NEW DEVELOPMENTS OF MILITARY SCIENCE IN THE INFORMATION AGE

Colonel (ret) Professor Gruia TIMOFTE, PhD

1. The Characterization of the Information Age and the Information Society

There is absolutely no doubt that advanced Information and Communication Technologies (ICT) and the capabilities that they impart will significantly change the nature of military roles, missions, and methods. Change will come not only to the militaries of powerful nation states but to the militaries of smaller states and non-state actors.

The first modern information revolution began in the mid-nineteenth century and extended for approximately 100 years. This first revolution primarily enhanced communications. During this period, technologies such as the telegraph, the telephone, and the radio came of age. These technologies transformed not only humankind's ability to communicate, but also people's lives. Especially in industrial societies, they changed the ways that people related to one another and altered the ways that business, government, and military and foreign policy establishments conducted their affairs. Given the dimensions of their impacts, these technologies also helped modify the structure of the international system. The second modern information revolution extended from the mid-twentieth century until perhaps the 1980s. During this period, technologies such as the television, early generation computers, and satellites linked the world together in ways that it had never been linked before. These technologies, like the telegraph, telephone, and radio before them, again transformed humankind's ability to communicate; changed the ways in which people related to one another; altered the conduct of business and government; and modified the structure of the international system[1].

We are thus on the verge of a third modern information revolution, one that perhaps should be labeled as "knowledge revolution" since it encompasses advances in information technologies that significantly alter the politics, economics, sociology, and culture of knowledge creation and distribution. The most important technologies of the contemporary information revolution are as follows: advanced semiconductors; advanced computers; fiber optics; cellular technology; satellite technology; advanced networking; improved human-computer interaction; and digital transmission and digital compression. As important and significant as the advances in Information Age technologies are, they are not the only technologies rapidly advancing. When they are combined, they promise to provide the military forces that obtain them the ability to engage in warfare, conflicts, and operations other than war in truly revolutionary ways.

An *information society* is a society in which creation, distribution, diffusion, use, integration and manipulation of information is a significant economic, political, and cultural activity. The knowledge economy is its economic counterpart whereby wealth is created through the economic exploitation of understanding. [2].

The International Telecommunication Union (ITU) established a useful conceptual framework to describe the process countries are going through in their evolution towards information societies based on the basic three-stage model: (1) ICT readiness, reflecting the level of networked infrastructure and access to ICT, (2) ICT intensity, reflecting the level of use of ICT in the society, and (3) ICT impact, reflecting the result of efficient and effective ICT use. Also, ITU defined some indicators for the evaluation of the information society development at states, regions and globe levels according to ICT evolution and access to them. These indicators were grouped in 3 categories, as follows [3]:

a. ICT infrastructure and access: fixed telephone lines per 100 inhabitants; mobile cellular telephone subscriptions per 100 inhabitants; international Internet bandwidth (bit/s) per Internet user; proportion of households with a computer; and proportion of households with Internet access at home;

b. ICT use (primarily by individuals, but also households, businesses, others as data become available in the future) and the intensity of use: Internet users per 100 inhabitants; fixed broadband Internet subscribers per 100 inhabitants; and mobile broadband subscriptions per 100 inhabitants;

c. ICT skills (or capacity necessary to use ICT effectively): adult literacy rate; secondary gross enrolment ratio; and tertiary gross enrolment ratio.

Some data regarding the global and regional extension of Internet, up to June 30, 2010, are shown in Table 1 [4].

World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000 - 2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9%	2,357.3%	5.6%
Asia	3,834,792,852	114,304,000	825,094,396	21.5%	621.8%	42.0%
Europe	813,319,511	105,096,093	475,069,448	58.4%	352.0%	24.0%
Middle East	212,336,924	3,284,800	63,240,946	29.8%	1,825.3%	3.2%
North America	344,124,450	108,096,800	266,224,500	77.4%	146.3%	13.5%
Latin America	592,556,972	18,068,919	204,689,836	34.5%	1,032.8%	10.4%
Oceania /Australia	34,700,201	7,620,480	21,263,990	61.3%	179.0%	1.1%
WORLD TOTAL	6,845,609,960	360,985,492	1,966,512,816	28.7%	444.8%	100.0%

