computing systems, radar, sensors and weapons, as well as to the ship's "hotel loads" (i.e., electric lights, water-purification system, and cooking and cleaning appliances).

The efficient distribution of energy is one way that an electric propulsion system reduces fuel costs. Though the unit is still powered by gas turbines, the ability to adjust energy needs according to demand reduces fuel consumption.

There are other benefits, such as longer periods between refueling, which increase cruising range, and a reduced infrared signature due to lower emissions of exhaust gases. Moreover, since an electric propulsion system has fewer mechanical components than conventional turbine motors, it doesn't require as many personnel for operation and maintenance, which fits in with another goal of the DDG 1000 ships--reduced crew size (though this will largely be achieved by extensive automation). The Zumwalt is designed for a crew of 142; the Arleigh Burke-class destroyer, by contrast, has a crew of 341.

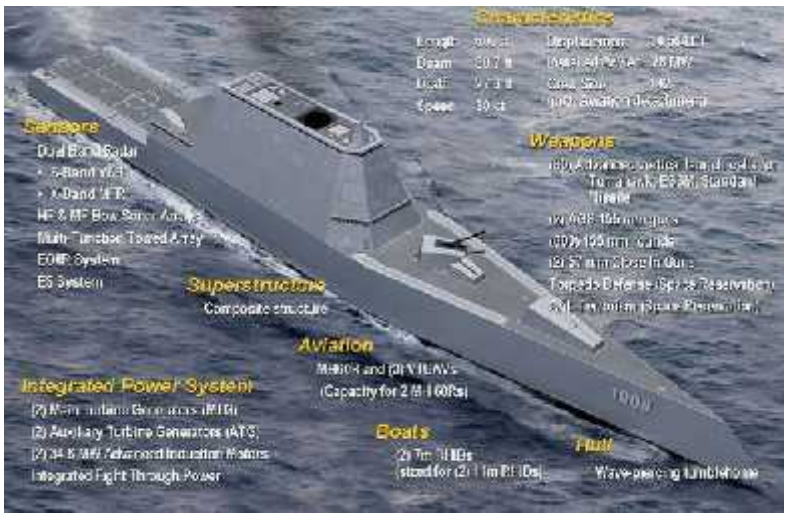


Fig. 6 DDG 1000 design features and systems

II.3 Electrical weapon

In future conflicts, naval forces envision conducting ship-to-objective maneuvers as an integral part of the joint campaign. Joint ground elements will consist of increasingly light, highly maneuverable forces that will employ indigenous light, lethal fires from advanced ground combat vehicles while directing heavy joint fires that will be delivered increasingly from the air

and sea. The integration of special operations forces and joint fires during Operation Enduring Freedom was just a glimpse of how the relationship between ground forces, fires, and maneuver elements will transform future military operations. Naval forces must continue to extend their operational reach from the beach to 200 miles inland and beyond. Future operations will require the capability to engage thousands of targets a day, up from the current capability of sea-based missiles and carrier aviation to engage a few hundred targets in that time frame. To support the ground campaign, sea-based naval fires also must achieve performance equal to or greater than that currently available from shore-based artillery systems.

Constrained by physics and cost, conventional guns have reached their inherent limitations. The limits of gas expansion prohibit launching an unassisted projectile to velocities of greater than about 1.5 kilometers per second (km/sec) and ranges of more than 50 miles from a practical conventional gun system. Alternatively, the extended range guided munitions (ERGM) and advanced gun system (AGS) would launch rocket-assisted shells to extend the range of conventional guns, but tradeoffs between size, rocket fuel, and lethal payload requirements make these options prohibitively expensive beyond their expected ranges.

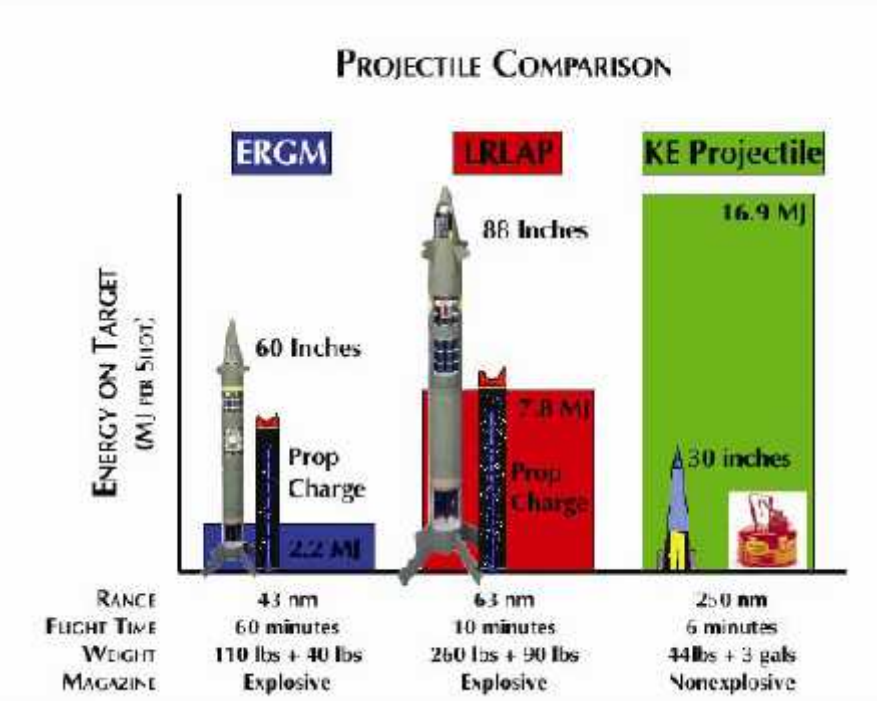


Fig. 7 Projectile comparison

Electromagnetic rail gun technologies offer the most mature, unconventional, extended-range fire support solution. Increased muzzle velocity is the key to cost-effective increases in range, lethality, and responsiveness because it provides these benefits without onboard propellants or explosives. Rail guns are the only systems that have demonstrated a capability to launch

projectiles to 4.4 km/sec, and recent technical developments have significantly reduced the technical barriers to fielding naval systems.

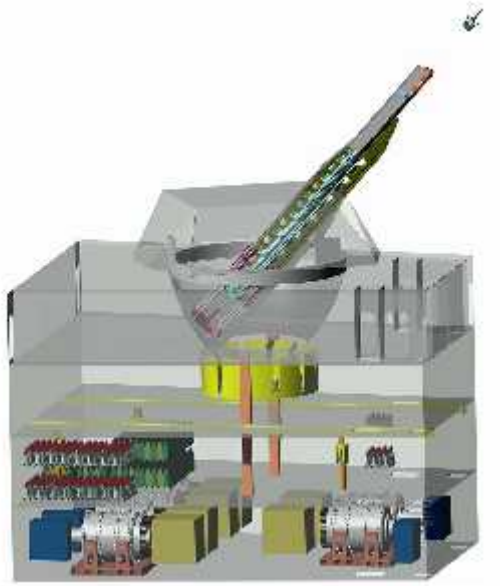


Fig.8 Naval Railgun

Developing rail gun technology would shift the possibilities for naval fire support to a new performance curve, allowing tremendous future growth potential in gun technology. To put things in perspective, current 5-inch gun has muzzle energy of 10 megajoules (MJ). ERGM will increase this to 18 MJ, and AGS will press the limits of conventional gun physics by attempting to achieve muzzle energy in excess of 33 MJ. In contrast, naval railguns will achieve muzzle energies from 60 to 300 MJ. Research indicates that a notional first-generation naval railgun with a 2.5-km/sec muzzle velocity could deliver a guided projectile with an impact velocity of Mach 5 to targets at ranges of 250 miles at a rate of greater than six rounds per minute. Mature rail gun technology is predicted to produce a much greater capability.

An important advantage of rail guns is the ability to exploit the high kinetic energy (KE) stored in the projectile for extremely lethal effects. One test demonstrated that the release of the rail gun projectile's kinetic energy alone would create a 10-foot diameter crater, 10 feet deep in solid ground, and achieve projectile penetration to 40 feet. Hypervelocity projectiles provide deep penetration to destroy hardened targets that are extremely hard to kill by other methods. Nothing prohibits the use of explosives, but lethality studies suggest that rail gun KE projectile concepts will be sufficiently lethal—three to five times more deadly than current gun systems.

Compared with propellant guns, railguns can fire at higher velocities and do not require gun propellant but use ships' fuel. These features lead to important advantages, including shorter time of flight (important for ship defense), higher lethality on target (important for direct fire), and very extensive range capability (important for support of troops on shore). Such extended

range capability also supports the sea-basing concept in which a forward deployed battle group is able to operate far enough off shore to be safe while providing a long reach for distant targets.

CONCLUSIONS

During the time the weapons was based by mechanical energy (bows, catapults) and chemical energy (guns, missiles). Now more and more weapons are designed using electromagnetic energy. Instead to accommodate new systems on old weapons the weapons designers are looking to integrate all systems in an electrical powered weapon. Despite the fact the speed of development are different, now we can see the two wings of revolution in military affair started at the end of industrialization age.

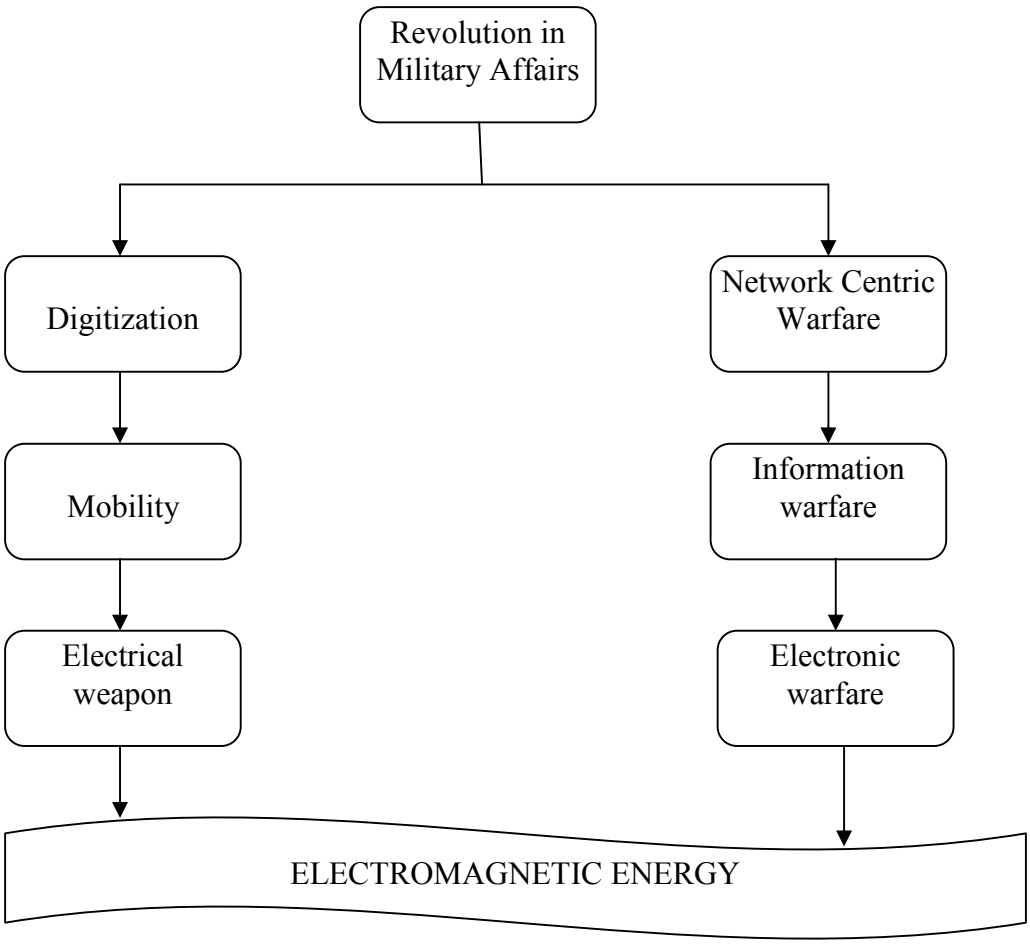


Fig.9 The two wings of RMA

REFERENCES

[1] David Alberts: *Power to the Edge: Command… Control… in the Information Age*, CCRP publication series, 2005;

[2] David Alberts: *Network Centric Warfare: Developing and Leveraging Information Superiority,* CCRP publication series, 2000;

[3] Dr. Edward A. Smith, Jr.: *Network Centric Warfare: Where's the beef?* Naval War College Review, 2000;

[4] Maj Dr. Eng. Laurian Gherman: *Warfare in the Information Age,* Journal of Defense Resources Management 1/2010;

[5] Lt. Commander David Allan Adams, U.S. Navy, N*aval rail guns are revolutionary,* 2003;

[6] I. R. McNab, and F. C. Beach, *Naval railguns,* January 2007;

[7] Harry D. Fair*, Progress in Electromagnetic Launch Science and Technology,* January 2007;

[8] Khershed P. Cooper, Harry N. Jones, and Robert A. Meger, *Analysis of Railgun Barrel Material,* January 2007;

THE RISKS OF ATTACK ON INFORMATION SYSTEMS

Captain Adrian DUMITRACHE

INTRODUCTION

In less than a generation, the use of computers, virtually every dimension of society has changed the way people and organizations obtain or disseminate information or conducts business, allowing for greater efficiency, enhanced operational control and quick access to information. Along with many benefits, however, and interconnection of computers has negative aspects, such as the emergence of new types of crime (distribution of computer viruses, for instance), and the possibility of committing traditional crimes through new technologies (such as fraud or forgery, for example).

The proliferation of computers, increasingly more powerful and available at prices ever lower, and the dramatic expansion of inter (inter alia) have given potential attackers the opportunity to make rapid attacks and without geographical constraints, often with serious consequences for victims and low probability of detection or criminality. Since electronic attacks against information systems can produce a series of negative consequences - financial, operational, legal or strategic - at individual, organizational or even national, electronic attack risks must be well understood to be alleviated or even eliminated.

In this paper we propose to discuss the risk of electronic attack on information systems, which are the potential attackers and their motivations are, what types of threats, vulnerabilities and exposures, as well as approaches of risk analysis.

I. ELECTRONIC ATTACK RISK

I.1 Growth of electronic attack risk factors

Computer information systems are essential for the proper conduct of most modern activities; consequently, their security must be an important concern related organizations.

A number of factors may be considered to have increased the risk of electronic attack against information systems:

- Difficulties inherent security (Landwehr, 2001; Loscocco et al., 1998);
- Increasing globalization;
- Insufficient awareness and educate the users of information systems (Siponen, 2000) and attitudes or practices that do not comply with the procedures manual (Schneier, 2000);

- Availability of information on the penetration of information systems without authorization;
- Unclear legal regulations and jurisdictional difficulties.

I.2 The concept of information systems security risk

Whether an organization's computer information systems are insufficiently protected against certain attacks or loss shall be appointed by Straub and Welk (1998) "system risk." On the other hand, Adams and Thompson (2002) considers that the risk is somewhat subjective, referring to a future that exists only in imagination, at least initially. According to Turban (1996), "risk" is defined as the potential threat to materialize. The risk is, in the context of computerized information systems, the amount of threats (events that can cause harm), vulnerabilities and value of information display:

Risk = Threats + Vulnerabilities + Value of information.

Before determining threats, vulnerabilities and mitigate risks before, must determine what it is trying to protect - as argued Berryman (2002), to do a complete inventory of information system. Electronically stored information is valuable. Incidents that will adversely affect the information stored electronically and the individual or organization that depends on or uses such information. Information is evaluated against the impact the incident will adversely affect the information. Threats, vulnerabilities and possible impacts should be combined to obtain a measure of risk they are exposed to information.

A schematic representation of the concepts suggestive of computerized information systems security and relations is proposed in the standard Common Criteria for Information Technology Security Evaluation (adapted and presented in Figure 1):

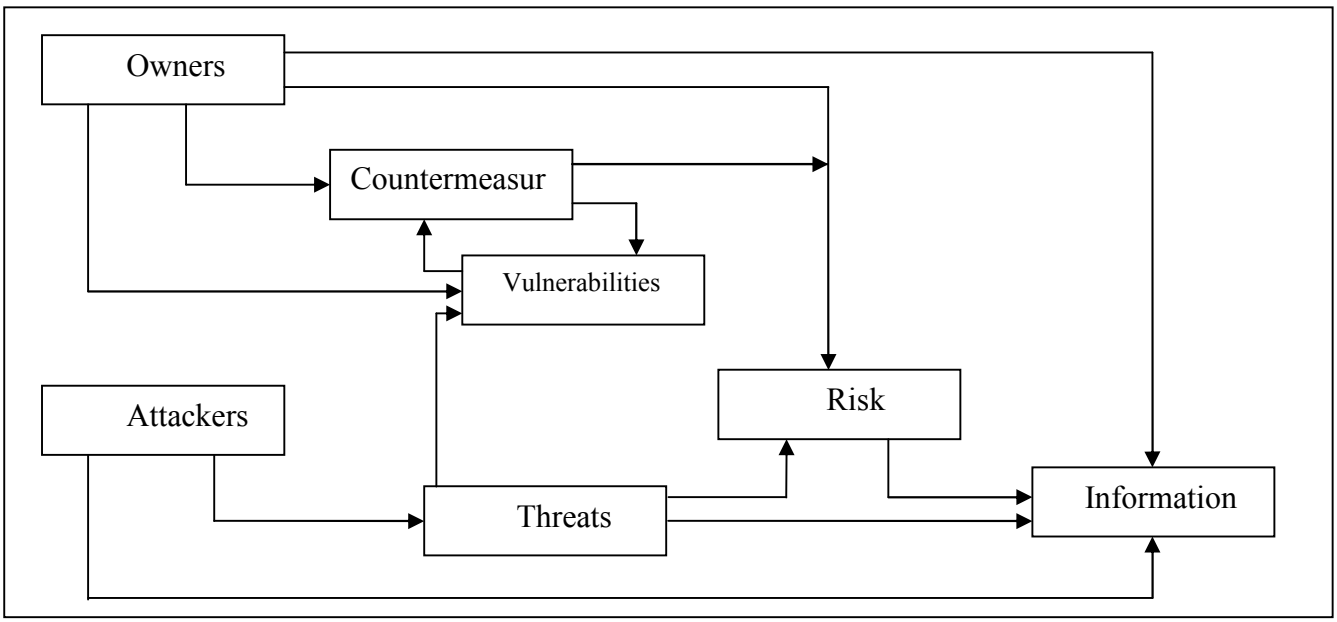


Figure 1: Information systems security concepts and relations

A security model of effectiveness is a computerized information system proposed by Kankanhalli et al. (2003). Under this model, top manager's commitment, organization size, deterrence and prevention efforts are regarded as among the most important factors (Figure 2).

