ENSURING THE SECURITY OF TECHNICAL EQUIPMENT OF THE STRATEGIC INFORMATION SYSTEM

Ovidiu MOŞOIU

„Henri Coandă" Air Force Academy, Brasov, Romania

Abstract: *The information society, through the influences of information technology, has caused profound mutations in the military domain. Ingenious use of new technologies, coupled with significant changes in the military doctrine and operational and organizational concepts, cause fundamental changes in the character and conduct of current and future armed combat, signing us up for the so-called concept of "military affairs revolution".*

Keywords: *Information society; the technical and military domain; operating system; network server; network administrators; equipment security; communication systems.*

1. INTRODUCTION

In the "Unique Perspective - 2020" (Joint Vision - 2020) document developed by the Joint Chiefs of Staff of the U.S. Army, it believes that the fundamental objectives in the military domain are full domination in all spectra, information superiority and technological innovation. To achieve an effective military force in 2020, a full intellectually, operational, doctrinal and technical integration is necessary. In the military and technical domain, communication and information are particularly important, their unquestionable importance being caused by the multitude of vulnerable targets, quickly accessible in a broad and increasingly spectrum that requires more resources of protection (techniques, tactics, procedures, weapon systems, and means of warfare).

The confrontation for obtaining and maintaining dominance, information superiority and supremacy and the increasing dependence on systems and information technology, machinery and related software have led to risks, threats and vulnerabilities that require appropriate measures in the context of new Military Affairs Revolution and the War Based on Network.

From the military perspective, these technologies of the Informational Revolution, will be the means leading to military efficiency, reducing losses and decreasing budgets, a unitary cohabitation of the military and social perspectives for the benefit of more efficient military structures and the directions in which this structures can develop, will be essential.

2. TECHNICAL METHODS OF SOLVING COMPUTER PROBLEMS

No matter how well designed and implemented a computer network is, situation in which a user cannot access the local server or a hierarchically placed above or below server can be reached at any time, or multiple users will not have access to the peripherals resources of the system (printers, faxes and so on). This problem can be caused by a user error, a software problem or a physical connection problem. Errors generated by users can be solved by preparing users to operate applications as well as rights of access and operation. These errors can be avoided by preparing users within level courses as well as preparation in structures where they belong, during the trial period of the application or on specialized training.

Software generated problems will be solved by network administrators using operating system utilities software of the network server. For this purpose, it is necessary to purchase complete software package of the operating system and network documentation and updates provided by manufacturer.

Regarding servers, monitoring activity focuses on tracking processor performance, paging files, for diagnosing memory and HD problems. For this purpose, overuse of components that would reduce system performance is taken into consideration. Monitoring the functioning of components can be viewed as histograms, charts or reports through programs under which the servers operate (for example, Windows Server uses system performance monitoring application).

By setting up a performance alert to a preset threshold, depending on the tracked feature, overloading the system hardware components can be avoided. In this sense, if we follow the overload of file server HD by setting a minimum threshold of 30% of free space in Windows Server an alert is enabled from log workstations application. By comparing system components performances with default usage standards, system crashes, premature wear of parts or replacement of parts that prove to be insufficiently dimensioned within maximum traffic conditions, can be avoided. Network monitoring can be done using software and protocol packages. Through these programs, capturing and analyzing network data frame is done.[1]

Analyzing traffic between network components during communication sessions can determine a baseline network (Habraken Joe, 2002). When there is a significant difference between the basic standard of the network and information provided by another data frame capture, the network administrator must determine whether intervention is required in the system. For example, if there are an excessive number of messages sent from an address corresponding to a workstation, an intervention is required because the network card is defective.

1 www.ethereal.com

Connection problems related to hardware, network cables, hubs, switches, amplifiers, and network interface cards other hardware devices important for network communications can be solved largely with the help of software tools[2], by adequate training of users and personnel destined for the technical implementation of network infrastructure. However, there are a number of physical cabling issues such as network disconnections, interruptions, faults or other issues that, although detected by software, it can only be solved through the intervention debugging groups equipped with special devices. These devices can be fitted to cables to detect any faults or interruptions. To troubleshoot these problems voltmeters or reflectometers can be used. The Domain Reflectometer[3] can pinpoint where the cable is cut, greatly facilitating debugging circuits. Another accident could occur by random or deliberate disruption of supply or failure of one of the network components).

To ensure optimal operation of strategic information system, given that its technical support is achieved by a system sensitive to power supply, it is necessary to solve the problem of power supply. We believe that this problem can be solved by providing uninterruptible power supplies for servers and workstations.

3. SECURITY POLICIES OF THE STRATEGIC INFORMATIONAL SYSTEM

From the analysis it appears that ensuring the security of the strategic information system for real time management of human resources and of its computer networks, specific policies must comply with NATO and the EU, and the legal framework of Romania, according to the CERT model of response to accidents protection of the Ministry of Defense systems.

2 ww.cisco.com/warp/public/44/jump/ciscoworks.shtml

3 www.tm.agilent.com (time domain reflectometers)

By respecting the commitments assumed by the Ministry of National Defense ,,The capability to respond to security incidents "concerning information and communication technology, for the ,,Cyberdefence and Information Assurance in the NNEC Framework" objective assumed by Romania in the ,,The proposals of the 2008 Force" it is believed that strategic information system security can be assured. Also a very important problem consists of information security measures during traffic in the informational system. The system is vulnerable, especially by intercepting communications in the transmission medium. A viable solution to this problem is data transmission and information encoding.