Table 1: World Internet Users and Population Statistics

Despite the recent economic downturn, the use of ICT services, such as mobile phones and the Internet, seems to have suffered little from the crisis. This is supported by continuously falling prices of devices such as computers and handsets. The most important data shows that the last decade was characterized by an accelerated development of ICT infrastructure and main data by the middle of 2010 are as follows: a growth of the number of mobile cellular subscriptions, reaching an estimated 4.7 billion and a penetration of 69 per 100 inhabitants globally; 1.3 billion fixed telephone lines and a penetration of 19 per 100 inhabitants; an estimated 28.7 per cent of the world population (or 1.96 billion people) were using the Internet and 65 per cent of them were using broadband connections (at least 256 kbit/s); the fixed and mobile broadband telephony remained at a low level of development (10.0 per cent, respectively 8.0 per cent). Even though economic recovery is now well underway, the recent global economic and financial crisis has not spared the ICT industry. The production of IT-related equipment has experienced reduced demand and investments. There has also been some evidence of reduced investments in planned network upgrades, and the rollout of next generation networks has been delayed or abandoned as a result of financial constraints.

Computing technologies. *Computing* is abroad at the heart of defense with software – intensive procurement running in into billions of dollars in the pipeline. There are hardly aspects of defense that do not now, or will not soon, depend on computing technologies: the collaborative development and maintenance of operational plans; analysis of intelligence data, support to intelligence analysts, and dissemination of intelligence reports; computer-assisted battle management and combat system support in ships, on aircrafts and on the battlefield; control of weapon systems – be they conventional as artillery, or the latest generations of intelligent munitions; the military organizations have a large requirement for business support software for personnel, management, office automation and logistics [5].

Software will become more predictable for a number of reasons: software development processes are maturing; reusable software components are (painfully slowly) becoming a reality; software programmers are becoming better trained and more professional; organizations are starting to apply best practice to software development. Technologies to facilitate better *interaction between computers and humans* are attracting major investment for: new technologies for larger, more portable, less bulky, more robust, lighter, higher resolution, cheaper, less power hungry displays; advanced visualization techniques such as virtual reality; software agent technology to allow more intelligent interfaces and tools for construction of complex internet systems; speech recognition; gesture and facial expression recognition. *Knowledge* is the key to competitive advantage: natural language processing allows computers to analyze the meaning of the text; data mining techniques use advanced analytical algorithms to spot trends and patterns in large data sets; metadata allows the structure of data to be explicit. Future benefits to the military will be ensured by: having superior intelligence information; making better decisions than the opponents; reacting faster; being able to bring overwhelming force to bear; applying force more precisely; communicating our messages more effectively. The application of computing will address the full range of operational processes, including: strategic, operational and tactical planning; strategic and tactical intelligence analysis and dissemination; logistics; command and control; embedded systems in military platforms; smart weapon systems, etc. *Quantum computers* have the potential ability to carry and process large amounts of information in parallel and at very high speeds. For example, computer scientists at the U.S. Defense Advanced Research Projects Agency are asking industry for novel technologies and approaches that offer dramatic advances in *high-performance military computer* performance, and enable so-called extreme scale computing - the notion of exceeding today's peta-scale computing to achieve one quintillion (10^{18}) calculations per second [6]. Also, the computers need to meet the relentlessly increasing demands for greater performance, higher energy efficiency, ease of programmability, dependability, and security in aerospace and defense computing for military sensors, platforms, and missions. Topics of interest in the program include software that not only reduces requirements for high performance computing, including memory and storage, but also that enables programmability to reduce the need for users to understand complex system aspects like heterogeneous cores and memory hierarchy; hardware and software for managing component failure rate, as well as shared information and responsibility among the operating system, runtime system, and applications; scalable input/output systems that may include alternatives to file systems; self-aware system software; programming models that allow developers to express their execution goals for achieving security, dependability, power efficiency and performance; and low-power circuits that can be used across multiple or extreme scale system designs. In Table 2 are presented the main characteristics of the fist 10 super-computers in the world in June 2010 [7].

