INFORMATION RISKS, THREATS AND VULNERABILITIES AGAINST MILITARY FIELD. TENDENCIES AND DIRECTIONS OF DEFENCE POLICIES IN THE INFORMATION ERA

Col. Dumitru NEACŞU[*], Ph.D. Candidate
M.U. 02472, Bucharest

The development of operational capabilities in the intelligence field represents a permanent concern in modern armed forces. The technological progress in this field has determined the achievement of new means, methods and procedures for collecting, processing, analysis and dissemination of intelligence in the space of interest.

Of these, Space Reconnaissance together with IMINT and SIGINT represent important components in the intelligence architecture at a national or alliance level.

The intelligence risks, threats and vulnerabilities are based on a series of reasons that should not be overlooked in order to establish the necessary protection measures.

Modern armed forces have as a primordial objective supremacy in the intelligence battle of present strategies and visions for development. The basis to win this battle is represented by the successful implementation of intelligence technology in the integrated battle field as well as the protection of these systems and technologies.

Keywords: information system; Space Reconnaissance;Management and Tehnical Collection; Information Methods and Procedures; Risks, Threats and Vulnerabilities; Information Revolution; Infomation Vision.

According to information technologies, the global information medium has two distinct poles: USA (with a considerable technological advance) and other important actors (with some advances in some domains): Russia and China and lately: France, Israel and a consortium of some European states[1]. The previous hypothesis is based on the fact that the current information

[*] e-mail: *neacsu_dumitru_army@yahoo.co.uk*

[1] Space reconnaissance and the management of technical collection, http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-15.pdf

technology is most advanced in programs like: Space Reconnaissance and Management of Technical Collection, where USA is the most technological advanced state, having an important technological advantage, but more important, unique operational capabilities which are hard to challenge on short and medium period.

Moreover, Russia and China are still having difficulties with these advanced programs, because of the profound internal transformations after the fall of the USSR in Russia's case and because of the insufficient level of development in these domains in China's case. The other states, new entered in the exclusivist club of entities capable of space collection have more modest concepts, probably because of the lack of financial possibilities to sustain such systems.

Starting from these hypotheses and taking into account the information capabilities of medium and above medium developed states, we can observe that most of them have specialized services on internal and external areas of interest, military and other form useful for information assurance of internal services. Moreover, where space collection capabilities are present, they are under military control. There are two organizations in the Department of Defense of USA:

1. US Space Command (SPACECOM), which supervises the so called "white world satellites" – satellites made public as being part of military programs;
2. National Reconnaissance Office (NRO), which supervises the so called "black world satellites" – intelligence satellites[2].

The new advanced technologies in domains like IMINT (Imagery Intelligence) and SIGINT (Signals Intelligence) greatly impacted the current concepts and notions on which the information systems implementation and development are based. All these implies the jump to new technological levels in IMINT domain for caption, transmission and data base creation for video images and platforms (satellites, manned or unmanned aerial, terrestrial, maritime and sub maritime systems); on the same note, SIGINT has an explosive evolution in communication means, sensors, collection and data base creation and platforms.

The impact of technological development on the concepts evolution regarding information are so important that it generated changes in the information structure and architecture, both in agencies organization and its responsibilities and competencies. At the extreme, there has been created new agencies with the goal to satisfy some specific requirements. Examples of

[2] Space reconnaissance and the management of technical collection, http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-15.pdf

such impact are: SIGINT management generated both more responsibilities for Defense Intelligence Agency (DIA), taken from CIA and the creation of National Intelligence Agency (NSA) [3]. According to the official data, NSA is a specialized stand alone agency, responsible for SIGINT collection, data processing and products dissemination to US agencies interested in such products. NSA's exceptional performances proved both the efficiency of the intelligence agency and the fact that the concept is operational and defined NSA as the main source of SIGINT intelligence for the other information systems and as the domain management coordinator in National Intelligence Community (NIC).

Moreover, NSA is today the interface between the commercial sector and Department of Defense in communication technology domain. Practically, all research and development activities in this domain are duplicated inside NSA for SIGINT technology creation. This type and level of influence of the information is not specific only to the national programs of USA. Information technology development has a similar impact in all the states involved in such programs. The result is reflected not only on the information architecture and operation procedures inside the Information Communities, but also on every member, both on his capabilities and on his profile as an adaptation to the system requirements.

