MIKLÓS ZRÍNYI
NATIONAL DEFENCE UNIVERSITY

INFORMATION SECURITY TASKS AT HUNGARIAN DEFENCE FORCES, AS A PART OF SECURITY

Written by LTC. Károly Kassai

Tutored by ret. COL. Miklós Sándor (PhD, Military)

Extract of Thesis

– 2007 –

BACKGROUND

The fast development of society and technology increase the importance and quantity of information nowadays. This is the situation at Hungarian Defence Forces (HDF) too, so the modernisation and the creation of a more flexible, robust and secure military communication and information system (CIS) is an actual issue in Hungary. NATO and EU membership is a challenge in information security field.

The information security at the HDF meets laws and other governmental requirements of course, but these regulations don't cover every protection possibilities same level, and they don't have full compatibility between different fields (e. g. NATO or EU and national classified information).

HDF doesn't have official comprehensive approach for information security at the moment. The required regularisations, protection methods have some overlapping and different point of view.

RESEARCH OBJECTIVES AND SPECIFICATIONS

The basic hypothesis is that the examination of information systems and their protection possibilities, methods and applied measures with system-specific approach can balance the information threats. Detailed research aims:

- Statement of information security issues in Hungarian strategic level documents and pointing out the propriety of this support from HDF perspective. Analysis of the most important Hungarian military doctrines from information security's point of view, characterisation of deficiencies and to take recommendations.
- General characterisation of information security fields, element and processes, pointing out the most important deficiencies from a network-centric point of view, and development of general security principles.
- Examination of the harmonisation between NATO, EU and national regulations and pointing out the main problems with cooperation between national and alliance owned communications and information system (CIS).
- Describing information security management issues, characterisation of the different influences of laws and other governmental requirements, and creation of recommendations for complex information security regulation system.

This research has some specifications and limitations.

The foreign and Hungarian sources use expressions "information" and "data" in different ways. The Hungarian governmental language (e. g. laws and other edicts) uses "data protection" only for protection of personal data. HDF organisations use the special expression "secret protection" because of historical reasons but this term covers only classified information.

The expression "data" in this study has a complex meaning (e. g. personal data, classified data, economic or other sensitive data) and because of this situation inside this examination the expression "information security" covers the traditional Hungarian meaning "data protection".

The "information security" is the largest, generic category for comprehensive protection of data and data handling system in HDF, so the cryptography or electronic (e. g. informatics)

information system protection is a part of this terminology (but decades ago tens the meaning was equal to crypto security).

English sources use “security” with three meanings: as a status, an activity or an organisation. The Hungarian language distinguishes them clearly. In this study “security” means status (or result) and “protection” means activity (for this status). Inside HDF organisations which achieve information security functions generally called “information protection”.

This research is based on the needed information security requirements and protection methods and this perspective has a priority. Financial, economic or other organisation reasons could have other conclusions that this study was written according to the decision of leadership.

This study is independent from technology, specific technical solutions or system-specification.

Finally, the examined issues are the author’s own point of view and not official HDF’s stand point.

RESEARCH METHODS

The Hungarian military science has not determined theoretical and practical issues in (military) communication system field exactly yet. HDF doesn’t an official determination, model or generic high level approach in information security field.

Because of this defiance the appropriate method for researching the objects is the next logical line: WHY is there a need for protection of information systems)? – WHERE is the appropriate protection)? – HOW CAN ORGANISE and MAINTAIN the appropriate security system.

There are some general supporting methods for research: examination of cause and consequence relation; working out from the simple towards to the difficult and vice versa, generalisation, summarisation, and conclusion.

This work is based on public information. Mainly from the internet, official governmental security and other strategic/high level documents, standards, international and EU recommendations, and other forums e. g. conferences, seminars, and published papers in military, security and information technology (IT) field.

The other pillar for working up planned issues is the continuous consultation with military specialists at planning and operational organisations, and users of different national and NATO, EU communication networks and real full life cycle work about these networks.

The third source is the civil and military education and training system and the author’s practical experiences during information collection, inspection, accreditation, training at military and civil organisations.

RESEARCH REVIEW

First part of research

The Hungarian National Security Strategy and foreign security strategies, high level official strategic documents are underlying statements that the official Hungarian point of view is up-to-date but it isn’t a good basis for other lower level documents. The complexity of protection in information field and the needed supporting background for secure critical

infrastructures (e. g. research and development, manufacturing, certification, training and accreditation) could be the reason for the creation of a baseline for a national wide cooperation in a national defence strategy and launch planned national information strategy.