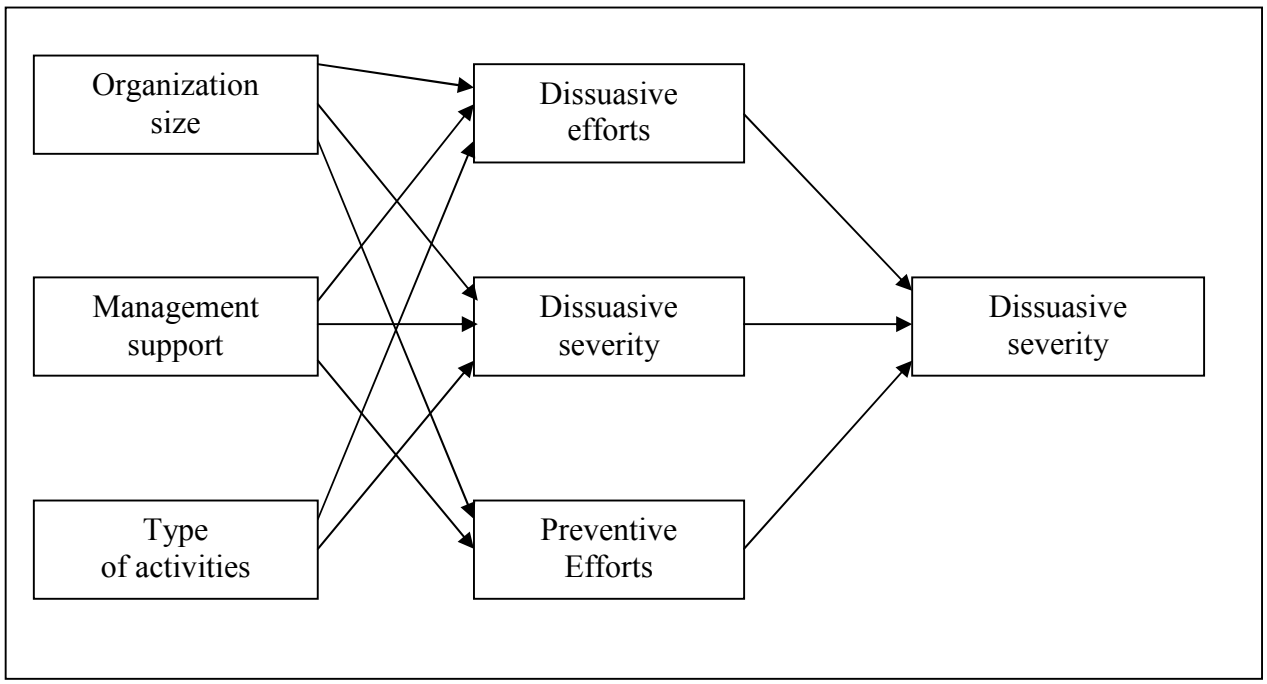


Figure 2: Model of an information system security effectiveness
(Kankanhalli et al., 2003).

To assess the potential of possible attacks (the importance and potential impact of a security incident), it is necessary to understand the expertise, motivation and intent of potential attackers. An attacker who selects a victim based system of insecurity which he presents is different from an attacker who selects a particular attack to commit certain acts.

To select and implement appropriate countermeasures risks of computerized information systems is necessary that these threats to be thoroughly assessed. The following sections discuss the categories of potential attackers, their motivation to address threats to computer information systems.

II. ATTACKERS, THREATS AND VULNERABILITIES

II.1. Potential attackers of information system.

Individuals within an organization and accidents or natural disasters are the main sources of risks to information systems. People from the outside are also an important source of risk because they are in some cases, more motivated and more difficult to detect and investigate only those within organizations.

According to Ozier's assertions (1999), organizations must explicitly address the following elements in any analysis of risks:

- Threat agents;
- Motivation attackers;
- Capabilities attackers;
- Threats to information;
- Frequency of threats;
- Impact of threats;
- Likelihood of attack;
- Vulnerabilities of their systems, and
- Controls available / implemented.

Based on the results of the work A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses (Cohen et al., 1998), is considered the next 'actors' can cause problems for computer information systems security:

- Employees. They are invested with confidence and have access to the information system, allowing them to know the weaknesses of the systems, carry out operations that may be detrimental to those organizations, and deleting digital records (Vasiu and Vasiu, 2004);
- Consultants and system maintenance personnel. These people often have access to sensitive areas of information system, which allows a wide variety of operations;
- Suppliers / Customers. Their reasons are not economic in some cases matching those of the organization and, in some circumstances, may perform certain actions that may present security risks;
- Competitors: Other individuals or organizations who will benefit from losses caused by attacks on the organization's information system;
- Crackers[1] / Mercenaries computer / professional criminals. People who illegally penetrate information systems and intentionally causing damage, the motivations are, in general, different;
- Experts in espionage. People who specialize in obtaining information that will benefit other organizations. This person a high level of technical knowledge, are well paid and can often be detected without actions do;
- Accidents / natural disasters: They can cause loss of important information or freezing them.

Information systems attackers can be classified according to several criteria. Depending on the motivation, there are four main categories (and Vasiu Vasiu, 2001):

[1] R. Stallman (1984), who call themselves hackers, and recommends using the term 'cracker' for those who penetrate information systems in violation of security measures.

- Social motivation. The attackers in this category try to get a sense of superiority or control over other attacker's acceptance or inclusion in a particular group.
- Technical rationale. The attackers in this category are trying to 'beat' system as a kind of intellectual challenge.
- Political motivation. Attackers in this category are trying to get political attention to promoting a particular cause.
- The financial motive. Attackers in this category attempt to obtain personal gain (such as, for example, spies, mercenaries computer, various organizations or persons responsible for distributing confidential information, etc..).

II.2. Analysis of attack threat

It is widely used by organizations (see Blakley et al., 2002), even if the authors (such as, for example, Jacobson (1996)) considers that risculi analysis is subjective, inconsistent and sometimes even unnecessary.

According Wilsher and Kurth (1996), organizations need to address risk in four stages:

1. Identify and assess important information
2. Identify and evaluate threats,
3. Vulnerability assessment and
4. Risk Assessment.

Also, to provide answers to the following fundamental issues within a risk analysis (Ozier, 1999):

1. What undesirable events may be happening?
2. If it materializes, will be the impact?
3. How often undesired event can occur?
4. How safe is information that defines the three elements?

Berryman (2002) argues that organizations need to identify threats, vulnerabilities and then to quantify the potential impact of vulnerabilities.

Thus, for each vulnerability, it must be considered likely to be exploited and damage that would result if it is operated.

Have countermeasures to mitigate identified risks and their costs must be thoroughly quantified.

The costs incurred to mitigate risks should be compared with the costs of the organization if the vulnerability is exploited, so that managers can decide what risks to prevent, limit or accept.

There are several approaches to risk analysis, but all they can talk about two major categories of approaches: the quantitative and qualitative.

Quantitative risk analysis focuses on the probability of an event and estimates the likely losses that might occur. This type of risk analysis using so-called estimated annual loss (Blakley et al.,

2002) times the estimated annual cost. Calculate the value for a particular event by multiplying the probability of potential losses unwanted party event. This approach makes it possible hierarchy of events in order risk, which allows for decisions based on this hierarchy.

Such an approach has, however, the drawbacks caused by low reliability and poor accuracy of the data. The probability of an event only rarely can be estimated precisely. Additionally, controls and countermeasures are limited to addressing a number of potential events. Despite these shortcomings, a number of organizations have successfully adopted quantitative risk analysis.

Qualitative risk analysis, which uses only estimated amount of loss, is the most widely used in this field. Most qualitative risk analysis methodologies to use a set of interrelated elements:

Threats. They are present for each system and is what might happen or what might attack a system. The threats are varied and attacker's objective is to obtain benefits for himself or harm others or just information system owners. Were defined as follows:

- a possible threat to a system (Kabay, 1996).
- a circumstance that has the potential to cause a loss of organization (Pfleeger, 1997, Castano et al., 1995, Neumann, 1995).
- circumstance or event which may cause violation of system security (Summers, 1997).

Vulnerabilities. This is due to inconsistencies or errors in design, implementation, operation or maintenance of programs (Bishop, 1999). They make a system more likely to be successfully attacked and were defined as follows (inter alia):

- a point where the system is likely to be attacked (Kabay, 1996).
- a weakness in security system that can be exploited to cause injury or loss (Pfleeger, 1997).
- a particular weakness of a system that allows its breach (Summers, 1997).

Controls. They are for vulnerabilities and countermeasures must be commensurate with the criticality of the information system and the likelihood of an undesired event. Can be identified following categories of controls:

- deterrent controls that reduce the likelihood of a deliberate attack;
- preventive controls that protect against vulnerabilities (these attacks are impossible or very difficult);
- corrective controls that reduce the effects of an attack;
- detective controls, allowing the discovery of attacks and trigger preventative or corrective controls;
- recuperative controls that allow system restoration after an attack.

III. THE THREATS AND VULNERABILITIES

III.1.Types of threats

Threats should be clearly defined in order to choose, therefore, appropriate security measures and controls (panko, 2004).

Castano et al. (1995) classified bipartite threats according to mode of production:

1. *non-fraudulent (accidental)* and
2. *fraud (intentional).*

Another possible classification grouped the threats to information systems:

- *Natural Threats*: These are called the insurance field as force majeure (fire, storms, lightning, earthquakes, floods, just a few examples of this category) (D'Arcy, 2001);
- *Threats Accidental* procedures performed incorrectly, power failures, interruption of electric cable, the failure of a disk etc.
- *Intentional threats*: sabotage, unauthorized access, use or deletion of information or of media, planting Trojan horses or computer infected with computer viruses, etc..

Threats to information systems can be classified (buff, 2000) as follows:

1. fundamental threat,
2. threats that facilitates,
3. an indirect threat.

Attacker a computerized information system in general will come to a position where it will represent a fundamental threat through the use of other threats that facilitate or through an indirect threat.

*Fundamental threats***.** This is what an attacker wants to achieve. These threats are categorized by Buffa (2000) the disclosure of information, altering data, rejection, denial of service and unlawful use, and are discussed in the following subsections.

Disclosure. Important information that should remain confidential, are accessed and disclosed by unauthorized person (or persons employed by unauthorized) or exceeding their powers. As some information has great value, a value significantly diminishes or is lost through a breach of confidentiality, this type of attack can have adverse consequences, very serious for organizations.

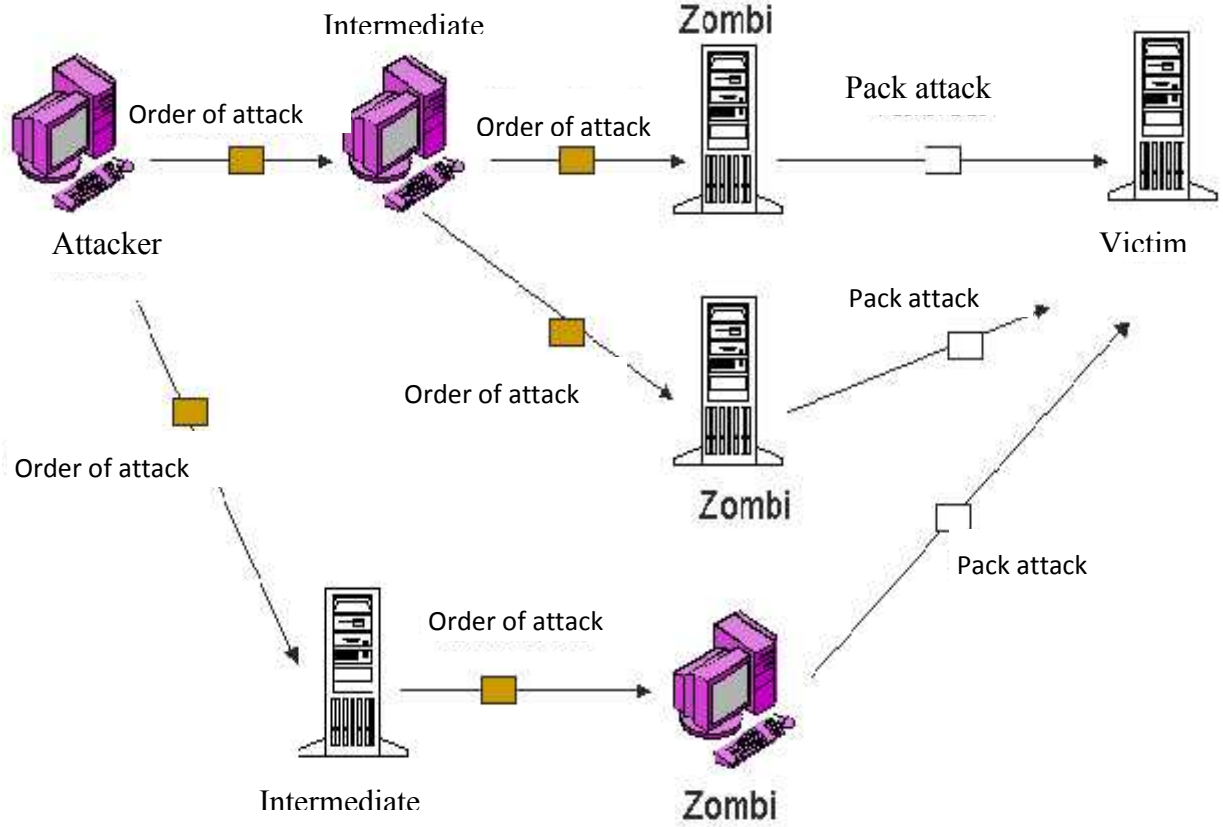
Altering information. The information is entered into the system without authority, amended or overridden by unauthorized person (or persons paid by unauthorized persons) or exceeding their powers. As some decision or action depends mainly on the information obtained, this type of attack presents a danger great potential for organizations.

Repudiation. The ability of a person or action to deny the identity of the sender, content or time of a communication or transmission of an email. Because the messages or electronic communications are of great importance for organizations to ensure their non-repudiation.

Denial of service (denial of service, DOS). Attacks of this type use computerized information system resources, resources to serve legitimate users. There are two main sub-categories in this category of attacks: logic attacks and attacks of 'flooding' (flooding attacks)[2].

*Attacks Distributed Denial-of-service (DDoS).*It is a type of attack are used tens or even thousands of compromised computers to automate the transmission of data that will 'flood' systems targeted, attacked. Are compromised computers controlled remotely by planting, often, computer trojan horse, which produces a group of computers 'zombies' (which will act as the entities with the same name from the voodoo legends). These attacks are dangerous because they are very difficult to offset.

Illegitimate use. The information is used by unauthorized persons or for unauthorized purposes. Because some information (eg, results of investigations or details of customers) may have significant value, this action presents a major danger for organizations.



[2] Attacks such as the Ping-of-Death exploit vulnerabilities in software systems to block or significantly decrease their performance. 'Flooding' (flooding) is another attack in this category, in which computerized information system resources (CPU, memory or communication) are exhausted by sending a large number of false claims. Since it is very difficult to distinguish between real and false claims, these attacks can be very difficult to counteract. The most common Denial of service is "SYN flood", which consists of a series of TCP SYN (Synchronize) directed to a TCP port of the system attacked. This type of attack can prevent a system to exchange data with other systems.

Threats that facilitates. If security measures are present, the attackers will not generally go directly to the fundamental threats, thus facilitating execute threats by 'positioning'. Such threats are threats that allow access to fundamental threats. Threats can be categorized to facilitate as follows: masquerade, malicious programs, circumvent security measures, violations of approval (buff, 2000) and are discussed in the following subsections.

Masquerade (masquerade). User identity authentication is based on one or more of the following (Frisch, 1995):

- Something that only the user knows (eg a secret key)
- A recognized physiological characteristic of the user (eg fingerprint, hand geometry, typing rhythm or tone of voice)
- Something the user possesses exclusive (for example, a card or chip magnetic).