The requirements complexity of different intelligence products based on the exploit of information technologies and on the huge and very specialized volume of information created by technical collection created the need for several concepts of distinct structure on domains and sub domains, regarding the responsibilities for collection and production, in accordance with a coherent management of the information collected and available for processing. The most technological advanced states divided SIGINT in: COMINT (Communication Intelligence) and ELINT (Electronic Intelligence). ELINT has three sub domains: FISINT (Foreign Instrumentation Signals Intelligence), TELINT (Telemetry Intelligence) and RADINT[4] (Radar Intelligence).

The same way and based on the influence of the technological development, MASINT (Measurement and Signature Intelligence) divided its responsibilities in subdivisions according to the collection and processing domain: ACINT (Acoustical Intelligence), OPTINT (Optical Intelligence), ELECTRO-OPTICAL (Electro-Optical Intelligence), IRINT (Infrared Intelligence), LASINT (Laser Intelligence), NUCINT (Nuclear Intelligence) and RINT[5] (Unintentional Radiation Intelligence).

---

[3] *Idem*.
[4] Gary H. Mills, SHAPE Senior analyst, *The role of rhetorical theory in military analysis*, 2003, p. 16.
[5] *Idem*.

We may say that, if during the 70s and 80s, the commercial producers efforts were to answer the visions and dalliances of the information market, nowadays, these entities only produce new and more performing products for concepts developed at the beginning of the 90s, increase the collection, processing and archiving capabilities, making more efficient the concepts on which the whole specter of information interest is based.

Information risks, threats and vulnerabilities in military domain

Information risks, threats and vulnerabilities are based on the following considerations:

- permanent confrontation in order to obtain and keep information domination, supremacy and superiority;
- increased dependency on information systems and technologies, on technical equipments and embedded software;
- new technologies and capabilities, which will provide significant advantages to modern armed forces, are sold everywhere and may be bought by groups which can threat security and stability;
- modern collection equipments high level of connectivity with the information and decision networks generates the need for specific measures to protect and maintain the operability status of military systems and ensure the management continuity, secret actions, information unity (to ensure unitary and homogenous information coordination and execution links), behavior and adjustments functional flexibility (to avoid functional discontinuities and ensure its dynamic, self regulation, adaptability, viability and systemic coherence);
- changes of the global information medium, its structure and its environment will determine dramatic mutations in the strategic domain;
- information technologies extend the place and role of multinational corporations, NGOs and international VIPs who can play important roles in influencing the events;
- new technologies enter more and more in business domain, having an important impact on defense policies (the wider the series of potential factors which may drastically influence specific national interests the more difficult the identification of potential serious threats for the decision makers);
- modern systems interconnection and information technology and communication progress cause, in some cases, high difficulties in avoiding information floods;
- information considered unacceptable or undesirable may be disseminated very easy, information which serves specific interest groups and may impact national security;

- information technology and communications studies and researches can be conducted by small teams and even individuals;
- transformation by a potential adversary of commercial means in true "weapons" for provocation and threats proliferation;
- different options available due to the information and communications technology allow many actors, including non-state ones, to have access to tools which can be used for threats and provocations development (cyber war, hackers war or cyber terrorism);
- ignoring the borders and constraints generated by space or time;
- increased vulnerability for information technologies and systems and for technical equipments and embedded software due to unauthorized access, accidental or planned destruction and alteration of data and software. The current tendency is represented by the extension of connectivity, especially to Internet and Intranet networks, making more and more difficult illegal access points identification or aggressive behavior users. This type of vulnerability can generate huge damages, directly or indirectly, as a result of information "leaks" of both personal and economic or military data;
- there are many vulnerable targets in technical-military domain, which can be accessed quickly and widely and which generates the need for more protection measures;
- information era characteristic is not only the information quantity or technology proliferation but also its rhythm and dimension.

Basically, any state or NGO with hostile intentions can access technology needed to threat a military information system. Due to the low cost of the necessary equipments needed for an information attack, compared with the costs of a protected information system and to the fact that many knowledge are available on Internet, threats may come even from NGOs, terrorist groups or civilian hackers.

Threat to information security approach implies the consideration of the fact that vulnerability does exist during all stages of its organization and its representation must be used when ensuring its protection. In conclusion, there's no clear distinction between information and the medium where/through it resides/flows, from information security point of view[6].

Threat to information implies threats to the medium where this information resides or to the communication channel through which it flows. Information protection implies different security measures than those needed for electronic memories and communication channels.

[6] Ion Roceanu, Iulian Buga, *Information, conceptual landmark and security coordinates*, AISM Publishing House, Bucharest, 2003, p. 59.