The national interests, threats, vulnerabilities, resources and tasks are the basic framework for an effective analysis or establishing a start position for a new strategic level document.

The key information security elements in strategic level documents (e. g. National Defence Strategy, National Military strategy, National Information security Strategy) are the next:

- The information services are basic governmental interests. The governmental information system has public services and other information services for secure official data and classified information protection (according to the threat and vulnerability).
- The new information services (e. g. internet access, interconnections of networks) launch new challenges and threats because this evolution supports the exploitation of attacking methods and procedures. The intentional and accidental actions have an accumulation effect and the different threats can attack independent points and time in asymmetric method. The targets are not only military capabilities but the key elements of the critical infrastructures and services nowadays.
- The national independence in sensitive parts of national critical infrastructures, the implementation of emerging technologies, and the co-ordinated protection methods, training, accreditation and inspection processes are the key elements of governmental or military systems with focus on detection, prevention and reaction. Similar to the development of attacking methods the system operating organisations need to develop the risk assessment and management methods, the flexibility of information services and the recovery capabilities. The organisations' co-operation, standardisation, common principles for evaluation, certification and accreditation, interoperability have more and new dimensions in the age of connected networks. Against terrorism and computer crime the monitoring of new technology and upgrade of protection measures is a continuous issue.

The examination of joint Hungarian military doctrines from information security perspective points out some overlapping and terminology problems inside information operations (IO) and information security field, too. In the next version of Joint Doctrine it is necessary to make some correction in the elements of IO, and a more practical solution is to put a new part inside IO chapter for information security including computer network defence issues and to delete the independent old security parts of CIS section.

The new global NATO view is a good motivation for member nations. The NATO Feasibility Study and the Vision and Concept (the Military Challenge) are a new concept for the new generation military power. The main elements of new military capabilities are the information superioirity and the NATO network enabled capability (NNEC). The study shows the main issues of this development direction form information security's point of view.

Second part of research

For the best implementation of information security elements (e. g. physical, personnel, documentation and electronic information security) and their measures more suitable a new general classification system in Hungary according to NATO, EU compatible classification

system (e. g. UNCLASSIFIED, RESTRECTED, CONFIDENTIAL, SECRET, TOP SECRET, and specific handling specifications) for governmental organisations. Inside security classes focus on confidentiality, integrity and availability of information in their complexity (and not only confidentiality or value of information assets) are needed.

The equivalent level protection requires detailed, modern national risk assessment methods because the national network enabled capabilities will not operate in secure mode if the governmental organisations have different risk management approach with not compatible methods, terminology and priorities.

The modern information security system requires a new concept inside HDF with detailed measures of each security class. This study summarises the main security issues in each classification level and identifies the more important general protection capabilities of CIS's according to network enabled capability approach. Based on practical experiences from 1999 (e. g. implementation of NATO Security Policy, Directives and supporting Guidelines in the appropriate networks, and new communications establishments), the study underlines the main difficulties in security field and gives some recommendation for future implementation.

Because of the lack of general, system and classification independent governmental principles the study identifies 17 security principles for Hungarian military CIS based on international and national standards and the author's experiences.

Third part of research

Hungarian governmental level consists of more than practical offices and authorities in communication and security field. The concentrated security management from HDF perspective is primary issue (during the last few years inside Ministry of Defence there were separated security organisations with different competence and own organisation goals) because the correct translation of governmental and NATO, EU requirements into the supporting CIS is key organisation security issues.

The NATO/WEU Central Registry and the NATO/WEU National Distribution Authority have larger responsibility than HDF's organisational responsibility. The actual governmental regulation doesn't cover the registries specific responsibilities, so some changes in the next revision of governmental requirements could be useful.

The next critical topics in information security field are the separation between general managerial responsibility and responsible expert position. The development in information technology (IT) field in case of comprehensive networks requires different knowledge, capabilities and organisation contacts, so future challenge at HDF is to separate leaders and specialists appropriately. Based on this decision the next stage is to create a suitable education and training program according to the selected responsible persons.

The views of unclassified HDF regulation documents are underlying the deficiencies of an approved summarised security requirements. Because of this lack this study creates the general baseline for HDF's information security policy. The recommended HDH Information Security Policy is an unclassified high level documents approved by minister of MoD. The main purpose of this document is to make an appropriate interface between governmental and NATO, EU security organisation, standards and other requirements and HDF in information security field.