Rank	**Site**	**Computer/Vendor Year**	**Cores**	**R_{max}**	**R_{peak}**
1	Oak Ridge National Laboratories, USA	Jaguar – Cray XT5-HE, Cray Inc., 2009	224162	$1759x10^{12}$	$2331x10^{12}$
2	National Supercomputing Center, Shenzhen, China	Nebulae-Dawning TC 3600 Blade, Dawning, 2010	120640	$1271x10^{12}$	$2984x10^{12}$
3	DOE/NNSA/LANL, USA	Roadrunner-Blade Center QS22/LS21 Cluster, IBM, 2009	122400	$1042x10^{12}$	$1376x10^{12}$
4	National Institute for Computational Sciences, University of Tennessee, USA	Kraken XT-5, Cray Inc., 2009	98928	$831.7x10^{12}$	$1028x10^{12}$

5	Forschungzentrum Juelich, Germany	JUGENE-Blue Gene/P, IBM, 2009	294912	825.5x10^{12}	1002x10^{12}
6	NASA/Ames Research Center/NAS, USA	Pleiades-ALTIX, SGI, 2010	81920	772.7x10^{12}	973x10^{12}
7	National SuperComputer Center, Tianjin/NUDT, China	Tianhe-1-NUDT TH-1 Cluster, NUDT, 2009	71680	563x10^{12}	1206x10^{12}
8	DOE/NNSA/LLNL, USA	Blue Gene/L-eServer, IBM, 2007	212992	478x10^{12}	596x10^{12}
9	Argonne National Laboratory, USA	Intrepid-Blue Gene, IBM, 2007	163840	458x10^{12}	557x10^{12}
10	Sandia National Laboratory, USA	Red Sky-Sun Blade, Sun Microsystems, 2010	42440	433x10^{12}	579x10^{12}

Table 2: Top 10 List of Super-computers in June 2010

NOTES: 1. R_{max} (maximal performance achieved) and R_{peak} (theoretical peak performance) values are teraflops.
2. Cores – number of processors.

Opinions about an impending "revolution in military affairs" began in the 1980s. However, it was not until "*Operation Desert Storm*" in 1991which put the United States' arsenal of precision weapons on display for Iraq to experience and the world to see that most people realized how far they had come technologically. In the months and years after *"Desert Storm",* discussion, analysis, and speculation about the implications of Information Age technologies for warfare and conflict multiplied. Quickly, military scholars, analysts, and planners acknowledged that the implications of the new technologies for national security and defense policy extended far beyond precision force. As a result, the defense doctrine began to be altered to take account of impending capabilities. Meanwhile fears multiplied about the threats of information and infrastructure warfare as more and more people admitted that Information Age technologies provided not only new capabilities but also created new vulnerabilities.

2. Information Age Influences in Military Domain

Most analysts identify the consequences of the Information Age that will have profound effects on militaries such as: time and distance will become less important as constraints; more international actors will affect events; boundaries between international actors will become more permeable; democratic governments and free market economies will flourish, but will not become the only forms of government or economic organization; trends toward regionalization and globalization will accelerate; the disparity between haves and have-nots will increase; challenges and threats to national security may come from more diffuse sources and that asymmetric warfare presents a real—although not new—security danger; strategy, operational art and tactics will change; as important as Information Age technologies are in inducing change, they are not the only technologies that are experiencing sizeable advances. Thus, the real revolution in military affairs may well arrive when advanced information and communication technologies are combined with the many other technologies that are advancing rapidly and which have military applications.

The opportunities that advanced information and communication technologies – that are Information Age technologies – provide for the militaries improve the way they organize, equip and fight. Specifically, we are talking about sensors, radar, and other information collection devices that are being improved on an almost daily basis. These improved collectors are increasingly capable of being networked together to provide military commanders with an enhanced awareness of the battle space including Global Positioning Systems allowing even individual soldiers to know precisely where they are. And we are talking about the following components [8]:

•Highly reliable high-speed global communication systems that provide the opportunity to communicate this enhanced battle space awareness to any point on the planet where it is needed;

•Advanced information and communication technologies are the basis for precision strike capabilities that improve lethality while minimizing collateral damage;

•Once a strike of any kind is delivered, Information Age technologies provide the ability for better battle space damage assessment, which increases both effectiveness and efficiency;

•Greatly increased needs of "Information Operations" that can protect own information and destroy an enemy's information;

•Define and re-define the "new terms" used in the literature including: "system of systems," "information operations," "information superiority," "information warfare," "network-centric warfare," and "the revolution in military affairs";

•Ensure information superiority as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

In addition to the changes that the Information Age is inducing in individual human endeavors and undertakings, it is also altering the global international system, the structure of the system, and the way that the system works. As a result, the strategic environment within which defense policy will be pursued will change, perhaps drastically. These changes will have sizeable implications for defense policy.