Masquerade is the process by which an intruder, unauthorized, assumes the identity of an authorized user - any user who is in possession of identification features can be authenticated as another user (authorized).

Playback is another kind of masquerade, in which the responses or the initiation of a transaction by a user or computer are recorded and re-run quietly, as if coming from the user. Insert sequential numbers or encrypted message type stamp date / time may counteract this variety of masquerade.

The mock attacks known as IP (IP spoofing), the attackers claim to use a trusted computer (by IP address), operates the appearance of the existence of a communication between computers that are used to attack to gain access to sensitive information or to run programs privileged.

Malicious programs (malware). Malicious code (malicious code - malicious) is classified, usually according to the information system penetration method, propagation and objective in the following categories: computer trojan horse, computer virus, back door, worm and spyware information. These categories are discussed in the following subsections.

*Trojan Horse computer***.** This type of malicious program will display certain legitimacy to 'picture' as something useful or authentic to contaminate a computerized information system. Named after the ancient myth, the Greeks invaded Troy warriors by fooling the Trojans with a "peace offering" (wooden Trojan horse that allowed warriors to enter the city and conquer), Trojan horse computer users may have hidden features which can lead to the insertion or alteration of data, formatting the disk, the interception of passwords, to stop certain processes, peripherals, etc. blocking In some cases, Trojans self-destroying computer after the malicious actions.

A Trojan horse computer classification is proposed Bontchev (1998): Trojan horse computer normal (regular) kickers (droppers), injectors (injectors) and bacteria (germs)

- Launchers: particular computer Trojan horses that install viruses attacked the system;
- Injectors: Trojan horses similar to those kickers but, unlike them, this type of destructive code memory installed an information system, not on the disc;
- Germs: product through assembly or compiling program source code (or the result of disassembly or decompilation) of a virus or an infected program. Germs are appointed and the first generation of virus (first generation Viruses).

*Logic bomb computer (Logic Bomb)***.** A logic bomb is a set of computer instructions of a program or a stand-alone program or the state determines the conditions that are triggered:

- An action that facilitates the unauthorized access of an information system
- Destruction of data or other unauthorized actions.

This type of destructive program is used or preferred by a particular class of attackers, which can be triggered when control such unauthorized action. Logic bombs are often placed in an information system via a Trojan horse.

*Computer virus***.** Computer viruses have the ability to attach to host programs for achieving self-replication and unauthorized actions (payload), often destructive.

Because the effects of infection with computer viruses can be very significant in some countries (such as, for example, California), infection of the systems is punishable by imprisonment or fine.

Computer viruses can be classified by several criteria: spreading environment, operating system, the destructive capacity, duration of effect, scope of operation, the exploited vulnerability, mobility, modularity, etc.. Amor (2000), the damage caused by viruses classified as follows:

- Level 1: For example, displaying messages on the screen, which does not cause significant damage.
- Level 2: Shows messages on the screen and prevents the execution of programs, but the damage is not permanent.
- Level 3: Destruction of infected program information, without interfering with other information.
- Level 4: Destruction of all information, preventing operation of computers, etc..

*Back Door***.** The security mechanisms of computer information systems are implemented to prevent unauthorized access or unauthorized insertion of data or programs. Back doors is a mechanism for violations of restrictions on access or write to disk, which allows violations of confidentiality of information, unauthorized modification information, planting information, etc. Trojans.

*Worms***.** Worms are confused, often with computer viruses. Even if similar programs can be malicious activity (such as, for example, deleting or changing information), there is one major difference: worms do not need a host program to reproduce or to engage in running (Vasiu and Vasiu, 2004a). Worms can be used for a variety of destructive actions.

Worms can move to attack computer networks and / or contaminate other systems. This program was invented as an experiment by John Socha and Jon Hupp of the Xerox Company, Palo Alto, California, in 1980, with the hope that such programs can take over some administrative tasks required in a computer network (one of their worms seek and try solving the problem of broken computers). In the hands of malicious people, but worms can cause very difficult problems.

*Spyware***.** Spyware is a program placed on a system of information without consent (informed) users to obtain information about the system, to capture what users type, after obtaining information from being transmitted to that or those who control program will be used to attack information systems.

*Circumvent security measures***.** The security measures of information systems installed in some cases may work incorrectly or be incomplete or may even block, leading to the possibility of unauthorized access to an information system.

*Violation of authorization***.** This threat is associated with people who have an authorized account, but made unauthorized actions (eg, the insertion of false or delete vital information). This type of attack is a threat to an organization associated with employees (insiders).

*Indirect threats***.** As argued Buffa (2000), this kind of threat derives from the basic features of the Internet and information infrastructure. The following sub-categories can be tracked in this section: interception, scavenging, indiscretion and administrative error.

*Interception***.** Programs that allow the 'scent' passwords (password sniffers, keyloggers) monitor and record their user names and passwords. After obtaining this information, attackers can impersonate an authorized user and access confidential information, alter existing information or launch other programs or commands that can cause damage.

*Scavenging site***.** This is the use of tools to recreate the information from media, after they have been deleted or overwritten. Another form of this action is to uncover information that could be useful in bins or other places where information is printed on paper are thrown (Dumpster diving).

*Indiscretion***.** In this category included actions that lead to the disclosure of passwords or authentication techniques used, leaving the computer without concluding a work session or social engineering - a naive approach attempts to obtain passwords by techniques such as "I need X password configuration to perform "or" I Y, I forgot my password ".

*Administrative error***.** Errors of administration of a computerized information system (eg, misconfiguration, maintaining a user account on an account holder system after firing, the wrong set of authorizations, etc..) Onset of action can create or obtain unauthorized access unauthorized.

III.2 Vulnerabilities and exposures

The vulnerability means any event which presents a problem in terms of information system security in a given context. Vulnerabilities are loopholes through which the threat occurs. Common Vulnerabilities and Exposures seeks standardization developed by Mitre known vulnerabilities.

A universal vulnerability is defined as a state in an information system that:

- Allows an attacker to execute commands by im-personing an authorized user,
- Allows an attacker to access information otherwise access procedures,
- Allows an attacker to conduct a denial of service attack (denial of service).

Stoneburner et al. (2001) has the following basic rules to mitigate risks associated with intentional threats. These rules are applicable, except the third, and mitigation of natural or accidental:

- When a vulnerability exists, it reduced the possibility that vulnerability to be exploited;
- When a vulnerability can be exploited, to be implemented on multiple levels of protection and administrative controls that can minimize risk and prevent exploitation of vulnerabilities;
- When an attacker's cost is lower than the potential gains to be applied which decreases the motivation of the attacker protection by increasing its cost;
- When potential loss is too large to be applied to non-technical and technical protections to minimize potential loss.

An exposure is a state of an information system that is not a universal vulnerability, but which:

- Allow an attacker to carry out activities to collect information about the system;
- Allow an attacker to hide his activities (illegal);
- Includes a functionality that can be easily compromised;
- One is a point of entry that an attacker can use to access the system or information;
- One is considered a problem in terms of policies (procedures) for use of the information system.

CONCLUSIONS

As organizations become increasingly dependent on computerized information systems function effectively, the security of these systems is becoming increasingly important (Kankanhalli et al., 2003).

Stoneburner et al. (2001) suggest basing risk mitigation programs associated with computerized information systems on the following:

1. an active commitment of top managers within organizations;
2. a support and participation of all staff;
3. a team responsible for competence analysis and mitigation;
4. a cooperation of users, who must follow the procedures manual and safety rules;
5. a continuous evaluation of the risks.

Electronic attack risk varies according to:

1. type of organization
2. potential vulnerabilities
3. various catalysts, inhibitors and enhancers.

REFERENCES

1. Adams, J. şi Thompson, M. (2002). 'Taking account of societal concerns about risk: framing the problem', Health and Safety Executive, Research Report 035.
2. Berryman, P. (2002). Risk Assessment: The Basics.
3. Bishop, M. (1999). Vulnerabilities Analysis. In Proceedings of the Second RAID Conference.
4. Cohen, F., Phillips, C., Swiler, L. P., Gaylor, T., Leary, P., Rupley, F., Isler, R. şi Dart, E. (1998). A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses: A Cause and Effect Model and Some Analysis Based on That Model, Sandia National Laboratories.
5. D'Arcy, S. P. (2001). Enterprise Risk Management. Journal of Risk Management of Korea
6. Kankanhalli, A., Teo, H.-H., Tan, B. C.Y., Wei, K.-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management.
7. Stallman, R. M. (1984). Letter to ACM Forum. Communication of the ACM
8. Stoneburner, G., Goguen, A. şi Feringa, A. (2001). Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology.
9. Summers, R. C. (1997). Secure Computing: Threats and Safeguards. McGraw-Hill.
10. Vasiu, L. şi Vasiu, I. (2004). Dissecting Computer Fraud: From Definitional Issues to a Taxonomy. In Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, USA. IEEE Computer.

.

INFORMATION TECHNOLOGY DIRECTORATE IN JORDAN ARMED FORCES

LTC Ala Nadeem QOUL

INTRODUCTION

Jordan's economy is among the smallest in the Middle East, with insufficient supplies of water, oil and other natural resources, underlying the government's heavy reliance on foreign assistance. Information technology sector is one of the developed sectors in the Jordanian economy, represents the entrance channel for new technologies and creates the opportunity framework for a future development of the country's economic and social life.

His Majesty King Abdullah II stressed the need to create an enabling environment to achieve the necessary support for the IT sector information and communication, being one of the most promising sectors to boost the national economy and achievements in a positive return on the development of the sector and the need to develop a deliberate plan to set goals and provide the conditions necessary to support the information technology sector, which achieved success, pointing across the past few years and could contribute to future successes in the light of the available opportunities.

Jordan assumes a leading role in the area of information technology and communications, in order to adapt to the economic transition and the world rapid development. This took the shape of the establishment of telecommunication infrastructure and advanced computer networks, in accordance with the spirit of the times and the sustainability of an educated workforce, which is one of the top priorities in Jordan.

Jordan was the first country in the Arab world to have a fully liberalized telecommunication market and has modernized 75 percent of its ICT related laws, improving the business environment for local and international investors. Jordan also led the region by establishing the first independent telecommunications regulatory body to create a fair, transparent, and competitive investment environment.

Intellectual property laws are in effect and are considered to be the model in terms of structure and compliance across the developing world. Jordan also is an attractive place to consider in terms of overall attractiveness as an outsourcing destination. Growth of the market is due to market oriented regulations, foreign direct investment and incumbent Jordanian entrepreneurs interested in expanding the Internet skill and wage advantage of the labor force.

Information Technology Directorate in JAF has a magnificent role in improving the IT knowledge in JAF and in the society, by implementing the government strategy in this respect. It collaborates with the government and private sector to implement the vision of His Majesty King Abdullah II to achieve sustainable development, raise the standard of living of all Jordanians, as a safe way to meet the global recent challenges. Also works hard to align Jordan to the standards of other developed countries, modern and exporters of excellent human skills and able to compete regionally and globally.

I. INFORMATION TECHNOLOGY HISTORY IN JAF

In the past all military units contained offices that had as prime responsibility the management of computer infrastructure. There was no coordination and connection between these units, programs implemented were limited to the unit level and the development of those programs depends only on the needs of the unit itself.

JAF recognized the need for a special department which can deal with the new, fast improving technology and in 1984 a dedicated office was created in the JAF Directorate of Planning to handle all the information technology related topics. While the technology was moving fast and more specialists where needed, more responsibilities was handled to the IT Office, in order to "grow with the technology" and to prepare more ideas ready to be implemented.

In 1986 the military headquarters decided to establish a special directorate named *Information Technology Directorate* that can, not only be aware of the new technologies, but work as an independent department and develop new programs that can improve the work in JAF, relying on a new generations of well prepared Jordanian engineers, programmers, data analyses and technicians.

The main tasks of the Directorate are:

- the creation and implementation of new programs;
- the establishment of new computer networks;
- the analysis of the need for new technologies to be used in JAF;
- the education and training of military staff, as well as civilians;
- how to use IT and what IT can offer in order to implement the vision of JAF regarding Information Technology and
- the cooperation with the government and the private sector, sharing and exchanging ideas and experiences, and providing a needed tanning to IT staff in Jordan or outside Jordan.

During these 24 years of work in JAF, IT directorate was able to improve and create new programs and applications used now in JAF, connect all JAF units into one network, establish and implement E-army, providing all JAF units with the needed IT equipment, helping them doing the job in the best way possible.

The Information Technology Directorate, in cooperation with the Government, Ministry of Communication and Information Technology, Ministry of Education, Ministry of Health, Ministry of Planning, and with the private sector remained focused to improve the IT infrastructure in Jordan and to raise the whole community to the future.

II. MISSION AND VISION

The mission of Information Technology Directorate is *"to provide excellent and safe IT service to all military units, with commitment toward development, continuous improvement, and best utility of available resources through qualified and competent staff, and modern technological tools and equipment aimed at ensuring an effective contribution in increasing the level of Information Technology in Jordan Armed Forces"*.

Information Technology Department is responsible for the management and support of the technology architecture, hardware and software, the development and implementation of new technology programs. Its main duties in JAF and in Jordan in general can be summarized as follows:

- Promotion of Information Technology and Information Technology enabled services and Internet;
- Assistance to other departments in the promotion of E-Governance, E-Infrastructure, E-Medicine, E-Commerce, etc.
- Promotion of Information Technology education and Information Technology-based education;
- Matters relating to Cyber Laws, administration of the Information Technology and their Information Technology related laws;
- Interaction in Information Technology related matters with national and International agencies;
- Provide IT Software Support services to JAF;
- Promotion of Standardization, Testing and Quality in Information Technology and standardization of procedure for Information Technology application and tasks;
- National Informatics Centre (NIC);
- Saving and updating all matters relating to military personnel;

- Provide IT Hardware and Maintenance support services to JAF;
- Implement security policies to safeguard the security of DATA and hardware;
- To design, develop, manage and maintain the JAF website and ensure understanding of website usage;
- Provides technical support for the use of information and communication technology in the form of specialized training.

III. IT DIRECTORATE BRANCHES AND DUTIES

1. Research and Development Department

The responsibility of this department is very important, it's main role is to search and study all the military units and find the way to improve their performance using the new technology and develop new programs that they may use to help them doing the job faster and efficient, also to ease the jab, main duties for Research and Development Department can be summarized as:

- Implement and monitor the JAF Policy related to Information Technology, and Internet.
- Initiatives for development of Hardware / Software including knowledge based enterprises.
- Design, develop and implement data processing needed to develop JAF.

2. Training Department

The Training Department coordinates its own training internally for all Ranks. The training Section is specialized with training in Hardware and Software. The department has trained at various levels from which soldiers were able to acquire their A+ and Network Plus Certifications, which has helped to boost the Hardware Section substantially. On the Software domain, training is done on the Microsoft Office Specialist (MOS) curriculum. Further training is done at external institution. Training is primarily done at external institutions for Officers and Senior Non Commissioned Officers namely Government or private Technical Institute.

Special training center in JAF for Information Technology established to ease the training process and to reduce the training cost, qualified officers hired to conduct training.

Training Department within the Information Technology Dept. plays an important role in raising IT knowledge among military staff , providing training to all military staff, arrange international exams for the military staff (ICDL, CISCO, A++…).

Another role training related is the initiation and improvement of IT staff knowledge in new programs and new technologies and their preparation to pass the international exams for the subject related to there specialists such as (ORACLE, MCSE, MCSA, etc.).

3. Maintenance Department

Mission of maintenance department is *"to repair, service, and maintain the IT related equipment, and responsible of keeping all in JAF IT equipment in good working conditions, provide new IT equipment to all JAF units according to the yearly planed schedule"*. The main duties of this department are as follows:

a) to maintain all IT related equipment in JAF, including PCs, printers, servers, networks etc.
b) to participate in the training process;
c) to participate in procurement process related to Information Technology in JAF and in the Government (if needed);
d) to implement the monthly maintenance plan and
e) to implement the preventive maintenance plan.

4. The Internet Department

The main duties of this department are as follows:

a) Provide internet connection to JAF.
b) Provide internet to all JAF unites using local JAF network or anther internet server's providers.
c) Maintain and update JAF web site.
d) Support all JAF units and directorate in creating and publishing their web sites .
e) Coordinate with other directorate to establish a policy of using the internet in JAF.

5. E-Army

Information and communications technologies are playing an increasingly vital role in the daily lives of people. In the realm of army, Information Technology D. applications are promising to enhance the delivery of services to all JAF unites, not only by improving the process and management of the army, but also by redefining the traditional concepts communications.

During the last years Information Technology directorate developed a great deal of applications and programs that are now used in many JAF unites some off these programs are:

- Medical record information system – Royal Medical Center;
- Financial information system;
- Human resources system;
- Inventory system;
- Procurement system.

All this systems are working in all JAF, to help the user and the decision makers to take the appropriate decision in an appropriate time.

6. Procurement Division

Procurement division in Information Technology Directorate is responsible for participating in all IT related equipment acquisitions for JAF. The main roles of this division are:

- Study the need of the new equipment;
- Put the right specifications;
- Participate in procurement process;
- Search the market for the new equipment and/or software that can be implemented in JAF.