HDF is a horizontally and vertically large organisation, so the next step is to create an appropriate frame for different level security documents. This study shows a useful model for a three level regularisation system. The key factor for a modern regulation is the changing point of view from organisation point of view to system-specific approach.

Under the HDF Information Security Policy could be useful a central regularization level. In electronic information security field the appropriate document in this level the HDF Electronic Information Security Requirements Statements. This document could be a core library for general security requirements all classification level in case of networks, stand alone or mobile equipments. Besides this document in this level shall establish appropriate physical, personal and documental security policies as a background for appropriate protection methods, measurements and control for correct information handling.

The third level is the local and system-specific protection issues. According to NNEC conception at HDF organisations could focus on system specific approach.

Large, complex CIS or high sensitive information handling process requires separated system specific security documents (security requirements and security operational processes). This separation can support the life-cycle model. The specified security requirements by this study depend on risk evaluation and operational requirements and the management and security staff should refresh this document in each life-cycle stage regularly.

The governmental level accreditation system is not complete in classified information field because NATO, EU system required a central, structured accreditation process by National Security Authority but a national system has only system owner authorisation. The complex, governmental and international networks and the equal protection level theory require central processes with same criteria, methods and parameters. This study outlines the key issues of the accreditation decisions.

The full life-cycle point of view requires permanent security control of information handling systems. This study separates the security inspection into two main parts: organisation and system-specific issues. The organisation type inspection covers the critical management and regularisation question's view (e. g. security management structure, organisation's self-inspection system, operation and security tasks, education and training system, incident handling) through years. Other side should organise a system-specific control method for view details, technical parameters (e. g. hardware and software configuration, maintenance logs, security settings, ports and interconnections, emission security measurements, system and security log analysis). The modules of control system can support the accreditation and re-accreditation processes too.

SUMMARISATION

The first chapter deals with strategic level information security issues. Key elements are the lack elements in Hungarian security strategy level, summarisation of national security strategy, establishing a model for information security parts of strategic level documents, analysis of key joint Hungarian military doctrines, recommendation for modern information security part inside IO chapter and a short review of NNEC model form information security perspective.

The second chapter's topic is high level summarisation information security elements, risk assessment process, security classification of information, and protection issues and typical problems, challenges according to classification level, and creation of system and classification independent security principles.

The third chapter review the key security management elements, as responsibilities, new HDF regularisation system in information security field under umbrella of HDF Information Security Policy, new approach in regularisation for the appropriate support of system-specific issues, accreditation, and the most important control issues.

RESULTS OF STUDY

1) Determination of information security frame in Hungarian Military Strategy and strategic level HDF documents. Identification of main deficiencies in joint doctrines and recommendations for appropriate information security part inside information operations.
2) Systematisation of information security elements and identification of national regularisation problems against national and alliance level network enabled operations. Determination of system and classification independent security principles for the equal level protection in information handling systems at HDF organisations.
3) Determination of not adequate harmony between HDF regularisations in information security field. Recommendation for a synopsis of HDF Information Security Policy and its supporting documents structure. Formulation of the basic general governance tasks and revision requirements of regularisation system.

UTILISATION AND RECOMMENDATIONS

The study identifies the main key points for a coherent information security system at HDF organisations.

The implementation of the recommended information security issues in Hungarian Military Strategy, Information Operation part of HDF Joint Doctrine can establish a high level comprehensive summarisation and input for lower level military documents according to the NATO, EU and governmental requirements.

Development of a high level summarizing document (HDF Information Security Policy) could be an interface between enterprise level requirements and can establish a common basis for lower level regularisations in case of regular updating.

The background information about strategic level documents could be a practice summarization for planning officers.

The summarisation of NATO, EU research goals and topics could be useful for planning and operating organisations, persons.

The recommended security principles could support system planning activities and system specific decisions.

Generally the study could be useful supporting documents in the educational and training system.

PUBLICATIONS

The author's publications in connection with this study:

1) A vezetés ellenőrzési funkciójának érvényesüléséről; Hadtudomány ISSN 1215-4121, 1999. 3-4. szám p. 94-106.
2) The difficulties of scope of control duties; Hadtudományi Tájékoztató ISSN1419-7758, 2000/4 p. 93-106.
3) A vezetés korszerűsítésének technikai feladatai; Hadtudomány ISSN 1215-4121, 2000. 1. szám p. 63-71.