a. Time and distance will constrain less than in the past. One of the chief hallmarks of the Information Age is that the relevance of time and distance as constraints on human activity and productivity will be sharply reduced. With more and more types of messages and information traveling at the speed of light over long distances with little or no loss of clarity, accuracy, or meaning, time and distance are becoming less and less restrictive on many forms of human activities and capabilities. The implications of this for defense policy are contradictory. On the one hand, as bandwidth and reliability increase and it becomes increasingly possible to flash information about developing situations in real time from the point of contact to a command authority, it could mean that command and control become increasingly centralized. This may be especially true in highly sensitive situations. Conversely, the flood of information that increased bandwidth and reliability will provide to command authorities may dictate that more and more decisions be made on the ground at points of contact. The combination of more information available at the tactical level and too much information at the operational level may thus drive more decision making to the tactical level. Hierarchy will remain, but it is likely that the number of levels between top and the bottom will decrease.

b. More international actors will have the ability to affect events. The strategic environment of the Information Age will also be changed by a proliferation of international actors that could play a major role in affecting events. Many factors contribute to this phenomenon, but Information Age technologies are among the most prominent. The proliferation of potentially prominent international actors takes place in two ways. First, advanced information technologies expand the role that multinational corporations, non-governmental organizations, and even individuals play in the international arena. Second, as Information Age technologies permeate human affairs more and more - widely, more and more businesses, non-governmental organizations, and individuals are empowered to involve themselves in the international arena in meaningful ways. As more and more actors gain potential to have major impacts on the national interests of a state, a state's command authority will not be able to identify those actors who present a serious threat to its interests.

c. Information flows ignore national boundaries. The nature of modern networked systems and other information and communications technologies is such that the flow of information can be curtailed only with great difficulty, and sometimes not at all. This reality is a two-edged sword. On the one hand, it means that all types of intercourse between international actors will increase. Conversely, it also means that information some deem unacceptable or unfavorable can spread easily. The permeability of national boundaries also means that the disruption or corruption of information flows can spread widely and rapidly, at global level. In the globally networked environment of the Information Age, the increased permeability of the boundaries among international actors requires information security measures that are reliable, discriminating, rapid, and effective.

d. Democratic states and free markets economies will flourish. Although claims that the Information Age favors democratic forms of government and free market styles of economic organization often go beyond what documented evidence supports, there is logic to the argument that the free flow of information enhances human freedom and productivity. It is likely, then, that the most successful international actors of the Information Age will be democratic states with market economies. But not all states or other international actors will be democratic or market-oriented. Some states and, on occasions, other international actors as well, will attempt to restrict, deny, or otherwise curtail access to information technologies and the capabilities that they afford, arguing that they are protecting traditional values, defending national security, promoting morality, or preventing subversion.

In addition, isolated outposts of like-minded individuals and groups who oppose democracy and free markets may use Information Age technologies to band together to further their own purposes. Democratic states and free market economies may flourish in the Information Age, but new challenges and threats will arise, and many traditional challenges and threats will remain and perhaps grow.

e. The trend toward regionalization and globalization will accelerate. The ability to transfer information regionally and globally at a moment's notice will accelerate the drive toward regionalization and globalization. The rapid transfer of information enables the creation of distributed production systems that extend beyond localities and states to entire regions and even the world, thereby, at least in theory, driving down production costs as businesses take advantage of lower production costs that exist beyond local or national boundaries. As the economies and other interests of states become increasingly intertwined, so too will their defense policies. In some instances, this will present no real problems politically or operationally. Economic integration has important effects in military domain growing the technological and military gap among the different states.

f. The disparity between haves and have-nots will increase. As those who know how to use advanced information technologies within both advanced and developing countries employ those technologies, their wealth will accumulate more rapidly than the wealth of those who are technologically incapable. This phenomenon will occur both within and between countries. Thus, disparities in the distribution of wealth between have and have-not countries may be expected to increase as well, at least during the early years of the Information Age. If the gap between rich and poor increases, resentment of the poor against the wealthy may increase, leading to unrest within states and tension between states.