7. IT Security Division

Information in the army is very sensitive, vital and obvious can not be accessible to everybody, because it could be lost, damaged or altered. Because it must be prevented the possibility that un-authorized personal get access to information, a special IT security Division working in Information Technology Directorate was created to ensure that.

The main roles of this division are:

- Day to day administration of systems and user IDs.
- Data Centre physical access administration.
- Sensitive data protection administration.
- Hardware and Software inventory collation.
- Documentation of processes, procedures and policies.
- Maintenance of the network's authorization infrastructure, as well as network backup systems.

8. Data Center

The data center is very important for any organization and it's more important in an organization such as JAF. The most important aspect is that "it brings everything in one place". Keeping all the servers and hardware at one physical location is vital because it reaps more benefits and provides easy maintenance. It contains not only servers but also network equipments that help the servers to communicate one to each other. It offers high availability and business continuity.
The Data Center in JAF provides all needed connection to the authorized staff and store all date updates and movements that will allow the availability of information at any time. Beside the

main Data Center in the JAF HQ, a backup Data Center was established in another city to keep the data and the application safe and handy in case of emergency.

IV. MAIN PROBLEMS FACING INFORMATION TECHNOLOGY

As one part of the society, the problems for all IT sector are alike and can be listed as:

- Lack of infrastructure;
- Lack of Focus;
- The scarcity of funding;
- Absence of a well established e-Society;
- Lack of coordination;
- Resistance to change.

On an institutional level within government agencies analysis showed a number of problems which can be categorized in different domains starting from the expected cultural problems, accountability problems, technical problems related to knowledge management issues, behavioral problems such as the employees' adaptability to the introduction of new working methods.

V. FUTURE VISION

To improve the level of Information Technology in Jordan Armed Forces and to maintain a high level of efficiency requires a lot of effort and follow-up research in all fields, including technological. The role of the Directorate of Information Technology is to support the progress towards the future at a steady and clear rhythm, to help the Jordanian Armed Forces to grow and evolve to keep pace with developed countries:

- Increased IT awareness in Jordan Armed Forces (IT literacy in the Jordanian Armed Forces);
- Program and implement secure network and secure Data transfer between all military units;
- Increased cooperation between the private and public sector with the Jordanian Armed Forces;
- Increase the manpower working in Information Technology Directorate to support all areas of manpower needed;
- Create and activate new divisions such as Monitoring and Quality Control.

CONCLUSION

Jordan's IT landscape provides a case study in what it takes to succeed in the international market place - a combination of sound policy, strong telecom infrastructure and growing talent. Jordan’s main strengths are in its all-digital network, skilled labor force and strong government backing including the personal support of HM King Abdullah II.

Market witnessed a communications and information technology developed considerably, thanks to market-oriented policies and attracting foreign direct investment, and demonstrates that demand for business owners to expand the market for new uses of the Internet, and competitive wages in the sector.

Jordan had all the Arab countries to liberalize the telecommunications market, has also updated the 75% of the laws relating to telecommunications and information technology, bringing the business climate attractive to investment, both domestic and external. From the legislative side, Jordan has established himself first in the region an independent body to regulate the telecommunications sector, which acts to create an environment fair, transparent, and are eligible for competition among investors.

Since 2002, Jordan’s ICT industry has ranked amongst the top three for the highest annual FDI achieved. Sector revenues for telecom and IT have more than doubled over the last five years going from 70 million USD in 2003 to more than 770 million USD in 2006. Total exports reached 25% of total revenue in 2006 representing around 18% growth from the previous year. Similar growth rates are forecasted from the coming 5 years.

The information technology sector in Jordan sectors dynamic value-add, which plays an important role in moving the economic sectors of other major, has emerged as an economic powerhouse in Jordan since 1995 and adopt all economic activities, primary and secondary schools in the Kingdom of the inputs arising from the Information Technology sector.

And altogether, the Information Technology sector remains responsible for the increase of direct economic income of the added value that significantly affect the growth of national economy, such as education, public administration, business services companies and manufacturing. In addition to offering computer hardware and software technologies, the IT sector facilitates the inclusion of information technology industry sector in Jordan telecommunications as an important factor.

Compared with other countries in the region, Jordan has the highest percentage of graduates of colleges and universities, in addition to the fact that Jordanian people aged between 18-30 years represent more than 50% of the population, the highest percentage in the Middle East.

REFERENCES

1. www.pm.gov.jo
2. www.jaf.mil.jo
3. www.jordanembassy.com.qa
4. www.jordaninvestment.com
5. anwww.psut.edu.jo/about/about2.htm?_president.htmada Secretariat

WEB SITES AS A MODERN TOOL TO MANAGE, TRANSFER AND DISPLAY INFORMATION

MAJ Viorel GLAVA

INTRODUCTION

In the past, information considered to be areas of bureaucratic work and limited tool for decision-making. This information is considered as one of the main resources of society development, and information systems and technologies as a means to increase productivity and efficiency.

Most common information systems and technologies are used in the production, management and financial activities, although started movement in the minds of men employed in other areas, for their implementation and application.

It existed long ago, and with the development of computers and communications, began to appear different variations: "information and communication technology, computer information technology, etc. Information technology is the integration of computers, electronics and communications products.

In ancient times, to reach the masses some information has been used spokesmen and various forms of literature and art. Over time, the possibility of seeking information highly evolved. There are a variety of media: television, radio, countless newspapers, magazines, books, and finally on the Internet. Initially, the Internet has been divided into two camps: e-mail and www (World Wide Web).

Many ISPs offering Internet purposefully shared these services and sold separately by the Internet and e-mail services and access to Usenet newsgroups. In the end settled all information evolution to their seats, and now the most modern Internet users there is no confusion about the services provided by your ISP.

The most convenient for informing the masses was the WWW-world wide web consisting of sites. Websites owners have the possibility to place their information in a way that anyone from anywhere in the world can access it. Primary standard Internet sites was (and remains so far) markup language (HTML) THAT allow you to write text and ' tag ' it, i.e. influence the appearance of text, and create links to other texts or paragraphs of the text. The simplicity of the language allowed many people without special skills, place the information on their sites. On the other hand, has made the work of professionals, which is now using the language, which inherited the basic concept of the original HTML, rich, interactive Web sites and portals.

So, in short, can be thought of as evolved modern WWW. However, despite the advent of new technologies and constantly increasing requirements of interactivity and ease of use (usability), the Internet is a lot of so-called "Web pages" that are placed there by dumping groups, students and businessmen-lovers. If the site provides information about the man, his hobby or an Outlook is not too bad. However, it happens that such sites are serious business. Therefore, consider the possible evolution of the site in the Internet.

Web site or the site, in computer networks unified under a single address (domain name or IP address) set of electronic documents (files) of an individual or organization. By default, it means that the site is located on the Internet.

In this paper we aim to explore the topic Web sites as a modern tool to manage, transfer and display information. Namely, Genesis, that know what tasks were delivered for the first Web sites.

Classification of the sites to understand how the site works best in order to meet our mission and meet our requirements.

Also want to review applicable technologies to create websites and tendency of modern sites.

HISTORY OF WEB DESIGN OF TECHNICAL GRAPHICS TO MODERN SITES

Immediately after the World Wide Web, it is primarily used by academic institutions, Governments and the military as a means to share simple information "old" model. So the documents of those times were very simple. In the end, scientists and academicians are special cases to attractive Web pages.

The world's first Web site appeared, 6 August 1991[3] - his creator Tim Berners-Lee (Tim Burners-Lee) published the description of the new technologies World Wide Web (WWW), based on the data transfer protocol HTTP, URL addressing scheme and Hypertext Markup Language (HTML). Also on the site have been described the installation and operation of Web servers and Web browsers. The site has become the world's first Internet Directory, such as later Tim Berners-Lee has posted the list of links to other sites.

Remember, as were the first sites. So – the big red letters on a turquoise background (now those sites have students at free hosting, seems like a parody) or, very beautiful, very heavy and really dysfunctional resource. Really expensive. Really made by professionals, but in a totally different area. Beauty and functionality not found common ground. Ugliness, the truth, too – but ugly sites are cheaper for their owners.

[3] http://info.cern.ch/

So it comes as no surprise that the beauty of almost a decade became a scarecrow of Web Designer. It is ugly, but functional Internet resources set the fashion for many years to come. The design requirements were very simple: it must be unnoticeable. It should not prevent visitors to get acquainted with the offer. That, given the origins, it is not surprising: the de facto approach meant that the site doesn't have to be scary. The site is a tool. Beauty instrument is in its functionality.

On the other hand, the development of design was hampered by inadequate technology. The Internet is a new standard that extends the freedom to work for Web designers. This is HTML 5 and CSS 3, and evolving technologies such as Adobe Flash, Adobe Air, and Microsoft Silverlight. At an early stage of its development, the Web was a very limited information environment. At the beginning of the same HTML was simple: HTML tags are used only to specify is heading, paragraph, and so on.

And then to light a piece called "graphical browser (NCSA Mosaic). People began to include graphics into your pages. And they wanted their pages look better, attractive, and nice. While HTML was expanded to include tags, such as **bold, strong, italic sized**.

And people still have not been satisfied, they wanted more. And the ability to add more style to the text agreed in the form tag, tag, and so on. Now people can create pages with colorful backgrounds and fonts, almost like they wanted.

However, this was not enough. Appeared on the people who calling themselves the "designers". As many of them came from the world of paper design, they wanted more control over the appearance of your Web pages.

In 1996, has published a very influential book by David Siegel titled "creating Killer Web Sites", soon became a # 1 bestseller on Amazon – incredible for a book on Web design.

Page layout System described in this book was based on HTML tables and single-pixel GIF's. Pages were on the grid; content, whether text or graphics, fit into the cells of the grid. To prevent "collapse" the empty table cells, use transparent GIF 1 x 1 pixel sizes. Siegel (and not only he) went further and suggested to use single-pixel GIF's as a means of managing the gaps between letters in the text, and to create indentation.

The emergences of such methods allow designers to create visually appealing pages, placing aesthetic aspect of the sites along with the feature.

THE EMERGENCE OF IDEAS ABOUT USABILITY WEBSITES

However, all is well in measure, and at some point it became apparent that designers are not always able to deal with the opportunities provided to them.

Increasingly appear site due to bad design could not be read. Long menus, split across a page, a huge number of rods of GIF-banners, bright colors, contrast, bad navigation, more heavy page — these are typical signs of Web design.

At this moment has come to realize that when you create a site, you should think about the convenience of the user. Started application models HCI (Human-Computer-Interaction) to the Web.

The discipline of HCI is based on psychology and it allows experts to complex social interactions surrounding the new computer equipment. These models have allowed researchers to develop various recommendations and guidelines for creating Web interfaces. Later HCI became usability on the Web.

One of the founders of usability is Jacob Nielsen. It was released in 1999, the book “Designing web usability. The practice of at simplicity” (Web-design: book by Jacob Nielsen), which became one of the first (and most important at that time) guides to create usability sites.

At the same time, there was a revolution in HCI, too. HCI, traditionally based on models of cognitive psychology, now uses this knowledge field as anthropology, Linguistics and the theory of communication, and culture and the humanities. All things which are needed to improve understanding of the person who runs a computer in the era of the Internet.

Of course, the Internet boom could not last long. Too many people thought that they know the needs and desires of its users, but they never thought about how to use design tailored to the needs of users. A poor business model has meant that many companies simply threw huge amounts of money to create products that nobody could and did not want to use.

However, the idea that this was the signal the end of the Internet was premature. Those companies that can provide useful and convenient services that have survived. HCI and usability Methods have proven effective in preventing the risks of design. In addition to using usability techniques for Web services, they are also used in the design of mobile systems. Since the late 1990s, mobile devices have expanded the ways in which we interact with computers and each other. Mobile phones, PDA (personal digital appliances) and wireless networks have led to a new concept of ubiquitous computing: a world where technology is everywhere, but it is in the background.

People are no longer single, stand-alone devices users, people have become citizens of digital communities. It is clear that systems that have a fundamental impact on the ways our operation cannot be designed using old technologies. Human-centered systems require human-centered design and usability is a challenge for the next decade.

For those who have not understood what usability is, let's take a look at key factors that affect the user experience of the site.

- Availability. Easy development of simple tasks to get acquainted with the interface of the site.
- Effective use. Quick tasks after exploring the site.
- Retention. To avoid any need to examine the system anew after short periods of time.
- Possible user error: incidence, severity, can fix.
- Satisfaction. Like the user to work with the site.

Usability is important. Studies have shown that in most cases, when you visit the site the user is losing time. Not finding the information you need, you probably never visit a site. Therefore try to minimize loading page complex graph, unnecessary scripts which may cause the user annoyance.

All about everything you've got a few seconds. During this time, you must provide to the visitor the most important information and indicate the most important functions of the site.

CLASSIFICATION OF WEBSITES

Regarding the type or types of sites created confusion. This is especially evident when communicating with customers ' Web sites. Talking Portal implied a typical business website etc. To head, at least approximately dot on their sites and help you choose the type or type of website that will effectively meet its objectives.

Suggest that we adopt the following classification. Type (s) of site:

- personal site;
- business site;
- promotional website;
- e-commerce sites;
- information portals;
- online communication;
- sites of Special Purpose.

Each type of site is divided into subtypes.

Type No. 1. Personal website

Small personal page

Advanced personal page

Commercial and PR-oriented personal sites

Type No. 2. Business website

Site-card

Typical business website for small and medium business

Large business website

The internal intranet site (intranet), an internal corporate website

Promo site

Some classifications propose the division of sites on the promo-sites, representing a product, and promotional sites of service. But in practice, often these two types of sites have almost similar features, so we give typical for this type of site features:

- Time trend: promotional websites are created at the time of promotion or campaign.
- Informs: promotional websites must provide information about the campaign: the timing and location, conditions of participation, news and other information.

Type No. 3. E-commerce sites

Online shop

Online shopping from electronic payment system

This type of online store is identical us online shop, but with the only difference is that for the convenience of buyers, it uses an electronic payment system: Webmoney, Yandex-money and others that help your pay for goods ordered.

Exchange points

This type of site allows you to conduct transactions or purchase the exchange of electronic currencies according to the type of conventional exchangers. Very easy to use and allows real-time to make transactions with electronic money.

An example of an exchange office: ecoinex.com

Type No. 4. Information Portals

News Portal

Portals

Bulletin Boards

File archives

Wiki (Hawaiian word meaning "quick")

This type is a site content and structure which allows visitors to change along with services that are located on the site. The most famous representative of this type of site is Wikipedia. Conceived as a wiki site where anyone can change

anything. In practice, all changes follow the moderators to prevent ingress of advertising and other debris. Goal of creating a Wiki can be formulated in three points:

- Create information space for storage and knowledge management.
- Create a comfortable space to collaborate on documents and lists.
- Create a comfortable space for organizing cross-references.

Very useful sites that, among other things, is authoritative for the search engines.

Type No. 5. Internet communication

Forums

Blogs

Chats

Type No. 6. Sites of Special Purpose

Wap-site

Search engine

Catalogs and rubricates

Ratings sites statistics system

E-mail sites

SECURITY

There are many sites that are significant resources. These resources may be personal data (e.g., personal correspondence, addresses, and phone numbers) or financial information (e.g. banking sites). Hacking such resources may result in both direct monetary loss (for example, an attacker could send money from someone else's account on your own) and indirect distribution of confidential information, or simply a hacker can spoil the contents of the site. For many sites, it is important to ensure some level of security. The required level of security depends on the site.

The most common consequences of an attack on the site:

- unauthorized malicious changes (see: defacing, hackers)
- forgery website (design and content of the site may be copied and the user of such a site could steal passwords)

The most popular reasons for cracking popular resources, such as email or social network, are:

- jealousy
- profit: an attacker sends out spam from a compromised account

- theft to return to the owner for the money

THE CURRENT STAGE OF DEVELOPMENT OF THE WEB

Web-trends: how to change internet sites

Due to the active development of network infrastructure, whether the network 3G, IMAX or Wi-Fi becoming increasingly popular are beginning to acquire a compact device for internet surfing. Today, a growing number of people are using these devices to read mail, news, booking, and shopping. Anyway, these devices are beginning to have an impact on web-design: some companies have already launched an application for the iPhone and iPad, others are trying to adapt Web-based resources for these devices. Are we awaiting a massive redesign of what happens to the shape of the usual sites and their prices.

Where the wind of change

A new stage in the development process of thought has given rise to iPhone, and a little later iPad. On the growing popularity of these devices has been said already a lot. Of course, the fashion news from Apple is beginning to affect the appearance of websites. Sensor technology, combined with the latest software solutions offer more new features - has already appeared sign tools, scale, increasingly at designing sites using horizontal scrolling ("flipping" pages left to right is much more convenient) and smooth scrolling scroll through menus. Over time, reducing the cost of these technologies regular monitors will be replaced by a horizontal with touch controls, and the keyboard and mouse will, among other rarities. Will develop new sign commands, respectively, will sign multi-touch interfaces that compared with today would be much simplified.

How will the website design?

Will always be completely different design for mobile devices and large monitors, because basically they are two different interfaces, but the mutual influence cannot be ruled out yet. To date, all the global web-design is gradually beginning to return to minimalism: the texts are concise, and therefore more elegant, logos and illustrations are much larger, more professional and artistic expression. For example, the designer Thierry Mugler’s site, promo site Volkswagen. Such minimalism is not only to a certain degree of aesthetic, but practical - you can quickly and clearly provide the consumer with verbal and nonverbal ways their unique selling proposition, to cause the user to the appropriate emotions and coerce to the desired action.