The safety of the technical equipment is achieved mainly through training and equipping maintenance groups of the information system as well as training system operators. Given the system requirement to operate in times of peace, crisis and war, uninterruptible power sources as well power generators that allow powering the equipment in any condition, must be provided. Structures using the strategic information system must take security measures to reduce the risk of dissipating information or to degrade data and information.

The security problem includes legal, social and ethical issues concerning physical control (guarding and opportunity to block access / of entry terminals), setting access conditions, operational procedures (attachment of passwords) criteria for hardware control (hardware mode of accessing different components), protecting operating system (information and cancellation of intermediary results for data secrecy) issues relating to the concept of ownership of the information from the database and others alike.

INFOSEC is a basic domain in ensuring the security of data and information from the informational system and it is one of the key domains (***, 2011:25) of information operations. Because the concept raises confusion, it would be useful to see, first of all what INFOSEC is not. First, NATO experts say INFOSEC is not an abbreviation, they say INFOSEC does not mean "Information Security" and also that INFOSEC does not mean "Information Security Sistems,, (Information Systems Security).

INFOSEC includes measures and procedures to protect the information as well as the systems. Therefore INFOSEC covers not only information but also communication and information systems (CIS). As a wide area of interest comprises four parts: computer security, transmission security, emission security and cryptographic security.

NATO considers INFOSEC as *"security measures to protect information processed, stored, or transmitted by computer systems, communications and other electronic systems against loss of confidentiality, integrity or availability, whether accidentally or intentionally, and also to prevent loss of integrity , availability of information processed, stored, or transmitted to those systems and non-repudiation. INFOSEC measures include measures related to computer, transmission, emission and cryptographic security. INFOSEC measures also include the detection, documentation and annihilation of threats to information and systems."* (***, 2002:3)

We believe that the application INFOSEC in the strategic informational system will be to implement specific procedures and measures in four functional areas: computer security - aiming denial of access and unauthorized exploitation of own computers and computer networks; transmission security - with measures to ensure the protection of data and information transmitted by the information system against unauthorized interception and exploitation; emission security - to prevent unauthorized exploitation of information that can be obtained through the interception and processing of electromagnetic emissions of electronic equipment from the endowment of the information system; cryptographic security - with results in the endowing of the information system with encryption equipment and proper usage of equipment. The implementation of these procedures will be done according to NATO security directives, and all nations within the alliance must comply with the alliance's directives in this domain.

In conclusion, to ensure a security environment in which the strategic information systems can operate without the risk of affecting information, a series of measures, procedures on different domains - physical personnel organization, information security and INFOSEC - should be developed and implemented. In this way confidentiality, availability, integrity and non-repudiation of classified information stored, processed or transmitted by the strategic information system will be ensured.

BIBLIOGRAPHY

1. Alexandru, M., Stoica V. (1995). *Sistemul informațional militar*, Bucureşti: Ed. Academiei de Înalte Studii Militare.
2. Angheloiu, Ion. (1990). *Automatizare şi informatizare în domeniul militar.* Bucureşti: Editura Militară.
3. Bălăceanu, Ion. (2001). *Revoluția tehnologică contemporană şi impactul ei asupra potențialului militar*. Bucureşti: Editura Academiei de Înalte Studii Militare.
4. Dumitru, V., Stoian, I., Baltă, C., Toma, Ghe. (2000). *Sisteme informaționale militare - analiză şi proiectare*. Bucureşti: Editura CERES.
5. Gruia, Timofte. (1999). *Comunicații militare moderne.* Bucureşti: Editura AISM.
6. Habraken, Joe. (2002). *Rețele de calculatoare pentru începători*, Bucureşti: Ed. BIC ALL.
7. Nicolaescu, Ghe., Simileanu, V. (2005). *Restructurarea sistemelor informaționale*. Bucureşti: Ed. Universității Naționale de Apărare „Carol I".
8. Neacşu, Dumitru. (2012). *Perfecționarea sistemului informațional strategic în contextul noului mediu operațional.* Bucureşti: Ed. Universității Naționale de Apărare „Carol I".
9. Pantazi, Stelian. (2007). *Tehnologia şi acțiunile militare în era informațională*. Bucureşti: Ed. Universității Naționale de Apărare „Carol I".
10. Teodorescu, Constantin. (2005). *Războiul informațional – Agenții şi servicii de informații*. Bucureşti: Ed. Universității Naționale de Apărare „Carol I".
11. Tudorache, Paul, Mandache, RA. (2009). *Implicațiile noii revoluții în afacerile militare în armată*, în sesiunea anuală de comunicări ştiințifice cu participare internațională *Stabilitate şi securitate regională.* Bucureşti: Ed. Universității Naționale de Apărare „Carol I".
12. *** (2004). Department of Defence, *Network Centric Operations Conceptual Framework, version 2.0.*
13. *** (2003). *Doctrina pentru sprijinul cu informații al operațiilor întrunite*, Bucureşti: Editura Militară.
14. *** (2011). SMG/C.O. – 10.0, *Doctrina operațiilor informaționale*, Bucureşti: CTEA.
15. *** (2002). Glossary to C-M(2002)49, *Security within the North Atlantic Treaty Organisation (NATO)*, Brussels: NATO HQ.
16. *** (2001). *Network Centric Warfare*, Department of Defense, Report to Congress. Appendix, 27 July.
17. *** (2007). *Sistemul de comunicații şi informatic din cadrul Statului Major al Forțelor Aeriene*, Bucureşti: CTEA.
18. *** (2012). *Studiul C4I2SR pentru Armata României.* Bucureşti: CTEA.
19. www.ethereal.com
20.www.cisco.com/warp/public/44/jump/ciscoworks.shtml.
21. www.tm.agilent.com (time domain reflectometers)