g. More actors as challengers and threats. One of the hallmarks of the Information Age will be increasingly available and increasingly affordable information and information technology. In some cases, information and information technology will be applied to existing weapons and weapon systems to enhance their capabilities ("information enhanced weapons"). In other cases, information and information technology will become so central to the functioning of a weapon or a weapon system that the weapon or weapon system will not be able to function in its absence ("information enabled weapons"). In still other cases, the increased reliance of civil societies on information and information technologies will render them vulnerable to attacks against its information and information technologies by new and innovative weapons ("information warfare"). What is more, advances and breakthroughs in information and communication technologies can often readily be achieved by small teams of researchers, or even individuals. Sometimes, advances and breakthroughs may be achieved using relatively inexpensive "off-the-shelf" technology available from commercial vendors. In both cases, advances and breakthroughs can sometimes be translated by potential enemies into challenges or threats.

h. Asymmetric warfare as a threat. Asymmetric warfare is the "enfant terrible" of the early 21st century. Most often defined as warfare in which an enemy resorts to the use of weapons of mass destruction, terrorism, urban or guerrilla warfare, or information warfare, the dangers of asymmetric warfare are real and should not be minimized. At the same time, asymmetric warfare is not something new or revolutionary. Military strategy in the Information Age will be no different, regardless if it is employed by "peer competitors" that are major state actors, "niche competitors" that are small state actors or non-state actors, or any of a variety of lesser challenges that may spring up.

i. Defense policy and technological advances in fields beyond information technology. As important and significant as the advances in Information Age technologies are, they are not the only technologies rapidly advancing. Other "high tech" fields also experience rapid advances, and many have extensive implications for the defense policy. Impressive advances are made in technologies such as directed energy, stealth, robotics, miniaturization, micro-electro-mechanical systems, biotechnology and bioengineering, molecular biology, artificial intelligence, non-lethal weapons, non-human behavioral modification, materials, and nanotechnology. Individually, several of these technologies have extensive military utility and implications. When they are combined, they promise to provide the military forces that obtain them the ability to engage in warfare, conflicts, and operations other than war in truly revolutionary ways. All these modern technologies will transform the defense capabilities and defense policy when combined with those of the information revolution.

3. Information Characteristics of the 21st Century Conflicts

The importance of advanced information/knowledge and communications technologies for national security is not, however, just about new technologies for the military. It is about how these technologies will alter military strategy, operational concepts, organizational and command structures, doctrine and tactics. It is about all of the elements of a mission capability package—those things needed to turn a concept into a real operational capability.

A. Impacts of Information Age Technologies. Clearly, these new and emerging technologies will enhance humankind's ability to communicate, to create and utilize information, and to overcome obstacles associated with distance, time, location, and even language. To understand the future, one needs to develop at least a broad conceptual understanding of the nature of the impacts that these technologies are likely to have. The impacts that these technologies are projected to have can be grouped into the following four areas [9].

First, the speed at which information can be transmitted, managed, manipulated, and interpreted will increase significantly. Information flows within and between organizations and among organizations and international actors will also accelerate, although at differing rates depending upon a host of factors. The increased speed of information flow will increase the tempo of interactions within and between international actors.

Second, the capacity to transmit information will also increase significantly. Again, increased capacity will become available at different rates to different international actors. As with increased speed, greater information and communication capacity will benefit some organizations and international actors more than others.

Third, Information Age technologies will enhance the flexibility of information flows. Those needing information will be able to reach out and get it from more sources. Those needing to communicate with someone will find it ever more easily to do so quickly and directly. This greater flexibility will be available to some more quickly than to others, will matter more for some than for others, and will be embraced more quickly by some than by others.

Fourth, these technologies will provide more and more individuals greater access to more and more people, organizations, and information than ever before. This, some observers have argued, will lead to the democratization of information and communication flows throughout the world, that is, a decreased ability of a few (e.g. governments, businesses, and the other "haves") to dominate information and communication channels. This will free information from the hierarchy, or in the case of the military, from the chain of command. None of these anticipated impacts means that the time, distance, or location no longer matter—they still do. This will lead to different types and rates of change in different international actors. Factors that will influence the way and rate in which advanced technologies will be absorbed, diffused, and made operational include, but are not limited to: purchase and upkeep cost; age and utility of in-place technology; an actor's social and cultural receptivity to new technology; degree of insularity within an actor; level and reliability of an actor's human, technical, and economic support infrastructures; level and strength of traditional values and outlooks within an actor; levels of concern over sovereignty on the part of states, and over control of decision-making processes on the part of the actors; and many political, social, and economic factors idiosyncratic to each actor and therefore impossible to detail. Despite these constraints on adoption, Information Age technologies are indeed lessening the role that time, distance, and location play in human interactions.