What will change?

First and foremost to increase button and disappear small controls for sensory mechanism the click is essential.

Fundamentally change the Gallery-if often a set of ordered columns, they can be represented as small icons, on desktop that you can move and zoom to the desired size.

Audio players will become much larger, as it is convenient to use them only on the PC

Technological changes are associated with a massive rejection of the Flash in favour of conventional hypertext markup and better use of Java-script, the emergence of a new language version of HTML - HTML5.

Inset:

The Coming Conflict users: Microsoft is currently announced competition iPad device - HP Slate, the main advantage is called the support of flash. As a result, corporations do not offer universal solutions to the user, dividing them into two warring factions. Web designers in such a situation would be forced not only to optimize sites for mobile devices, but also offers a combined solution that would suit both corporate adopters. At the moment, a compromise solution could be normal html-page with a large and beautiful flash-saver as the cap or the main graphic element.

The cost of change

With all the effort to minimalism falling prices for manufacturing sites still will not, because design often makes up about 20% of the total value of the site. Development of an Internet resource will become even more complicated, not only in terms of technology but also design the interface - the simpler the interface, the more difficult it is to design.

More and more companies, especially overseas, understand that only the use of modern technology makes it possible to turn a website into an effective instrument sale.

The company eBay, has built a successful business on the Internet thanks to an intuitive user interface that is not afraid to invest in modern technology. As a result, the applications of eBay for the iPhone and iPod Touch users have enjoyed great popularity, which brings the online store, a tangible part of the profits.

Massive redesign of the requirements of the new compact device is still not observed and is unlikely to be. Most likely, changes in web-design will be smooth, as is the case with any technological innovation. The further we move away from standard mechanisms Clicking in sensor technology, the worse the advanced website design will be compatible with conventional monitors, because eventually there will be new forms of interaction. However, despite all the smooth process, it is important to closely monitor current trends, which if used properly, tomorrow may bring the owner and competent synthesizer of this information serious competitive advantage.

TRENDS OF DEVELOPMENT OF WEB TECHNOLOGY

Someone may say: "We are still in Web 2.0 is not understood, and you have about three zero start ...."

Indeed, although there are technologies SMO (Social media optimization - promotion of social networks identified thus Web 2.0), the exact definition of the term Web 2.0 does not exist yet. Rather, under this concept implies a certain general tendency of development of the World Wide Web. And someone did, and said string of numbers on the Web was incorrect and unnecessary - a network and alternatives to it do not.

In this case, starting a conversation about Web 3.0, by default means that Web 2.0 - it's social networking services, which are based on user-generated content, by themselves, and consumption (the treatment to date is common).

So, a little research, using modern methods of information retrieval (web by keywords), revealed the most frequently used terms that users, professionals, analysts and academics associated with Web 3.0, and hence the future of the web.

1. Semantic Web - «part of a global concept of development of the Internet, which aims to implement the possibility of computer processing of information available on the World Wide Web. The main emphasis of the concept is at work with the metadata that uniquely characterize the properties and content of the resources the World Wide Web, instead of the current text analysis of documents "(Wikipedia). That is - it's sort of a network over a network that contains metadata about the resources the World Wide Web and the existing parallel them.

Optimists hope that when the Semantic Web technology will be sufficiently developed, they can be used to describe the objects of the real world - the physical objects will be presented on the Web by using metadata.

Aaron Marcus (one of the leading world experts in the field of design and usability) agree with the advocates of Semantic Web: «I understand Web 3.0 as the absolute spread of the Semantic Web on the Internet when information in the global network is not simply accumulated, but also

understood, comprehended. Marcus believes that the software in the Web 3.0 will have the capacity to collect, organize, analyze, provide information to people in these new formats, in which we imagine we cannot. What is particularly relevant now, when the flow of information generated as a professional Web-master, and the users themselves, has grown so that the bearings in it, each time more difficult.

In my opinion, similar to the understanding of how Web 3.0 Semantic Web and several other concepts and ideas associated with the development of the Internet in the future:

Web 3.0 - it specific sites. There is a view that network will evolve towards a more differentiated vertical social networks. People will rally around one particular favourite business, profession, hobbies, share opinions, give and receive advice, recommendations. A today example - culinary, medical websites.

Web 3.0 as a social institution recommendatory, which is based on the principle of automatic recommending. According to experts, Web 3.0 kind is different from Web 2.0 so that users themselves will not only create content, but the same it will be certified: note that the merit of their adherents. The system allows you to do it automatically. For example, imhonet.ru. Based on your impressions of the books they read and viewed the films you are given a list of referees - those whose interests coincide with your best.

Web 3.0 - «manager of knowledge", which in principle is similar to the preceding paragraph. This is a new profession, which will be a link between Web 1.0 (detached from the user content) and Web 2.0 (social networking, where users are direct participants in content creation). According to this version of the expert ("knowledge manager") - is the same referee, but is not automatically selected, and earned his position real work within the community.

Web 3.0 as "live search". Search by keywords are not robots, but real people, professionals in their fields, which can in addition also discuss all incidental matters.

Web 3.0 - multimedia search. Back in 2007 IBM and the BBC have to create our own Web 3.0. The concept is a search engine able to search by content of video files. Search from IBM based on the identification of compliance of the internal content video with text search query. Until now, the search is done on text tags that describe videos.

2. Custom wireless network - Web 3.0. So he called his draft European researchers involved in the creation of custom wireless networks (WIP). In their view, if the content is generated by users - is a Web 2.0, is generated by network users - Web 3.0. Clients of such networks can independently integrate their own communication channels and create new wireless networks.

One of the developers of the project (Dr. Marcelo Dias de Amorim) explains: “The concept of Web 3.0 involves the creation of" a reliable, flexible, and optimized with the "friendly" to the users a set of technologies and standards that would allow any user wherever he may be, identify

any nearby device from it and create a network with it. It will be possible even in his lack of any kind was technical knowledge."

3. "Polar Systems, built on the principle of commerce-on-demand" - this is Web 3.0, is considered Russia's Internet entrepreneurs. According to their calculations, the owner of such a system participates in the division of profits, formed as a result of the transaction entered into using the system. Why Web 3.0? Because polar information systems, like Web 2.0, subject to the effect "self growth" due to the activity of visitors.

4. Worldwide network in 3D - this is Web3.0. There are opinions that the three-dimensional virtual worlds will be the next stage of development of the Web. We are waiting for not just games like Second Life, and the Internet in three-dimensional embodiment. Perhaps, soon, 3D-realized character will leave the game and move freely across the expanses of the World Wide Web. That go far, if today in the 3D Internet is built capital of Kazakhstan, Astana, and it is positioned as the development of emerging Web 3.0.

5. Web 3.0 - the rule of robots. Today, robots scour the search engines to find the right information, send spam and viruses, who knows what awaits us tomorrow? Maybe they will invent for our content, chat on forums and write blogs?

And for a snack ... The output (picked up at one of the forums):

WEB 0.0 - user dreams to connect with who or what

WEB 1.0 - user receives the content

WEB 2.0 - user created content

WEB 3.0 - the collective creation of content

WEB 4.0 - content thinks for the user

WEB 5.0 - the content deals with content

WEB 6.66 - the content deletes users, realizing that they are meaningless

WEB 7.0 - all content deletes itself, realizing that it is meaningless...

CONCLUSION

All Web sites make up the World Wide Web where communication (Web) brings together segments of information of the world community as a whole — database and communication of planetary scale. For direct access customers to Web sites on servers were specially designed the HTTP protocol.

Originally websites represent a set of static documents, type website. As communications, internal and external references. The site has become not only the role of help, annotations, and functional Office, news or Media Center. Currently, most of them are dynamic and interactive. In such cases the experts use the term Web application-ready software for your Web site. The

Web application is part of the website, but a Web application without this site is only technically. Shell (the form template) to populate and intensified. Website promotion has a capacious industry network.

Social networks and office workers

In Western countries, there has been a very interesting trend-bosses not forbid their employees spend some portion of their time on communication in social networks. In General, to large and middle companies control the communication of his subordinates are criticized not only for the employees, but also the authorities-in fact, "spy" for people from almost every country.

The results of the various statistical studies indicate that workers often communicate in social networks not to kill some time (at least in Western countries), and use modern means of communication with colleagues. For example the social networks.

In addition, the contact with colleagues and partners through social networks could save the company a solid means-in fact you don't need to hold meetings in realties, take large conference rooms to organize lunches. All can be done only by means of a computer, a webcam, microphone, and broadband Internet.

On-line services

But even at this seemingly perfect automated Internet businesses evolution of sites do not end there. Currently, the network appears more and more kinds «on-line» of services that allow us to make any transactions, sitting in front of a home computer. With the help of modern photographic technique to make an electronic image - a matter of minutes, go to jamaica.ru and order a T-shirt with your photo and text, choose a color, move the picture to the right place. You'll see your own product ready to directly in the Web browser!

Make payment by credit card on-line, pay for Internet access, without leaving the house, recharge your mobile phone - all these have not a luxury, but quite affordable services.

This list of on-line services is constantly growing. Feature of these services is their accessibility via the Internet. For example, before assembling the video clips were available only to specialists in video editing, but now, with Windows is Windows Movie Maker, which allows users to mount the video simple and the service site videascope.com makes the process not only easier but also allows you to publish created video on the Internet.

What awaits us?

Clearly, the Internet and provide information in it is far from exhausted. Not far off the appearance of an increasing number of different devices connected to the network: from telephones to refrigerators and coffee makers. Internet sites every day, providing services to millions, will become even more accessible and provide automatic access to these devices. How do you feel about the fact that your refrigerator will order products online store for you?

REFERENCES

1. www.wikipedia.org
2. www.artlebedev.ru
3. www.design.md
4. www.design.ua
5. www.livejournal.ru
6. www.cmsmagazine.ru
7. www.actis.ru
8. www.mdi.gov.md
9. www.cts.md
10. http://techcrunch.com/2010/12/05/social-networking-future/

THE COSTS OF ETHICS FOR CIO

LTC Ioan SOMESAN

INTRODUCTION

One may wonder if there is any relation between the ethics and costs as the ethics are generally considered to be just some morale principles which most of the time are not even written. Why would this be brought to the attention of the any Chief Information Officer, no matter what organization he is representing? In this paper you will find some answers to these questions.

Now, when the whole world is passing through the most serious financial crisis after the 2nd World War all governments in the world are analyzing the status of their economies, and reviewing their strategies, their policies in order to find solutions for actual problems and more, to resume the ascendant march of their economies and ensure a healthy and secure environment for their citizens. At these times any possible source of improvement should be carefully considered. However no matter what the new way to go for will be chosen, the ethics should be taken along, because the cost of having, implementing and respecting ethic's rules are way much smaller than the cost of not respecting them, which most of the time equals with complete failure.

I. DEFINITIONS OF ETHICS. GENERAL ETHIC PRINCIPLES

Origin: Latin *ēthicus* , Greek *ēthikós,* equiv. to *êth* (*os*) ethos + *-ikos* -ic

1. A system of moral principles: *the ethics of a culture.*[1]

2. The rules of conduct recognized in respect to a particular class of human actions or a particular group, culture, etc.: *medical ethics; Christian ethics.* [1]

3. Moral principles, as of an individual: *His ethics forbade betrayal of a confidence.* [1]

4. That branch of philosophy dealing with values relating to human conduct, with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions. [1]

5. A social, religious, or civil code of behaviour considered correct, especially that of a particular group, profession, or individual;[2]

6. The moral fitness of a decision, course of action, etc..[2]

As we can see there are many possible definitions however they are all showing that ethics is a set of rules and principles, a code of behavior considered correct, right or fair by a certain group, or organization. What is also important to be noted is that these rules are part of the culture of

the group or organization. As the manager of the change, the CIO should always be aware of the main traits of the organization's culture, and if necessary to change it also.

Before analyzing the costs of ethics we should first see what ethic rules and principles may be. Most of the ethical principles are basically the rules of common sense in almost any human collectivity, no matter the race, religion or level of education. This would be the honesty, integrity, loyalty, accountability, fairness, caring, respect, promise keeping.

To these, in the culture of most of the old nations responsible citizenship is also part of the general ethical principles. Going further, for different professional groups the ethical standards may differ. For example the honor, duty and complete dedication to the mission of defending the country are the core beliefs of all militaries in the service of their national armies.

As this papers is addressed specially to the chief information officers following you may find an example ethic principles to be observed by those in charge of managing information

II. THE CIO'S CODE OF ETHICS

On 30th of June 2003 Mary O'Doherty has published for the TechRepublic a guide of ethics rules to be observed by all CIOs specially with regard the managing the electronic data, using the knowledge and help of some very experienced CIOs.[6]

One of them is Sandy Hofmann, CIO at MAPICS, an Atlanta IT firm. One day, Hofmann discovered that a marketing employee had just given a 700-name customer list to a vendor. Hofmann chased down the vendor to retrieve the list. Then she gave the marketing associate a basic lesson in data management ethics: **Don't share customer information without the customers' permission**. "It's sort of like treating your family as well as your friends," said Hofmann, who works at MAPICS, a global IT firm focusing on manufacturing. Hofmann is one of a growing number of CIOs who are dealing with the responsibilities that come with being the main responsible of a company's data. CIOs, who are increasingly part of the top management team, are enacting strict controls over customer and employee data. They're also educating their employees about the responsibilities of ethical data management. Hofmann and several other CIOs helped TechRepublic compile the following code of ethics for managing electronic data.

1. **Customer data is sacrosanct.** Hofmann said CIOs are responsible for more than setting the rules. They also must be vigilant about making sure employees understand the rules. Hofmann said the incident was an object lesson about her duty to educate the new employees about MAPICS' customer information policies. At Worldspan, an online travel agency the company officials are so determined to enforce this rules that they're creating an online privacy course for employees who will be tested, said Sue Powers, CIO and senior vice

president. Powers discussed the idea at the last meeting of Worldspan's Privacy Council, a group she helped create after Worldspan officials noticed that the United States had few laws regarding privacy compared to other countries, particularly in the European Union. The security of customer data is a critical issue at Worldspan because customers give the company's employees their travel plans and credit information every day. In an effort to make her responsibility clear, Powers said, she's even been nicknamed the company's chief privacy officer. More strict these rules should be and thoroughly followed in the case of a governmental institution which is by law entitled to collect, and preserve private data of almost all citizens of a country.

2. **Make sure information gets to the top.** The trend of CIOs becoming part of top management means they have a duty to help shape an organization's values, said Stephen M. Paskoff, founder and president of Employment Learning Innovations, Inc., an Atlanta firm that trains companies on workplace ethics and fair employment practice issues. That means CIOs should create systems that enable employees to give information to the top bosses and then make sure that information is dealt with. For example, Paskoff said that could involve creating a way for employees to anonymously e-mail concerns to top management along with a system to follow up on the complaints. "CIOs should be thinking about internal complaints and issues with the same rigor that they are thinking about customer management. Is there a way to report a problem? Is there a way to make sure complaints get into the right person's hands? Is there a way under our system to make sure there is the proper follow-up?" said Paskoff, who was a trial attorney with the Equal Employment Opportunity Commission and represented management when he was in private practice with a law firm in Atlanta.
3. **Report accurate information, even if it's bad news.** Most of the times the bad news are much more important then the good ones. They are bringing up the problems to be addressed by the managers. If not spoken out the chance to be resolved is almost zero. Also sooner or later the problems will come to be known because the may aggravate to such an extension that they may compromise the entire activity of a company. Brian Oldham, CTO at Appriss in Louisville, said he's created an environment in which his employees feel comfortable reporting accurate and complete information to the bosses—even when they're pretty sure the bosses aren't going to like what they hear. At Appriss "We've adopted a culture that says share good news quick and bad news quicker," said Oldham, who as part of the senior management team is responsible for more than 90 employees. "We want our employees to know they can be safe presenting accurate information."

4. **Data must be protected over its lifecycle.** This would be part of the total quality management for the CIO. Every record has a lifetime, and CIOs are responsible for creating clear rules about what to do with electronic information from its birth to its death. Hofmann said she's tried to make it as easy as possible for employees to retain files. She's given them instructions on how to archive documents electronically and provided CD burners so they can download their material and send it back for off-site storage.
5. **Employee info deserves the same protection as customer info.** Because identity fraud is a threat to everyone; many employees have become more sensitive about the confidentiality of their personnel information. MAPICS learned that customers are sensitive about their information when it asked its 800 employees to update their emergency contact information. Some employees asked why they had to add their home addresses to a database to which all managers had access. MAPICS officials decided to limit access to the information to human resources and each employee's immediate manager.
6. **Give the right access to the right roles.** Through the policies enforced within the organization's information flows the CIO has the key role in establishing the right rules of access and correct authorities over the applications. For example the CIOs often have to mediate battles between software engineers and IT professionals over access. The software engineers say they need more access to operate efficiently. The IT folks say limits help keep data more secure. Oldham said his company preferred the safe side, even when that caution annoys the software engineers. "It does cause some frustration among software engineers who say if they have full access, they can get their jobs done quicker. But when access and security are in conflict, we err on the side of security," he said.