Compared with the traditional threats to military organization components we may observe an increased share of those associated with computers and computer networks in the case of military information systems. This share may be explained by the systemic integration role played by the computers subsystem and by the fact that the communication subsystem is based on computers. In the same time, we may notice that both principal hardware (workstations, network cables etc.) and software components (operation systems) in use were developed by civilian companies, which generates security concerns: many of them are available to anybody on the market, including their technical specifications. Dedicated military components, developed, produced and supervised in secure conditions are victims of industrial espionage, common characteristics of a free high technology market. It is more difficult to adapt these components to the evolving requirements and they may contain imported components or products verified outside the military sphere which can be altered intentionally through very well concealed processes. All military information systems were developed based on a logic component – software – which can be attacked with similar logic means, using cheap technologies which is developed and diversified permanently including by international criminal actors. Therefore, results of the civilian systems vulnerability study may apply to the military ones.

Specific threats for military information system, especially at the operative and strategic level, are influenced by the dependence of the communications and computers subsystem on national information infrastructure. Military related information presence in civilian mediums offers opportunities for potential adversaries to exploit uncontrolled sources.

The origin of system dangers that can become threats is diverse. Information threats may have different motivations, based on: politico-military objectives, revenge, economic gain, identity theft, blackmail and intellectual provocation.

According to specific publications, threat sources are classified by some criteria:

- *behavior:* manifested or open: direct (hacking) and indirect vandalism acts (malware), radio and radioreley, radiolocation and radio navigation jamming, SIGINT activities, electromagnetic pulse, special operations; under covered, disguised or conspired: espionage, sabotage and subversive acts, terrorist actions, criminal activities; by accident and natural;
- *origin:* internal, external or from the medium.

For the information operations, vulnerability represents a weakness, both in system projection from the information security point of view and as a consequence of inefficient internal control and security measurements implementation. These situations can be exploited to obtain unauthorized access to data and information or to the informational system.

For the communications and IT systems, vulnerability represents a point where the system may be attacked. The confrontation to obtain and keep information domination, supremacy and superiority as well as dependence on information systems and technologies and technical equipments and embedded software have generated risks, threats and vulnerabilities which must be countered with specific measures, in the context of the new *revolution in military business* and *network centric warfare*.

Tendencies and guidelines regarding informational medium evolution in the information era

The effect of the ongoing information revolution, *both in social and military domain* is monitored closely by the military strategic specialists, most of them agreeing on the effects of information revolution as a factor which will profound modify our society, democracy and our daily lives[7]. These technologies will constitute the means to increase the military efficiency and reduce the losses, both in blood and money. There is an essential need for a unified social and military perspective on the military structure and future developments options and directions.

The main effects of the information era on social medium, especially on military domain, are: time and distance become less important as a constraint; events may be influenced by many transnational and international factors; international borders become less significant; regionalization and globalization tendencies will be on an ascending trend; there will be a bigger gap between rich and poor; threats may be the result of multiple sources and asymmetric warfare will be a real danger; there will be significant mutations in strategies and tactics in order to be continuously adapted to the battle environment; real revolution in military domain will be realized using a mix of information technology and communications and military applicable technologies.

Opportunities offered by information technology and communications to the military domain are developed taking into account the provision of a better planning and lead of the modern warfare. It is about information systems offered by the integration of sensors, radars and other collecting equipments which are continuously developing. These equipments are more

[7] Z.K. Halilzad, J.P. White, A.W. Marshall, *Strategic appraisal. The changing role of information in warfare*, Rand, Santa Monica, California, 2001, pp. 26-32.

and more connected with information networks in order to ensure a better visualization of the battle space, including the location of every soldier and mechanized vehicle:

- global communication system with increased transmission speed and constancy which help accessing an accurate image of the battle space from any location on the Globe;
- increased high precision fire power which produce significant losses for adversary and diminish the amount of losses in friendly forces;
- possibilities to rigorous analyze the losses of battle space, which increases the efficiency and effectiveness;
- need for a rigorous information actions planning and conducting in order to protect own information and destroy adversary data base;
- ability to define and redefine specific terms like: systems of systems, information operations, information superiority, information warfare, network centric warfare, military revolution;
- ability to ensure information superiority, including: collection, processing and dissemination of a specific intelligence continuous flow and exploit of, or diminish of the adversary forces ability to respond.

Technologic evolution impact does not manifest only in the warfare space but also in *defense policy*, affecting many *directions*:

- information become essential in order to increase wealth, power and influence; information become more important than traditional resources and defense policy must rethink its objective and include actions regarding information defense and protection;
- continuous change of moral and material values, influenced by available information regarding possibility of using the technology to create them;
- information technology produces changes in structure and organization of all social components, including military, information flows providing real time command and control from locations which are independent of distances, platforms and hierarchical level.