B. Diffusion of Information Age Technologies. It is widely admitted that advances in information and communication technologies occurr incredibly rapidly. As important as the advances themselves are, however, three aspects of their diffusion require additional comment; diffusion is rapid, global, and uneven. It seems reasonable to assert that the future of organizations, industries, and even societies will depend, to some significant extent, upon their ability to harness information to create and maintain a competitive advantage in the domain in which they operate. Clearly, regardless of whether the technology under examination is personal computers, cellular phones, satellite broadcasts, or the Internet, diffusion proceeds rapidly. The three dimensions of diffusion—rapidity, globality, and unevenness—viewed together with the impacts of new and emerging information and communication technologies, have immense implications on national security, both in the context of enhanced military capabilities and in the context of a changed strategic environment. The first point that must be made is that, because of their relatively inexpensive cost and widespread availability, Information Age technologies will provide even the poorest states and global or regional actors with significant capability that may be used to challenge or threaten others. For example, they enhance an actor's ability to command, control, and communicate with its armed forces at the tactical, operational, and strategic levels.

Information Age technologies require a new way of doing business if military organizations are to fully reap their benefits. These include new concepts of operation, organization, approaches to command and control, doctrine and a redesign of combat support. Organizationally, the capabilities afforded by Information Age technologies tend to be put to best use by networked organizations in which decision nodes can interact with other decision nodes directly, rather than strictly follow a hierarchical protocol which requires decision at every level before action is taken. Nevertheless, in many cases, particularly when they are required to respond quickly to rapid information flows, a network-centric approach could be better. Thus, the organizational challenges presented by the capabilities provided by Information Age technologies will revolve around how best to meld traditional hierarchical structures required for some tasks with new networked structures required for other tasks.

Domestically, Information Age technologies help to create a state's—and other actors'—domestic political, economic, and military, capabilities. At state level, these are important components of the national security equation since every state, if it is to survive and prosper, must base a substantial portion of its national security policy upon its domestic capabilities.

Internationally, Information Age technologies extend the global knowledge and global reach of governments, businesses, militaries, and other international organizations and actors. They enable these actors to disseminate information (or disinformation). At international level, these technologies thus help establish both the international system in which a state must pursue its national security objectives and the international norms which help influence, and in some cases determine, what is and is not acceptable international behavior. They may also provide new capabilities to some international actors that can substantially increase the importance of non-state actors.

C. The main factors that influence information age conflicts. The analysis states from 5 theorems as follows [10]:

▪Information superiority as key to success in the new operating environment;

▪Asymmetrical credibility as key power resource;

▪Traditional boundaries blur in the Information Age (between states, military-politics, and military-civilian);

▪Networks versus hierarchies: from centralized hierarchical to decentralized flat organizations;

▪Asymmetry versus Doctrine of Dominance: small players harm the powerful easily.

● **Asymmetric credibility.** In today's information-saturated world, attention is an increasingly scarce resource and among actors struggling to accumulate information power, (asymmetrical) credibility or the reputation for providing correct information is crucial. The struggle for a high level of credibility therefore becomes an essential part of any political or military operation, aggravated by the skill revolution that lets the populace exert pressure on the decision-makers if their credibility seems questionable. This not only might result in loss of control over the situation, but also significantly reduce the overall success of operations.

● **Technology, terrain, weather, international law.** Prediction is a direct connection between case specific influencing factors like weather, terrain, and, for example, technological failures and the degree of satisfactory conduct of operations, because such factors directly hamper these. The same principles of the traditional law of armed conflict applied to bombs and missiles must also apply to a military cyber attack: such assaults aimed at civilian targets like financial systems, power and water facilities, could constitute a war crime. In the case of attacks involving foreign governments and major foreign movements or terrorists and extremists, it is not clear what laws apply, what constitutes an attack of war, and what kind of counterattack or offensive operation is justified. There are also many more ambiguous legal parameters involved, such as the fact that the role of third nations or "neutrals" in preventing the use of their cyber facilities and information systems is not clear.