7. **Reward responsibility with trust.** At MAPICS, which was spun off of IBM in 1993, Hofmann took a different tack. Hofmann said her company's lineage meant that many MAPICS managers were well trained in the ethics of data management. The data management team was unanimous when Hofmann asked it to set a goal for the coming year. "It was easy; we said we need to liberate information because we spend so much time playing traffic cop." The result was named information liberation. Essentially, MAPICS gave managers more decision-making responsibilities about who should have access to their data. They also used portal technology to provide secure access to managers. In many cases, employees were given access to view information but were not able to modify it.

Hofmann is convinced that the initiative resulted in greater access to information but only for the people who really needed it. The idea wouldn't have worked if she hadn't trusted managers to make the right decisions. In other words, she had to give up some control over the information she's responsible for. She said that's a difficult bridge for a lot of CIOs to cross.

Another reference source on the information management ethics is “Ethics of Information Management” by Richard O. Mason, Florence M. Mason, and Mary J. Culnan, a book written specifically for information professionals. The authors develop a model of an information professional, and they define the wide range of jobs that these professionals hold. Because organizations are increasingly dependent on such people, the authors suggest that information workers assume a much more powerful and prominent public role. They also think that along with this power comes a greater need for ethical responsibility.

The authors believe that the responsibilities of information professionals fall into these broad categories: "collective social responsibilities and individual professional responsibilities." The authors define the following five social responsibilities:

* Develop and maintain a body of knowledge;
* Educate and train professionals;
* Monitor and self-regulate practice and practitioners;
* Set and monitor standards of acceptable practice;
* Educate the public regarding acceptable practices; [7]

Although to these we may add other “translations” of the general ethic principles in the “language” of any CIO, I’ll now go further to see how much the ethic principles may cost.

III. WHAT IS THE COST OF ETHICS?

Generally a cost benefit analysis is done to determine how well, or how poorly, a planned action will turn out. Although a cost benefit analysis can be used for almost anything, it is most commonly done on financial questions. Since the cost benefit analysis relies on the addition of positive factors and the subtraction of negative ones to determine a net result.

A cost benefit analysis finds, quantifies, and adds all the positive factors. These are the benefits. Then it identifies, quantifies, and subtracts all the negatives, the costs. The difference between the two indicates whether the planned action is advisable. Of high importance when doing a cost benefit analysis is making sure all the costs are included and all the benefits and properly quantify them. Should we hire an additional IT specialist? Is it a good idea to purchase the new technology? Will we be better off putting our free cash flow into securities rather than investing in additional capital equipment? Each of these questions can be answered by doing a proper cost benefit analysis.

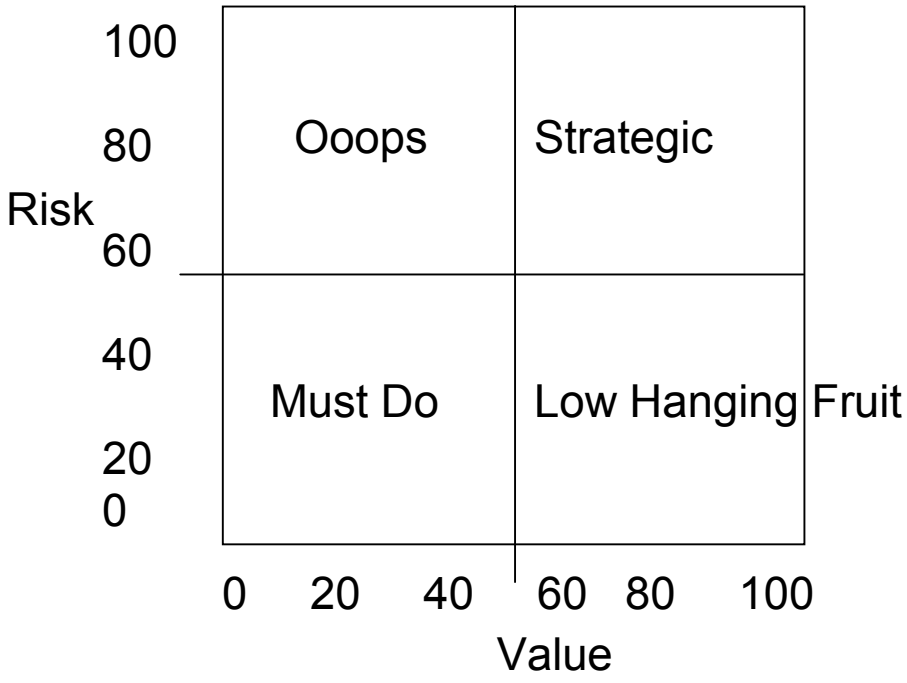
When we speak about ethics the cost benefit analyze becomes more difficult because the ethics is part of the organization’s culture, which are in fact abstract rules governing the behavior and actions of the majority of the people part of it. For a comprehensive approach I consider that the cost of ethics would be better described considered the following two situations:

1. What is the cost of implementing and respecting ethical rules?

2. What would be the cost of not implementing and respecting the ethical principles? These may be applied for a single activity, action, decision, or for the entire process developed by a specific organization.

1. The cost of implementing and fully respecting the ethic rules in any kind of business is given by the total amount of money spent over these, which may be:
   - the cost of the work time spent over establishing the set of rules to be respected within the organization;
   - the cost of the training of the personnel regarding this issues;
   - the cost of controlling the implementation and respecting the established rules;
   - the costs given by the assumed compliance with a specific set of rules, standards. For example the cost of creating and storing back-up data bases, preserving evidence of the products for the sake of showing responsibility and readiness to answer to any question may be raised by any stakeholder regarding the conformity of the product or the activity done.

Diane Bryant, CIO at Intel, says complying with ethical standards isn't cheap. Consider, she says, that Intel's storage requirements grow at 35% a year, driven in part by the need to retain data for compliance reasons and to fulfill potential e-discovery requests. "We do certainly talk a lot about the additional costs that come onto IT with all these additional ethics and security requirements. It's a very large spend for any IT organization, and it continues to grow," Bryant notes. "But it's talked about **as a must-do**. It's an accepted part of the IT budget." [5]



For a better understanding of what "must do" means for any investment, in the above diagram the "Must do" quadrant represents the part of the investments which are not expensive but without them the business can not exist. In other words even though the money spent on implementing ethics within the organization are small the result of not implementing them may cost as much as the whole business.

2. The cost of not implementing ethic principles in the life of any organization, as stated above may be as high as the complete failure of the business.

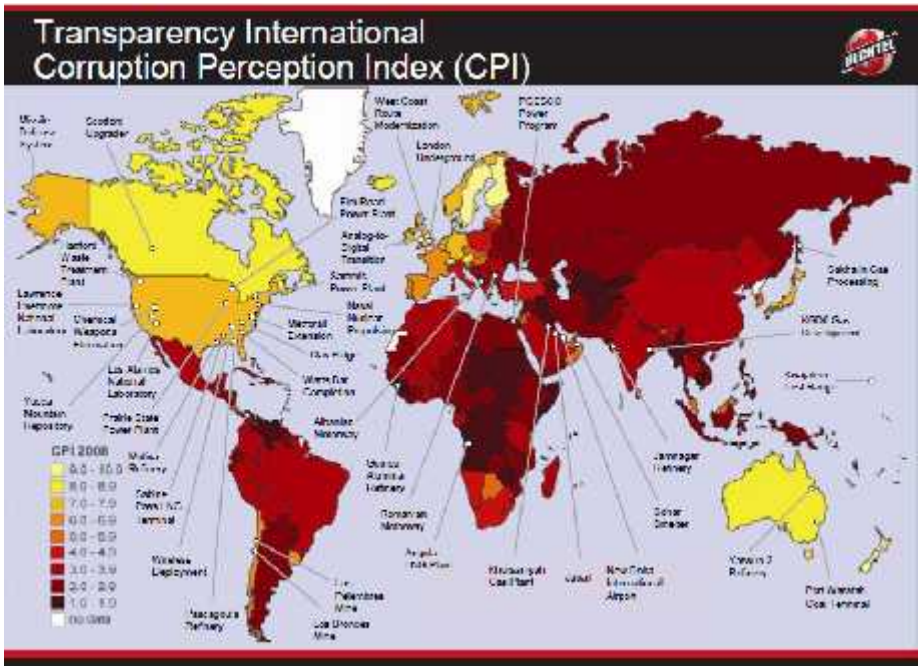
   From one end of any business process to the other the lack of ethics may result in direct and indirect losses. Starting with the sourcing of the business and finishing with the delivery of the final product or service, at all stages the process may be compromised. To name a few of many possible examples I may mention:

   - costly or useless acquisitions;
   - hiring unqualified personnel;
   - waste of resources;
   - abuses of any kind;
   - faked quality controls;
   - misuse of material and information resources;
   - break the contracted deadlines failing to meet the quality standards;

   No matter which is the ethical breach of the system, if not immediately addressed it will result in increasing costs, loosing of customers, failing the sponsors, and in the end the death of the business. Unfortunately for the state owned companies and governmental institutions when failing to meet the ethical principles loose will become public, harming the entire society. One may try to hide the problems from the system but the reality of the life shows that sooner or later the problem will show up.

As an example a 2008 report completed by Transparency International indicated that in a survey of 22 countries, construction in the public works sector was the most corrupt of 19 industry sectors.

Even though today the managers are expected to achieve good financial results with reduced costs and under the continuous pressure for a better and better quality of the products or services, the main cause of unethical behavior of the managers is one of the oldest human flaws, the greed, and the result of it is generally called corruption.



As shown in the same survey the institutional corruption is part of the every day life in throughout the world. However the bad effects are much more painful in the developing and poor countries, where each penny wasted or stolen is resulting in hunger, lack of medical assistance and death.

For this reason the corruption issue has been approached by most representative institutions of the world which have issued official and legal documents aiming to take this problem under control. Some of the most significant are:

- Foreign Corrupt Practices Act (FCPA)
- OECD Convention
- Corruption of Foreign Officials Act (Canada)
- United Nations Convention Against Corruption
- OAS Inter-American Convention Against Corruption
- Council of Europe Criminal Law Convention on Corruption

Going back to the information management, almost every day there are newspaper reports of unethical and illegal business activity. Much of this activity covers new and uncharted terrain; more and more of it relates to records and information management. In fact, reports indicate that the fastest growing crime in America is identity theft[7]. This is another reason of concern throughout the world, the privacy of our identity data. All stakeholders of any business have become more and more sensitive regarding this issue. As soon as they discover any misuse of their personal data they will for sure be avoiding working with that company.

To summarize the cost of not implementing and not obeying the ethical rules may be as high as the business itself. However in order to have a complete cot benefit analyze we should also consider the benefits of implementing ethics in the organization.

IV. BENEFITS OF ETHICS

God example of what may be the good outcome of implementing ethics in the organization is given by Carter McNamara in his "Complete Guide to Ethics Management: An Ethics Toolkit for Managers"[10] where he has given the following list describing various types of benefits from managing ethics in the workplace.

1. **Attention to business ethics has substantially improved society.** A matter of decades ago, children in our country worked 16-hour days. Workers' limbs were torn off and disabled workers were condemned to poverty and often to starvation. Trusts controlled some markets to the extent that prices were fixed and small businesses choked out. Price fixing crippled normal market forces. Employees were terminated based on personalities. Influence was applied through intimidation and harassment. Then society reacted and demanded that businesses place high value on fairness and equal rights. Anti-trust laws were instituted. Government agencies were established. Unions were organized. Laws and regulations were established.
2. **Ethics programs help maintain a moral course in turbulent times.** Attention to business ethics is critical during times of fundamental change -- times much like those faced now by businesses, both nonprofit and for-profit. During times of change, there is often no clear moral compass to guide leaders through complex conflicts about what is right or wrong. Continuing attention to ethics in the workplace sensitizes leaders and staff to how they want to act consistently.
3. **Ethics programs cultivate strong teamwork and productivity.** Ethics programs align employee behaviors with those top priority ethical values preferred by leaders of the organization. Usually, an organization finds surprising disparity between its preferred values and the values actually reflected by behaviors in the workplace. Ongoing attention and dialogue regarding values in the workplace builds openness, integrity and community - critical ingredients of strong teams in the workplace. Employees feel strong alignment between their values and those of the organization. They react with strong motivation and performance.
4. **Ethics programs support employee growth and meaning.** Attention to ethics in the workplace helps employees face reality, both good and bad -- in the organization and themselves. Employees feel full confidence they can admit and deal with whatever comes

their way. Bennett, in his article "Unethical Behavior, Stress Appear Linked" (Wall Street Journal, April 11, 1991, p. B1), explained that a consulting company tested a range of executives and managers. Their most striking finding: the more emotionally healthy executives, as measured on a battery of tests, the more likely they were to score high on ethics tests.

5. **Ethics programs are an insurance policy - they help ensure that policies are legal.** There is an increasing number of lawsuits in regard to personnel matters and to effects of an organization's services or products on stakeholders, ethical principles are often state-of-the-art legal matters. These principles are often applied to current, major ethical issues to become legislation. Attention to ethics ensures highly ethical policies and procedures in the workplace. It's far better to incur the cost of mechanisms to ensure ethical practices now than to incur costs of litigation later. A major intent of well-designed personnel policies is to ensure ethical treatment of employees, e.g., in matters of hiring, evaluating, disciplining, firing, etc.
6. **Ethics programs help avoid criminal acts "of omission" and can lower fines.** Ethics programs tend to detect ethical issues and violations early on so they can be reported or addressed. In some cases, when an organization is aware of an actual or potential violation and does not report it to the appropriate authorities, this can be considered a criminal act, e.g., in business dealings with certain government agencies, such as the Defense Department. The recent Federal Sentencing Guidelines specify major penalties for various types of major ethics violations. However, the guidelines potentially lower fines if an organization has clearly made an effort to operate ethically.
7. **Ethics programs help manage values associated with quality management, strategic planning and diversity management -- this benefit needs far more attention.** Ethics programs identify preferred values and ensuring organizational behaviors are aligned with those values. This effort includes recording the values, developing policies and procedures to align behaviors with preferred values, and then training all personnel about the policies and procedures. This overall effort is very useful for several other programs in the workplace that require behaviors to be aligned with values, including quality management, strategic planning and diversity management. Total Quality Management includes high priority on certain operating values, e.g., trust among stakeholders, performance, reliability, measurement, and feedback. Eastman and Polaroid use ethics tools in their quality programs to ensure integrity in their relationships with stakeholders. Ethics management techniques are highly useful for managing strategic values, e.g., expand market share, reduce costs, etc. McDonnell Douglas integrates their ethics programs into their strategic planning process.

Ethics management programs are also useful in managing diversity. Diversity is much more than the color of people's skin - it's acknowledging different values and perspectives. Diversity programs require recognizing and applying diverse values and perspectives -- these activities are the basis of a sound ethics management program.

8. **Ethics programs promote a strong public image.** Attention to ethics is also strong public relations -- admittedly, managing ethics should not be done primarily for reasons of public relations. But, frankly, the fact that an organization regularly gives attention to its ethics can portray a strong positive to the public. People see those organizations as valuing people more than profit, as striving to operate with the utmost of integrity and honor. Aligning behavior with values is critical to effective marketing and public relations programs. Consider how Johnson and Johnson handled the Tylenol crisis versus how Exxon handled the oil spill in Alaska. Bob Dunn, President and CEO of San Francisco-based Business for Social Responsibility, puts it best: "Ethical values, consistently applied, are the cornerstones in building a commercially successful and socially responsible business."
9. **Overall benefits of ethics programs:** Donaldson and Davis, in "Business Ethics? explain that managing ethical values in the workplace legitimizes managerial actions, strengthens the coherence and balance of the organization's culture, improves trust in relationships between individuals and groups, supports greater consistency in standards and qualities of products, and cultivates greater sensitivity to the impact of the enterprise's values and messages.
10. **Last - and most -- formal attention to ethics in the workplace is the right thing to do.**[10]

V. CONCLUSION

In the nowadays world, when the IT development and the exponentially growth of the speed and amount of data exchange which has a great impact over all aspects of our lives, the role and responsibility of the CIOs and all other information managers is higher and higher. To be sure that they are on the right way they should always observe and follow the ethical principles.

The father of the ethics is considered to be the Greek philosopher Socrates (469-399 BC), whom has identified knowledge with virtue. If knowledge can be learned, so can virtue. Thus, virtue can be taught. He also believed that "Our true happiness is promoted by doing what is right".

By now we have learned that the cost of implementing ethics is really small if counted in money, while the cost not implementing ethical principles may be the complete failure, the breakdown of the any company. In the same time we learned that the benefits of implementing ethical principles are kind of guarantee for a strong organization and healthy work environment, essential in the relation with customers and all other stakeholders.

It is at the hand of the managers to implement the ethical policies the compliance rules and more than that to practice everyday an ethical leadership stile, which by Socrates will lead the organization to the state of "happiness".