Continuous condensation of space and time, especially generated by technologic support and its concepts is not new, previous constraints being dramatically reduced or totally eliminated, in some cases. Different format of information and superior quantitative and qualitative support on different platforms allow direct contact pretty quickly and usually only for remote controlled armament systems, which provide security both for leaders and systems operators.

Border insignificance, including state border is a reality with two sides. Increased international entities interactions which are useful for democracy and economic development is one side of the coin. The other side

comprises unacceptable quick and rapid of unfavorable information availability, which represents a major threat. Borders permeability creates the need for new strategies regarding information control, which can be rapidly change from positive elements to risk threats for owners. Maintaining information security and protection and informatics and communication systems become an important priority for security and defense[8] in information era.

Information technology will encourage *regionalization and globalization tendencies*, rapid information transfer allowing production processes and relation to expand exponentially beyond state or regional borders. The true active factors of regionalization and globalization have the most important technical capabilities.

Economic integration will have a bigger impact in the military domain, generating: interoperability of forces owned by same evolutionist mediums; offer diversification; bigger technological and military gap between different states; access to specific technology, even for elements which uses violence as the principal instrument to attain its goals. Moreover, without global politics to eliminate such *major risk for regional and global equilibriums*, information technology will favor bigger gap between poor and rich spaces, generating an accelerated development of powerful states, increased differences and asymmetric wealth distribution, which inevitably generates internal and external disorders, major disparity and growing international tension between these spaces.

Risks generated by bigger dependence on information technologies and systems, on technical equipments and embedded software become more and more evident, entities with less personnel and using low cost methods being able to generate big losses, including financial, directly or indirectly, through aggressions on information systems, including defense and security ones (C4I, C4ISR, C4RISTA etc.). Current tendencies of interconnectivity, especially to Internet and Intranet networks increase the vulnerabilities due to the fact that it's more difficult to locate an illegal access point in the network or a rogue user.

From *technical-military* point of view, communications and information importance resides in the big number of vulnerable targets, rapidly and diversely accessible, which need protection means and procedures more and more diverse. According to future strategies and development visions, primary objective of modern armies is winning the information battle. Winning the information battle depends both on successful application of information technology in the integrated warfare space and protection of these systems and technologies.

[8] *The Internet and press freedom 2000*, New York, Freedom House, 2000, p. 27.

Information and communications technology has a *major impact* on *military strategy*. The main provocation of our times is not only the information quantity or technology proliferation but also its rhythm and format. World evolution is more efficient, complex and rapid than ever, entities which can adapt to this rhythm being the ones which make profit and dominates any domain, including the military one. There have been identified concerns inside different modern armed forces, solved through improvement of the network operations in all domains, including space[9].

According to different specialists, present and future warfare concept will be dramatically impacted by new technologies, especially in military operations command and control levels. Warfare is combined with a conservative strategic approach in which states, alliances and military structures will remain the most important actors. Armed conflicts will remain political instruments.

Standardized *information domination, supremacy and superiority* will be the key for success in military actions through the capability to control and maintain a more rapid actions rhythm than the adversary, allowing friendly forces to win and maintain initiative during operations[10] and ensuring success and the base for future actions.

Scarcity and disparity of more mobile *forces* and gradually implication in operations is more and more possible using the information technologies, allowing commanders to discover targets and conduct their own actions efficiently and effectively. Technologic and procedure development will continue tendencies of efficient global positioning, increased armament systems targeting, remote action platforms performances.

Confrontation asymmetry represents an important mutation produced in the military action, generated by this explosive technologic evolution, *concept manifested especially in:* utilization of high precision system and munitions or WMD against forces and means of inferior generations; terrorist actions against modern forces in order to weaken public support regarding utilization of military forces; option of quantitative utilization in order to compensate for terrain or urban medium constraints; a network organized adversary has a higher potential than a hierarchical one; cyber war; hackers community; ambiguity generated by actions situated on the border between military and non-military domain, between national and international jurisdiction, between classic warfare and peace.

As part of the society, armed forces need to transform, to remodel according to new requirements that society imposes. Being recognized by its

[9] Teodor Frunzeti, Vladimir Zodian, *World 2011*, political and military enciclopedy (security and strategic studies), Technical-Editorial Army Center Publishing House, Bucharest, 2011, p. 716.
[10] Joint Vision 2020, pp. 61-62.

conservative nature, armed forces oppose innovation – especially when change implies lowering the rank of some components.

Military domain revolution represents, in essence, radical and profound changes, not only in technology domain. There's a need for a radical change of doctrine, review and change of the whole force structure, namely the dimension, composition and number of internal structures[11].