4) A korszerű rádiókkal kapcsolatos információvédelmi feladatok és lehetőségek, Kard és toll (válogatás a hadtudomány doktoranduszainak tanulmányaiból) Budapest, 2000 ISBN 963 7037 40 3, p. 73-83.
5) A fizikai biztonság, mint az adatbiztonság pillére; Katonai Logisztika, 8. évfolyam, 2000/3. szám p. 154-165.
6) A vezetéshez szükséges korszerű információvédelmi feladatrendszer tanulmányozása és az arra történő áttérés fontosabb feladatai; Nemzetvédelmi Egyetemi Doktorandum 2001, ISSN1588-2233, p. 76-86.
7) A híradó és az informatikai rendszer korszerűsítése és védelme; Hadtudomány 2001/1 p. 92-98.
8) Vezetési és logisztikai műveletek, folyamatok az információvédelmi rendszer hátterében; Katonai Logisztika, 2000/4 p. 23-33.
9) A híradó és informatikai rendszer korszerű szolgáltatásainak hatása és az új információvédelmi feladatok; Nemzetvédelmi Egyetemi Közlemények, 2001. 5. évfolyam 1. szám, ISSN 1417-7323, p. 229-239.
10) Úton a korszerű híradó és informatikai rendszer felé; Új Honvédségi Szemle ISSN 1585-4167, 2001/4 p. 9-23.
11) Biztonságpolitika és információvédelem, Hadtudomány 2001/3 p. 71-76.
12) Responsibility for a secure CIS, 2001. Konferencia kiadvány ISBN 963 008819 3, p. 113-117. *i*
13) Az információvédelem újszerű megközelítése, Kommunikáció 2001. kiadvány, ISBN 963 008819 3, p. 193- 198.
14) Az információvédelem rendszerszintű feladatai, Nemzetvédelmi Egyetemi Közlemények, 2001. 5. évfolyam 4. szám, p. 111- 120.
15) A minősített információk és adatok védelme; Hadtudomány 2002/1 p. 64-70.
16) A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései Nemzetvédelmi Egyetemi Közlemények, 2002, 6. évfolyam 2. szám p. 163-170.
17) Kassai Károly – Magyar Sándor: A zártcélú hálózat felügyeletének biztonsági kérdései Új Honvédségi Szemle 2002/11 p. 88-95.
18) Az elektronikus információk védelmének területei, Hadtudomány 2002/3 p. 95-102.
19) Areas and activities for the information (and information system) security; Kommunikáció 2002. kiadvány, ISBN 963 86229 2 X, p. 75-80.
20) Az elektronikus információvédelem néhány szervezeti kérdése Kard és toll 2002, ISBN 963 7037 52 7, p. 128-133.
21) Az információk és információs rendszerek fenyegetéseinek stratégiai szintű megfogalmazásai, Új Honvédségi Szemle 2003/3 p. 28-36.
22) Az információs rendszerek védelméről, Hadtudomány 2003/1 p.119-126.
23) Az információk, a híradó és informatikai rendszer eszközeinek védelme, Hadtudomány 2003/3-4 p. 61-68.
24) Az információk, valamint a híradó és informatikai rendszer védelmének szabályozása, Kommunikáció 2003. kiadvány, ISBN 963 86229 62 p. 133-140.
25) Kassai Károly – Magyar Sándor: A híradó és informatikai rendszer csomópontjainak védelmi kérdései; Felderítő Szemle III. évfolyam 1. szám 2004. március ISSN 1588-242X p. 128-136.
26) Az elektronikus adatkezelő rendszerek védelmének fontosabb tendenciái (kiemelten a szabályozási területtel kapcsolatos feladatok); Kommunikáció 2005, ISBN 963 7060 11 1. p. 161-170.
27) Az elektronikus információvédelmi rendszabályok megalapozásának fontosabb kérdései, Kommunikáció 2006. kiadvány, ISBN 963 7060 18 2 p. 131-143.

28) Kassai Károly – Kiss József: Információ- és dokumentumvédelem; „A honvédelem négy éve 2002-2006”című kiadvány, HM Zrínyi Kht. 2006. ISBN 963 327408 7, p. 80-81.
29) Az elektronikus adatkezeléssel kapcsolatos kockázatok kezelésének egyes kérdései, Kommunikáció 2007. kiadvány, ISBN 978-963-7060-31-1, p. 77-82.