REFERENCES

1. Dictionary.com Unabridged Based on the Random House Dictionary, © Random House, Inc. 2010
2. World English Dictionary – quoted on the web page of the above mentioned source.
3. A brief history of information ethics THOMAS FROEHLICH, School of Library and Information Science, Kent State University
4. Running The Numbers By F. John Reh, About.com Guide
5. How the Recession Can Force Companies to Compromise Business Ethics - By Mary K. Pratt, August 23, 2009 - http://www.cio.com
6. The CIO's code of ethics for managing electronic data, by Mary O'Doherty – 30 June 2003 - http://articles.techrepublic.com.com/5100-10878_11-5035191.html
7. Book review: Ethics of Information Management By Bennett, James C, Publication: Information Management Journal, October 1st 2001
8. Department of Defense Regulation 5500.7-R, chapter 12, section 5, pp. 155-157
9. Ethics at All Cost, Adrian Zaccaria, April 30, 2009
10. Complete Guide to Ethics Management: An Ethics Toolkit for Managers, Copyright Carter McNamara, MBA, PhD, Authenticity Consulting, LLC. - **h**ttp://www.managementhelp.org/ethics/ethxgde.htm)

THE CIO's, HISTORY, PRESENT AND FUTURE

CAPT. Cozmin TRANDAFIR

INTRODUCTION

The point of departure is the information explosion and the growing recognition of the need to harness this resource. The problem of information overload is as great as the lack of information. Now, the focus of attention is the information not the technology.

The Paperwork Reduction Act from 1980, defined "information resources" as information collection requests containing a data profile for each request. The goal of Paperwork Reduction Act in federal agencies of the US was to improve the data/information management and ensure a common platform for agencies. The goals in the private sector centred on the elimination of redundant document processing activities and facilitating access to the information.

IRM has three goals: to maintain a global view of corporate data, to position the chief information officer at a high level in the corporate hierarchy, and to integrate both information and the information technologies.

The 1996 Clinger-Cohen Act establish in each military/civilian organization a Chief Information Officer (CIO) – to focus on IRM management, and one of the main issues was to management reform, institutional change and electronic government.

But E-Government Act of 2002 established "The Federal CIO" with the goal to "improve government performance through information technology".

I. CIO HISTORY

The **chief information officer**, or **information technology** (**IT**) **director**, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO typically reports to the chief executive officer, chief operations officer or chief financial officer. In military organizations, they report to the commanding officer. (From Wikipedia, the free encyclopedia)

Another definition of CIO: The executive officer in charge of information processing in an organization. All systems design, development and datacenter operations fall under CIO jurisdiction. CIOs have demanding jobs as information systems in an organization are often taken for granted until something breaks down. The CIO is responsible for explaining to executive management the complex nightmare this industry has gotten itself into over the past 40

years and why equipment must be constantly retrofitted or replaced. Justifying new expenditures can be a difficult part of the job.

Increasingly, CIOs are involved in creating business and e-business opportunities through information technology. Collaborating with other executives, CIOs are often working at the core of business development within the organization.

Information technology and its systems have become so important that CIO has come to be viewed in many organizations as the key contributor in formulating strategic goals for an organization. The CIO manages the implementation of the useful technology to increase information accessibility and integrated systems management. As a comparison, where the CIO adapts systems through the use of existing technologies, chief technology officer develops new technologies to expand corporate technological capabilities. When both positions are present in an organization, the CIO is generally responsible for processes and practices supporting the flow of information, whereas the CTO is generally responsible for technology infrastructure.

The prominence of the CIO position has risen greatly as information technology has become a more important part of business. The CIO may be a member of the executive board of an organization. As information technology and systems have become more important, the CIO has come to be viewed in many organizations as a key contributor in formulating strategic goals. No specific qualification is intrinsic of the CIO position, though the typical candidate may have expertise in a number of technological fields - computer science, software engineering, or information systems.

Typically, a CIO is involved with analyzing and reworking existing business processes, with identifying and developing the capability to use new tools, with reshaping the enterprise's physical infrastructure and network access, and with identifying and exploiting the enterprise's knowledge resources. Many CIOs head the enterprise's efforts to integrate the Internet into both its long-term strategy and its immediate business plans.

II. CIO TODAY

II.1. The role of the CIO

The role of the CIO varies as does the business models in place today. Many CIO’s evolved into these roles from a variety of early disciplines, such as technology, finance, manufacturing, service, and so forth. The particular expertise that a CIO develops over his or her career becomes a determining factor in the roles he or she fulfills, but is as equally a key determinant of the type of business that may employ him or her. The corporate leadership determines the type of CIO required based on the company's expectations.

The Technology Leader: Leaders of IT are promoted from information systems departments, where they were applications, operations, or business analysis leaders. This approach continues to provide CIOs.

This type of experience has been repeated numerous of times in which managers from engineering, software development, and others have successfully transitioned their careers into the IT platform.

The Business Leader: Business leaders from services, manufacturing or marketing industries have also transitioned into CIO roles the last 10 years. It's important to understand a business' specific needs. This led to the growth of business-driven CIOs within the IT arena. Just as well, IT managers are becoming more knowledgeable with tools and systems in order to compete. CIOs assume their positions not only to leverage the technology skills they developed as business leaders, but also because it's a vehicle to a CXX position.

The Strategist and Mentor: The strategist and mentor type of CIO operates in a fashion similar to that of a Chief Technology Officer (CTO) in a high-tech environment. These individuals focus on strategic directions for the corporation and perform as mentors and advisors to the corporate staff members such as other CXOs. These CIOs are typically grounded in strategic thinking, and play an active role in the product/service development side as well as the marketing/sales side. They focus on issues such as business and IT alignment, they attempt to uncover IT-enabled business opportunities, and apply IT initiatives to streamline business processes. These CIOs are the best candidates to become the CEOs of their companies. They have developed an all-encompassing view of the enterprise and therefore become key mentors the CEO.

The Corporate Influencer: This CIO is molded by the type of business environment he must support and his influence is driven by the characteristics of the business. More than likely the two areas of focus are strategy and execution. Most CIOs are expected to play an equally important role in both arenas. The strategic side of the CIO requires a focus on business, IT alignment, and IT-enabled opportunities. The execution side requires active participation in the execution of major projects in areas like ERP, CRM, and so on. Now, the role of Chief Technology Officer evolved, in the last few years, to further delineate between an execution-based CIO role and a strategic-based one, rather than combining these aspects. The CTO has been more focused on operations, technology, and product development.

II. 2. The challenge to CIO's

CIO's in today's business environment are challenged to deliver more results while reducing costs. Additionally, the business is challenging IT to clearly demonstrate its value. In essence,

business executives are demanding to understand how the millions invested in IT truly contribute to the business and what it wants to accomplish.

- *Value challenges* - A common concern is that IT executives do not fully understand the critical aspects of business and how technology contributes to desired business outcomes. Questions to be answered: How can IT drive business operations and growth? How can IT create business opportunities? How can IT transform the business? How do you demonstrate IT's contributions to desired business outcomes?
- *Alignment challenges* - IT is often criticized for acquiring technology "for technology's sake". A criticism often well deserved. Questions to be answered: How can you determine and demonstrate how IT as an organization can do a better job of aligning with the business? How do you acquire and utilize a clear view of business objectives to better inform and liaison with your peers on the executive management team, as well as the CEO? How do you align the behavior of your staff to stay on course with these business objectives?
- *Cost challenges* - In many, if not most, organizations IT is considered a cost center. Much has been written about IT as a strategic investment, but in reality, it is often a difficult-to-explain expense. Questions to be answered: Why is this failing? How do you make IT more cost-efficient, while effecting ways to incorporate return on investment evaluations into your planning and decision making processes?
- *Planning challenges* - IT often allocates sufficient resources to planning, but the process is seldom formalized. As a result, planning is disconnected and ineffective. Questions to be answered: How do you formalize and implement an IT planning process that is integrated with business planning and budgeting? How do you develop practical action plans to better manage your investments and outcomes?
- *Communication challenges* - Often IT appears to be operating in isolation. IT executives must improve their relationships and communications with other business units. With better internal communications IT can lower the silos and develop synergies. Questions to be answered: What should CIO's listen for when speaking with executive management? What is the most effective way to communicate "IT" to non-IT executives?
- *Culture challenges* - IT has credibility problems in many organizations. There is a culture of mistrust between IT and other business units. Questions to be answered: How can you make IT more adaptable and relationship-oriented? How can your IT executives create an environment to cultivate creative solutions? How do you deal with perceptions that centralized IT is bureaucratic?

- *Service challenges* - IT is a service provider and needs to behave in service-oriented and customer-centric ways. In many organizations there is a general lack of understanding about service management. Questions to be answered: What are the right things and the right ways to measure and manage your organization? How can your services become more cost-effective and efficient? How can your IT organization be more proactive in delivering critical services?
- *Sourcing challenges* - There are different ways to source new systems and services - build, buy and ASPs, among others. IT needs to explore alternatives to manage different types sourcing relationships and service levels. Questions to be answered: What are the key differences in managing your own staff and managing a vendor in the delivery of IT services? What are the appropriate service level agreements?
- *Technology challenges* - Keeping up with all the technology innovations is always a challenge. IT executives need to determine the real impact e-commerce, relationship management systems, broadband and wireless technologies have on business results, as well as the true costs. Questions to be answered: How do you assess, build and operate comprehensive and integrated technology architectures that have an impact on desired business outcomes? How do you improve availability, performance and security in cost-efficient and effective ways?
- *Process challenges* - If asked to select an area for improvement with the greatest impact on the ability of IT to contribute to the business, the answer is IT processes. At the core of 95% of IT problems are process and organization dysfunction, not technology. May we repeat: It's not about technology! Many organizations need to give serious consideration to their IT processes and the ways they manage requirements, changes, performance, capacity, problems, configurations, assets, releases, disasters and security, among others. IT processes are the number one source of issues. Questions to be answered: How do you implement centralized controls (standards, architectures, management systems) with decentralized operations? How can IT work closely with business units to identify project requirements? How do you fuse system development and infrastructure development lifecycles? How do you formalize continuous improvements? How do you change the behaviors of your whole organization?
- *Organization challenges* - Good IT staff are difficult to employ and retain and the gap between the demand and supply of IT skills will increase. Questions to be answered: How do you evaluate and implement alternate staffing and training solutions? How do you manage your staff with productivity and job satisfaction in mind?

II.3. Opportunities

It's not about the technology, and it never will be. It's about people and the way they go about their business. The goal is to support and drive the business. Technology is a tool, an enabler. In essence, technology enables people to drive the business.

With rapid changes in politics, economics, business, and technology, there are vast opportunities to leverage innovative solutions to initiate fundamental transformations in the business. There are real opportunities to drive the business toward its goals, providing more and better services (e.g., faster, simpler, more reliable, more secure, etc.). Given the current environment there are real opportunities for IT to:

- Transform the business
- Provide innovative solutions
- Contribute to desired business outcomes
- Drive business growth

All organizations are looking for ways to be more efficient and effective in their market space. With greater emphasis on achieving more value from IT, you are expected to deliver more and better services using fewer resources. Moreover, the technology is only as good as the people who make it, implement it, operate it and use it. To be in control, CIO's need a systematic approach.

III. CIO FOR THE FUTURE

III.1. Fundamental trait of a CIO

A CIO may focus on different aspects of his organization. Five especially important fundamentals that a CIO needs to be cognizant of are regardless of the current focus. If internalized by IT staffers, these fundamentals can dramatically transform a technology-centric IT organization into a business-focused one, almost without effort: Passion, Humility, Openness, Clarity and Agility.

Each of these fundamentals reinforces the effect of others.

Passion

There is no substitute for a CIO's passion for the industry and the business that he or she is in. In general, executives are hired not only for their professional qualifications but also for their experience in a particular industry, which enriches the collective wisdom of the senior management team. But CIO's are often hired for their professional qualifications alone, regardless of their experience in the industry. This is not a desirable practice.

If a CIO is interested only in IT, one should question his or her potential value to the business. Without developing a passion for the industry and the business that he or she is in, it will be

difficult for the CIO to develop the insights, acumen, and big picture mindset needed to help the business to achieve its goals. If a CIO's only value is running IT like a utility, there is little reason to keep that IT organization in house. Many IT outsourcing vendors can probably do better in this regard, at the least through economies of scale.

IT is about creating a competitive advantage for the business. That starts with a CIO who has passion well beyond IT.

Humility

In the past there was a huge technology gap between the haves and the have-nots-that is, between MIS professionals and business users. MIS professionals were seen as all-knowing people who wielded the power of mysterious machines in the basement. Then the revolution of the personal computer came. For the first time, business managers could perform rudimentary forecasts without the help of MIS.

Some might argue that it was all downhill for IT from there. IT is not about control, as in the old mainframe days. IT is about empowering IT customers to unleash their potential to succeed in whatever they set out to do. The more technically inclined IT customers are; the easier it is to empower them. The less time IT spends on technology, the greater the effort IT can devote to the business, and the more business value IT can generate.

CIO's, therefore, should not feel challenged by technically inclined customers; we should try to learn from them. Seeking first to understand is the key in creating alignment. They should learn from all of our constituents: IT staffers, executive peers, internal IT customers, their business's customers and partners, vendors, industry peers, analysts, everyone. They should strive to understand their goals, visions, concerns, fears, likes, dislikes, and even their own technical solutions, everything that they can possibly learn. They learn from people's successes, and other times they learn from their mistakes … and that is extremely valuable too.

CIO's should stop talking, and start listening with humility. Only by understanding our constituents can they possibly become a trusted partner, and help IT become more closely aligned to the business.

Openness

No doubt, CIO's are all very successful and smart people. Over the years, they build up certain beliefs and certain rituals. Things have got to be done in a certain way or they will fail; after all, they've tried all the alternatives. They have their battle scars to prove their point. If they keep doing what they were doing yesterday, how can they possibly create a competitive advantage for their business when their competitors are moving forward? Is it perhaps time to leave their baggage behind?

If a CIO encourages a sense of openness throughout his or her IT organization, IT staffers will be more inclined to be creative, think outside the box, take risks, and at the end of the day, perform often needed "miracles."

Clarity

Clarity is the ability to see the fundamentals, to be able to turn complex, muddy issues into simple, clear concepts and solutions. Clarity is a necessary skill for leaders; successful leaders use clarity in order to direct.

An IT organization, armed with its knowledge and tools, can add great value to a business by providing relevant and timely information so that business leaders can have clarity. IT was previously known as Management Information Systems; providing both clarity and the information that others need to have clarity is, in fact, at IT's root. CIO's should stay true to their roots. Not only they should provide clarity in every interaction with their constituents, they should inspire all their constituents, especially IT staffers, to do the same.

IT is sometimes perceived by their customers as providing the opposite of clarity. In fact, IT always seems to make everything more complex than necessary. In conveying a sense that it is doing IT for the sake of IT, IT becomes a runaway freight train. This problem is especially prevalent among technology-centric IT organizations. It is a very dangerous problem to have. Whether the CIO is at fault or not, he or she may quickly loose his or her credibility.

As both IT and the business its supports become more complex, CIO's should seize the opportunity to be true leaders. Instead of getting tangled in complexities, CIO's should:

- Practice simplicity, the best antidote.
- Ask simple, insightful questions to seek practical solutions.
- Consider everything in terms of its most basic fundamentals.

Very soon, the CIO can become a leader of clarity revered for his or her uncommon wisdom.

Agility

Agility: the ability to move quickly and effectively.

Agility can be thought of as the result of applying passion, humility, openness, and clarity. Passion gives them insight into the business that they support. Humility encourages them to listen to and understand all of their constituents. Openness enables them to embrace new ideas and to make the right decisions. Clarity allows them to be wise and able to direct proper actions. These four fundamentals, if combined and used, should almost always produce a competitive advantage in the form of increased speed for the business, such as quicker time to market, increased inventory turns, and so on.

This should not come as a surprise; one of the functions of IT is to make a business more agile. While some say that technology can make a business more agile, he thinks this is misleading.

Technology by itself can never make a business more agile, but the right IT people applying the right technology at the right time can.

Agility can also be considered separately, and can support the other four fundamentals. Think agile! Be proactive! Get something done! Treating agility as a separate fundamental is especially important to IT. While IT is helping the business to become more agile, IT needs to become more agile itself. Many of CIO's have had the experience of having the business perceive IT as an obstacle to agility.

To achieve better agility within IT, the CIO needs to put passion, humility, openness, and clarity into action, and encourage IT staffers to think and act agile.

In today's hyper competitive but cost conscious environment, agility is not only a much sought-after virtue, but can mean the difference between success and failure for the business that we support.

III. 2. CIO new challenges for the future

Many candidates for CIO position have Master of Business Administration or Master of Science in Management degrees. More recently CIOs' leadership capabilities, business acumen and strategic perspectives have taken precedence over technical skills. It is now quite common for CIOs to be appointed from the business side of the organization, especially if they have project management skills.

In 2007 a survey amongst CIOs by *CIO* magazine in the UK discovered that their top 10 concerns were: people leadership, managing budgets, business alignment, infrastructure refresh, security, compliance, resource management, managing customers, managing change and board politics.

The CIO is evolving into a role where he/she is creating and monitoring business value from IT assets, to the point that the Chief Information Officer (CIO) be replaced with Chief Internal Investments Officer (CIIO).

The economic downturn of late 2001, and the abrupt reversal of fortune for many technology giants, brought with it another shift in the role of the CIO. Those executives who had become business partners in a net-based system of inter-related services were now at risk. Those executives who had focused on the technology were now at risk, as they represented an irrational investment that had not yet produced the promised revenue. Now, those executives who remained “hands-on” managers of their institutions’ infrastructure operations found themselves without budgets, losing employees, and now directly supporting their internal customers. Unfortunately, as the recession impacted revenue streams, numerous companies removed the position of CIO entirely.