● **Asymmetrical challenge.** In the Information Age, small players increasingly have the ability to harm powerful foes with the right technology and knowledge. Aggressors are left with two options: they can pursue indirect or camouflaged aggression, or they can attempt to deter or counter asymmetrically. For example, there is no need of military power if private entities can effectively penetrate the adversary's decision-making cycle by using new media and tools. Another asymmetrical tool is the use of the cellular phone and the Internet. The degree of multiplication of actors is generally low: in conflicts, much of the traditional information monopoly still rests with the major conflict parties. The Internet challenges this information monopoly in some ways, but is too diverse to have a major impact.

● **Blurring the boundaries between the military and politics.** If the higher the degree of blurring boundaries between military and political domains faced by a conflict party the lower the level of successful conduct of operations by this conflict party, then we can assume that the more political parties influence military parties due to domestic pressure, the less successful the outcome. A solution to overcome the reluctance of modern democracies to go to war seems to be the promise of "zero-death" conflicts. The war, in many aspects, is a virtual war, automated and remote controlled, a "war-at-a-distance", without physical contact, a purely technological event, taking place behind radar and computer screens, with no casualties. Today, the enormous volumes of information can only be mastered by total dependence on and trust in technical aids to help organize and manage it. This reliance on computers has generally eroded manual skills to analyze and understand certain occurrences, or to distinguish between reliable and false information. Even more, the stream of electronic input can overwhelm the human ability to make decisions.

● **Multiplication of influential actors.** The more influential and relevant actors a conflict party has to deal with and the more these non-traditional actors have the ability to intervene against the wishes of the party, the lower the level of successful conduct of operations by this conflict party. It is necessary to redistribute power among the actors on the international stage that destabilizes traditional structures of authority, empowering small entities as well as individuals, with a multiplication of relevant actors and a growing complexity of the operating environment. The Internet challenges this information monopoly in some ways, but is too diverse to have a major impact. Generally, two categories of usage could be distinguished: the "peaceful" online collection and dissemination of information that is considered to enhance democracy, and the aggressive use of the Internet, in some of its facets called cyber-war, to potentially harm the adversary.

● **Blurring the boundaries between the military and politics.** The blurring of boundaries between military and political responsibilities in the context of coalition warfare makes struggles between the two factions inevitable. The high-tech conflicts that are promoted to be risk-free and casualty-averse seem to guarantee support of the democratic electorates at least as long as such an illusion can be maintained.

● **Blurring the boundaries between the battlefield and the civilian realm.** The higher the degree of blurring boundaries between the military and the civilian domains caused by a conflict party the lower the level of successful conduct of operations. Targets may exist in the physical space, in cyberspace, or be the human perception, with the objective of influencing this perception to affect decisions and resulting activities. In the new notion of "neocortical" warfare military power uses language, images, and information to assault the mind, hurt morale, and change the will. But not only decision-makers, policy-makers, and military commanders are the targets of these assaults, today, even entire populations might be subject to such attacks.

● **Information operations decisive in Information Age conflicts.** The last of the relationships is concerned with testing the relationship stating that there is a connection between the conduct of operations and the level of success in Information Age conflicts, by claiming that the higher degree of successful conduct of operations.

4. New Operational Concepts

a. Network-Centric Warfare. "Network-Centric Warfare" (NCW) represents the beginning of Information Age concepts because at its core lies the idea of building an information infrastructure, linking platforms and command structures together in ways that permit rapid information sharing. NCW is 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. The information network will enable individual platforms to become greater than the sum of their parts since they will develop the synergy that comes from cohesive action and will do so with greater efficiency. Receiving the right information in a timely manner should allow "sensor-shooter-supplier" linkages to become faster and should enable a smaller number of platforms to accomplish a greater number of missions. Additionally, some valuable synergy could result from rapid, secure, and accurate information sharing, not only among the various combat systems of each service, but also between combat and logistics systems and organizations. In short, NCW can provide a more comprehensive operational picture, an improved situational awareness, faster response times, and a more efficient concentration of effects [11].