Cold war ended the bipolar era. This aspect, combined with technological evolution constituted the momentum for doctrine remodelation, adapted to new threats and risks, current and predictable in the future. Adversary becomes more invisible and more active, taking different modes of manifestation and existence and attacking in diverse mediums. There's a need for an international security system, where state and individual security plays a central role and represent global problems. There's a need for flexible structures, more mobile and hyper specialized, adaptable both to action requirements and commander conception. Current armed forces relax a rigid command system into one where decision authority is located at a minimum possible level, "a digital force needing a centralized control less rigid, conducting unilinear operations in a rapid rhythm, in pulsatory and complete systems which are not adequate for a rigid, centralized control"[12]. There's a need for these structure to conduct more diversified actions: from food aid to locals after a disaster to training of an allied country in insurgency fight.

Moreover, we must not lose from site the leader's mentality. His intellectual matrice configuration needs a specific training, tailored both for destruction and helping others. Technical advance impact manifests in the fact that *new armed entities* assessed to be used in future military actions will be trained for battle using modern techniques and procedures, with special accent on training in similar conditions as the ones offered by the battle space. These ways, through simulation, commandants may realize an almost real image of stages and actions of the confrontation, in order to understand the critical moments and develop ways to overcome or avoid them in order to achieve final goals. Forces may be verified using sophisticated simulation systems and efficiency control elements related to different scenarios involving adversary actions, terrain constraints, time and season and other indicators which influences or changes the battle space.

Real image of *forces preparation and engagement* is presented in NATO doctrines[13]. These documents presents details regarding: use of force;

---

[11] Ion Bălăceanu (colectiv), *Interaction of strategies in context of the modern armed conflicts*, UNAp Publishing House, Bucharest, 2010, p. 63.

[12] Eugen Bădălan, Teodor Frunzeti, *Asymmetry and Idiosycrasy in the military actions*, Technical-Editorial Army Center Publishing House, Bucharest, 2004, p. 95.

[13] AJP-01 (B), *Allied Joint Doctrine*, NATO HQ, Brussels, 2001, pp. 3-12.

rules and procedure of engagement; importance of the theatre of operations culture and customs; basic and fundamental language and key expressions; importance of check points and blocking of operational routes; patrol actions, observation and reporting; search and rescue equipments and personnel; EOD tactics and techniques; mine finding and neutralization; equipment, technical equipments and warfare means identification; NBC protection procedures.

Information revolution *major result in military domain* is represented by the vision of informational warfare – a warfare which is using information as weapons and being the main target of the aggressive actions, in the same time. The possibility that this may become the main dimension of future warfare is more and more obvious, sustained by the following: possible military advantages through information utilization as a weapon against adversary targets – mental, weapons systems, support; vulnerabilities of both communications, economic and commercial and logistics and command infrastructures to hostile actions utilizing information technology and specific doctrines.

In conclusion, implementation of new IMINT, SIGINT and space collection technologies determined a reconfiguration of military information systems, of domains and subdomains regarding responsibilities in collection and production, for an efficient and effective management for intelligence products.

Modern confrontation space complexity generates information risks, threats and vulnerabilities and the need for specific protection measures. Information era impact effects in military domain generated rethinking actions for training and tactical, operational and strategic confrontation engagement of forces and for defense politics and its objectives. Information technologies create new elements in military actions management, maneuver capability, protection, force structure and information operations procedures.

BIBLIOGRAPHY

AJP-01 (B), Allied Joint Doctrine, NATO HQ, Brussels, 2001.

Joint Vision 2020.

Bădălan Eugen, Frunzeti Teodor, *Asymmetry and Idiosycrasy in the military actions*, Technical-Editorial Army Center Publishing House, Bucharest, 2004.

Bălăceanu Ion (collective), *Interaction of strategies in context of the modern armed conflicts*, UNAp. Publishing house, Bucharest, 2010.

Frunzeti Teodor, Zodian Vladimir, *World 2011, Political and military Enciclopedy (security and strategic studies)*, Technical-Editorial Army Center Publishing House, Bucharest, 2011.

Khalilzad Z., White J.P., Marshall A.W., *Strategic appraisal. the changing role of information in warfare*, Rand, Santa Monica, California, 2001.

Mills Gary H., SHAPE Senior analyst, *The role of rhetorical theory in military analysis*, 2003.

Roceanu Ion, Buga Iulian, *Information, conceptual landmark and security coordinates*, AISM Publishing House, Bucharest, 2003.

http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-15.pdf