Next four years will be a unique opportunity for success or fail said John Gantz, vice-president of International Data Corporation (IDC) during CIO 2009 Summit, organized in Auckland, New Zeeland. Word crises and opportunities are connected, but you must have an proactive attitude to get something good from crises.

Been proactive means a 100% involvement, which means that IT must work with business unit and suppliers like neither before. IT department will must reorganize or change their work stile. It needs must align to business objectives.

For CIO, Gantz said that in the next four years will be significant changes for IT. In this period will raise the request for IT personnel and number of servers will double. Number of mobile users will be tripled and amount of data will be four time bigger, all this conducting to increasing level of security and questions about data will be stored and data to renounce.

CONCLUSIONS

For looking to the future of the CIO we have to take a walk in the past. When IRM was born computer science was just at the beginning.

In the early 80's personal computer just appeared and for use you need special knowledge and special skills. So specialists must handle'it and specialist must take the task of explain their role. Don't forget that at the beginning of 1980' if you have something to compute you must go to a computing centre or a big company that afford a computer.

So, in that time a position like a director who is in charge with dealing with this increasing amount of data was necessary.

But in our days, I believe that things are changing. Most of the director was young in the early 1980, and most of them have at least basic knowledge of IT.

Where is the place for a CIO?

Well in the U.S. they still have this kind of director and especially in governmental agencies. Some corporation still have this position, some have the position of IT director, some companies don't consider this position important enough to published this position.

The U.S. Chief Information Officer (CIO) is a position newly created by the Obama Administration. The U.S. CIO oversees Federal information technology (IT) spending to ensure that the Federal Government is leveraging the spirit of American innovation and the power of technology to improve performance and lower the cost of Government operations. On March 5, 2009, President Obama named Vivek Kundra the first CIO of the United States.

Department of Defense is a place where CIO has its place with mission, vision, goals and objectives.

In Europe was started in the earlier 2000's with eEUROPE project. But here countries applied in the CIO concept in their traditional ways. Some countries adopted the CIO name another still keep the IT Director name but in instance is the same. Norway succeeded to confirm that the internet is a human right and allowed connection at a limited speed to anyone for free.

A CIO should in the first place situate in governmental agencies in that position that allowed them or to directors competence to invest in future technologies. In private corporation tasks for a CIO should be more difficult. CEO believe that CIO would offer for their companies state of the art technologies, but all that CEO wants is an IT strategy with reduced costs.

So the future for the CIO could be bright or could be ordinary. That depends of a lot of things. Informational era is at the beginning. Anything could happen.

REFERENCES

1. http://www. en.wikipedia.org/wiki/CIO
2. http://www.pcmag.com/encyclopedia_term/0,2542,t=CIO&i=39685,00.asp
3. http://www.harriskern.com
4. http://www.computerworld.ro

BALANCED SCORECARD – A MODERN MANAGEMENT APPROACH

CAPT Florin OGÎGĂU

INTRODUCTION

The balanced scorecard is a strategic planning and management system that is used extensively in business and industry, government, and non-profit organizations worldwide to align business activities to the vision and strategy of the organization, improve internal and external communications, and monitor organization performance against strategic goals. It was originated by Drs. Robert Kaplan (Harvard Business School) and David Norton as a performance measurement framework that added strategic non-financial performance measures to traditional financial metrics to give managers and executives a more 'balanced' view of organizational performance. While the phrase balanced scorecard was coined in the early 1990s, the roots of the this type of approach are deep, and include the pioneering work of General Electric on performance measurement reporting in the 1950's and the work of French process engineers (who created the ***Tableau de Bord*** - literally, a "***dashboard***" of performance measures) in the early part of the 20th century.

BALANCED SCORECARD A MANAGEMENT SYSTEM

The balanced scorecard has evolved from its early use as a simple performance measurement framework to a full strategic planning and management system. The "new" balanced scorecard transforms an organization's strategic plan from an attractive but passive document into the "marching orders" for the organization on a daily basis. It provides a framework that not only provides performance measurements, but helps planners identify what should be done and measured. It enables executives to truly execute their strategies.

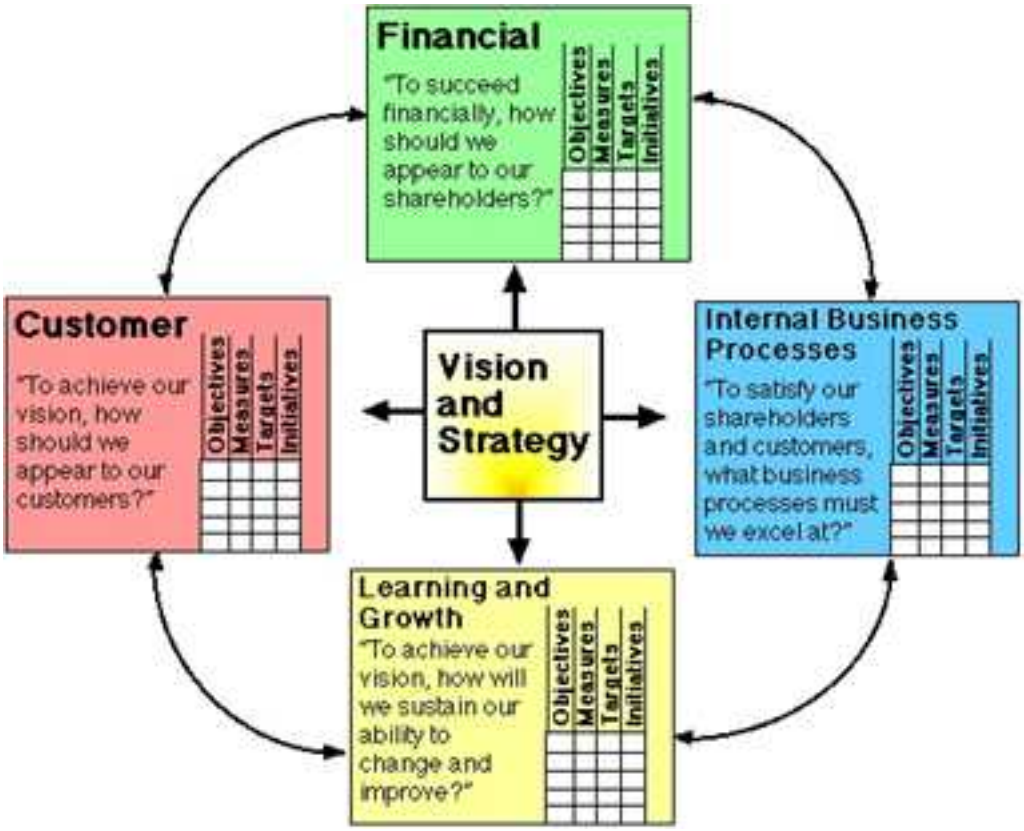
This new approach to strategic management was first detailed in a series of articles and books by Drs. Kaplan and Norton. Recognizing some of the weaknesses and vagueness of previous management approaches, the balanced scorecard approach provides a clear prescription as to what companies should measure in order to 'balance' the financial perspective. **The balanced scorecard is a management system (not only a measurement system) that enables organizations to clarify their vision and strategy and translate them into action. It provides feedback around both the internal business processes and external outcomes in order to continuously improve strategic performance and results.** When fully deployed, the balanced

scorecard transforms strategic planning from an academic exercise into the nerve centre of an enterprise.

Kaplan and Norton describe the innovation of the balanced scorecard as follows: *"The balanced scorecard retains traditional financial measures. But financial measures tell the story of past events, an adequate story for industrial age companies for which investments in long-term capabilities and customer relationships were not critical for success. These financial measures are inadequate, however, for guiding and evaluating the journey that information age companies must make to create future value through investment in customers, suppliers, employees, processes, technology, and innovation. "*

BALANCED SCORECARD FOUR PERSPECTIVES

The balanced scorecard suggests that we view the organization from four perspectives, and to develop metrics, collect data and analyze it relative to each of these perspectives:



The Learning & Growth Perspective

This perspective includes training and corporate cultural attitudes related to both individual and corporate self-improvement. In a knowledge-worker organization, people - the only repository of knowledge - are the main resource. In the current climate of rapid technological change, it is becoming necessary for knowledge workers to be in a continuous learning mode. Government agencies often find themselves unable to hire new technical workers, and at the same time there is a decline in training of existing employees. This is a leading indicator of 'brain drain' that must

be reversed. Metrics can be put into place to guide managers in focusing training funds where they can help the most. In any case, learning and growth constitute the essential foundation for success of any knowledge-worker organization.

Kaplan and Norton emphasize that 'learning' is more than 'training'; it also includes things like mentors and tutors within the organization, as well as that ease of communication among workers that allows them to readily get help on a problem when it is needed. It also includes technological tools: what the Baldrige criteria call "high performance work systems."

The Business Process Perspective

This perspective refers to internal business processes. Metrics based on this perspective allow the managers to know how well their business is running, and whether its products and services according to beneficiary requirements (the mission). These metrics have to be carefully designed by those who know these processes most intimately; with our unique missions these are not something that can be developed by outside consultants. In addition to the strategic management process, two kinds of business processes may be identified: ***a) mission-oriented processes***, and ***b) support processes***.

Mission-oriented processes are the special functions of government offices, and many unique problems are encountered in these processes. The ***support processes*** are more repetitive in nature and hence easier to measure and benchmark using generic metrics.

The Beneficiary Perspective

Recent management philosophy has shown an increasing realization of the importance of focus and beneficiary satisfaction in any business. These are leading indicators: if beneficiary are not satisfied, they will eventually find other suppliers that will meet their needs. Poor performance from this perspective is thus a leading indicator of future decline, even though the current financial picture may look good.

In developing metrics for satisfaction, beneficiary should be analyzed in terms of kinds of customers and the kinds of processes for which we are providing a product or service to those customers groups.

The Customer Perspective

Recent management philosophy has shown an increasing realization of the importance of customer focus and customer satisfaction in any business. These are leading indicators: if customers are not satisfied, they will eventually find other suppliers that will meet their needs.

Poor performance from this perspective is thus a leading indicator of future decline, even though the current financial picture may look good.

In developing metrics for satisfaction, customers should be analyzed in terms of kinds of customers and the kinds of processes for which we are providing a product or service to those customer groups.

The Financial Perspective

Kaplan and Norton do not disregard the traditional need for financial data. Timely and accurate funding data will always be a priority, and managers will do whatever necessary to provide it. In fact, often there is more than enough handling and processing of financial data. With the implementation of a corporate database, it is hoped that more of the processing can be centralized and automated. But the point is that the current emphasis on financials leads to the "unbalanced" situation with regard to other perspectives.

There is perhaps a need to include additional financial-related data, such as risk assessment and cost-benefit data, in this category.

THE BALANCED SCORECARD AND MEASUREMENT-BASED MANAGEMENT

The balanced scorecard methodology builds on some key concepts of previous management ideas such as Total Quality Management (TQM), including customer-defined quality, continuous improvement, employee empowerment, and-primarily -measurement-based management and feedback.

Double-Loop Feedback

In traditional industrial activity, "quality control" and "zero defects" were the watchwords. In order to shield the customer from receiving poor quality products, aggressive efforts were focused on inspection and testing at the end of the production line. The problem with this approach - as pointed out by Deming – is that the true causes of defects could never be identified, and there would always be inefficiencies due to the rejection of defects. What Deming saw was that variation is created at every step in a production process, and the causes of variation need to be identified and fixed. If this can be done, then there is a way to reduce the defects and improve product quality indefinitely. To establish such a process, Deming emphasized that all business processes should be part of a system with feedback loops. The feedback data should be examined by managers to determine the causes of variation, what are

the processes with significant problems, and then they can focus attention on fixing that subset of processes.

The balanced scorecard incorporates feedback around internal business process outputs, as in TQM, but also adds a feedback loop around the outcomes of business strategies. This creates a "double-loop feedback" process in the balanced scorecard.

Outcome Metrics

You can't improve what you can't measure. So metrics must be developed based on the priorities of the strategic plan, which provides the key business drivers and criteria for metrics that managers most desire to watch. Processes are then designed to collect information relevant to these metrics and reduce it to numerical form for storage, display, and analysis. Decision makers examine the outcomes of various measured processes and strategies and track the results to guide the company and provide feedback. So the value of metrics is in their ability to provide a factual basis for defining:

- Strategic feedback to show the present status of the organization from many perspectives for decision makers
- Diagnostic feedback into various processes to guide improvements on a continuous basis
- Trends in performance over time as the metrics are tracked
- Feedback around the measurement methods themselves, and which metrics should be tracked
- Quantitative inputs to forecasting methods and models for decision support systems

Management by Fact

The goal of making measurements is to permit managers to see their company more clearly - from many perspectives-and hence to make wiser long-term decisions. The Baldrige Criteria (1997) booklet reiterates this concept of fact-based management: "Modem businesses depend upon measurement and analysis of performance. Measurements must derive from the company's strategy and provide critical data and information about key processes, outputs and results.

Data and information needed for performance measurement and improvement are of many types, including: customer, product and service performance, operations, market, competitive comparisons, supplier, employee-related, and cost and financial. Analysis entails using data to determine trends, projections, and cause and effect that might not be evident without analysis. Data and analysis support a variety of company purposes, such as planning, reviewing company

performance, improving operations, and comparing company performance with competitors' or with 'best practices' benchmarks.

A major consideration in performance improvement involves the creation and use of performance measures or indicators. Performance measures or indicators are measurable characteristics of products, services, processes, and operations the company uses to track and improve performance. The measures or indicators should be selected to best represent the factors that lead to improved customer, operational, and financial performance. A comprehensive set of measures or indicators tied to customer and/or company performance requirements represents a clear basis for aligning all activities with the company's goals. Through the analysis of data from the tracking processes, the measures or indicators themselves may be evaluated and changed to better support such goals."

CRITICISM

A criticism of balanced scorecard is that the scores are not based on any proven economic or financial theory and have no basis in the decision sciences. The process is entirely subjective and makes no provision to assess quantities like risk and economic value in a way that is actuarially or economically well-founded. The Balanced scorecard does not provide a bottom line score or a unified view with clear recommendations; it is simply a list of metrics. Positive responses from users of balanced scorecard may merely be a type of placebo effect. There are no empirical studies linking the use of balanced scorecard to better decision making or improved financial performance of companies.

BENEFITS OF STRATEGIC MEASUREMENT WITH A BALANCED SCORECARD

The main advantages from using balanced scorecard in an organization are:

1. Simplifies managers' lives by providing focus and prioritizing actions and resources.
2. Eliminates information overload by bringing together crucial elements.
3. Improves communication by providing a common language and reliable information about current organizational strengths and weaknesses. Everyone understands the strategy, their role in helping achieve it, and how their efforts will be measured and rewarded.
4. Forces the management team to clarify the strategy to a level of specificity at which its implementation can be measured.
5. Helps managers understand interrelationships by tracking how improvements in one area impact other areas.

REFERENCES

1. Douglas W. Hubbard "How to Measure Anything: Finding the Value of Intangibles in Business" John Wily & Sons. 2007.
2. Cobbold. I. and Lawrie. G. "The Development of the Balanced Scorecard as a Strategic Management Tool". Performance Measurement Association 2002
3. Cobbold. I and Lawrie. G. "Classification of Balanced Scorecards based on their effectiveness as strategic control or management control tools". Performance Measurement Association 2002.
4. Kaplan R S and Norton D P "The balanced scorecard: measures that drive performance". Harvard Business Review Jan- Feb pp71-80.
5. Kaplan R S and Norton D P "Putting the Balanced Scorecard to Work", Harvard Business Review Sep - Oct pp2-16.
6. Kaplan R S and Nort'on D P "Using the balanced scorecard as a strategic management system". Harvard Business Review Jan- Feb pp75-85.
7. Kaplan R S and Norton D P "Balanced Scorecard: Translating Strategy into Action" Harvard Business School Press
8. Kaplan. R. S.. & Norton, D.P. Measuring the strategic readiness of intangible assets. Harvard Business Review, 82(2): 52-63.
9. Kaplan. R. S.. & Norton, D. P. Strategy maps: Converting intangible assets into tangible outcomes. Boston: Harvard Business School Press.
10. Kurtzman J "Is your company off course? Now you can find out why", Fortune Feb 17ppl28-30
11. Niven. Paul R. "Balanced Scorecard. Step-by-step. Maximizing Performance and Maintaining Results".
12. Per Nikolaj Bukh & Teemu Malmi "Re-Examining the Cause-and-Effect Principle of the Balanced Scorecard"
13. Norreklit H., The balance on the balanced scorecard - a critical analysis of some of its assumptions. Management Accounting Research, 11, pp. 65-88.
14. Papalexandris. A., Ioannou, G. and Prastacos, G.P. Implementing the Balanced Scorecard in Greece: a software firm's experience. Long Range Planning, 37(4), 347-362.
15. Papalexandris. A., Ioannou, G., Prastacos, G.P. and Soderquist, K.E. An integrated methodology for putting the Balanced Scorecard into action. European Management Journal. 23(2), 214-227.

16. Voelper S.. Leibold M., Eckhoff R., Davenport T., The tyranny of the Balanced Scorecard in the innovation economy, Journal of Intellectual Capital, Vol. 7, n° 1, pp. 43-60.

ALPHABETICAL INDEX OF AUTHORS