b. Rapid Decisive Operations. RDO represents an effort to make the following concepts operational: dominant maneuver, precision engagement, focused logistics, full-dimensional protection. As such, it serves as an umbrella concept under which other ideas, such as Effects-Based Operations, have emerged. In brief, the central idea of RDO is to leverage information and networks to conduct operations that are both quick and decisive. RDO is a *knowledge-based* concept that *describes* how to achieve rapid victory by attacking the *coherence* of an enemy's ability to fight. It is the synchronous application of the *full range of national capabilities* by a fully networked and coherent joint force in timely and direct *effects-based operations* against the adversary as a *system of systems*. RDO attempts to combine two properties – speed and decisiveness – into a single operational concept. To achieve *speed*, for instance, RDO must have: information superiority; an in-depth operational net assessment of the adversary; advanced planning; a standing joint force headquarters; forward presence forces; aggressive offensive information operations; and greater standoff-engagement capabilities. Similarly, to achieve *decisiveness*, RDO requires: precise identification of key links, nodes, centers of gravity, and critical vulnerabilities; an exploitation of the immutable relationship between intelligence, maneuver, and fires; relentless application of overwhelming firepower; denial or destruction of an adversary's most dangerous war-fighting and war-making capabilities; and rapid strategic deployment and support.

c. Effects-Based Operations. EBO is defined as "actions that change the state of a system to power." It is an approach to military operations that attempts to focus political and military decision-making on identifying desired effects and selecting the tools that can best achieve them. It is an attempt to move away from the traditional method of attacking and neutralizing or destroying an opponent's "capabilities" and measuring progress by a calculus of attrition or by the movement of lines on a map.

In essence, EBO is a method of planning that reduces an adversary to a number of targets that must be "serviced" in ways that, collectively or individually, appear likely to achieve the desired effect.

d. Operational Net Assessment (ONA). ONA is defined as a continuous, collaborative process that builds a common, coherent knowledge base. It links together various knowledge sources to develop a common understanding of friendly forces, opposing forces, opponent perceptions, and the operational environment. ONA provides the knowledge basis for EBO. It is not intended to be a static product, but a dynamic source of operational understanding that encompasses the enemy's war-fighting system as well as his political, economic, cultural, diplomatic, and informational systems. Recent experimentation with the concept has produced the following tentative insights concerning the value of ONA: it can become the key enabler of EBO; it complements and is complemented by joint intelligence preparation of the battle space; it is operationally feasible to examine the enemy as a system of systems; it can enable greater simultaneity in planning and decision-making; it resembles a collaborative process more than a tool; the process still requires "refinement" in terms of turning information into operational knowledge.

There are many other concepts which have new characteristics in the Information Age such as asymmetric warfare, parallel warfare, irregular warfare, hybrid warfare, compound warfare, counter-terror warfare, information warfare, cyberspace warfare, full-spectrum dominance, information and decision dominance, etc.

5. Conclusions

Information Age Technologies have an important impact on military science and its components. Therefore, military theorists, researchers and planners have to study all these developments and elaborate new concepts, procedures and methods of action in military science and military art. Also, the conclusions must be analyzed in a large context as well as DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability).

REFERENCES

[1] Alberts David S., Papp Daniel S. *The Information Age: An Anthology on Its Impact and Consequences*. Washington, D.C., USA: CCRP Publication Series. 1997. p. 14.

[2] http://www.wikipedia.org/Information_society

[3] International Telecommunication Union. *Measuring the Information Society*. Geneva, Switzerland. 2009. pp.15-17.

[4] Nielsen/NetRatings and International Telecommunication Union, http://www.internetworldstats.com/stats.htm

[5] Ministry of Defence: *Computing Technologies for Defence*. London. 2006. pp.4-7.

[6] Keller John. "DARPA pushes new frontier of high-performance military computing to approach performance of one-quintillion calculation per second." *Military & Aerospace Electronics*. June 2010. Virginia, USA.

[7] http://www.top500.org/lists/06/TOP10_June2010.pdf

[8] Alberts David S., Papp Daniel S. *Information Age Anthology: The Information Age Military*, Volume III. Washington, D.C., USA: CCRP Publication Series. 2001. pp.4-6, 14-25.

[9] Alberts David S., Papp Daniel S. *Information Age Anthology: National Security Implications of the Information Age*, Volume II. Washington, D.C., USA: CCRP Publication Series. 2000. pp.20-23, 30-38.

[10] Dunn M. *Information Age Conflicts: A Study of the Information Revolution and a Changing Environment*. Zurich, Switzerland: ETH. 2002. pp.85-86, 187-188, 208-209.

[11] Echevarria Antulio J. II. *The Interoperability of Future Operational Concepts of NATO Forces*. Carlisle, Pennsylvania, USA: U.S. Army War College. 2008. pp.23-38, 55-58.