MILITARY NATIONAL SECURITY SERVICE

I/2016.

NATIONAL SECURITY REVIEW

BUDAPEST

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

Lt-Gen József Kovács, Director General,

Chairman of the Scientific Board

Contact

Military National Security Service, Scientific Board
24-26 Bartók Béla Street, Budapest 1111
Pf. 117., Budapest 1502
E-mail: natsecreview@gmail.com

HU ISSN 2416-3732

THEORY OF NATIONAL SECURITY

GEOPOLITICS

INFORMATION AND COMMUNICATION SECURITY

BOOK REVIEW

CONDITIONS OF PUBLICATIONS

THEORY OF NATIONAL SECURITY

LT. COL. CSABA VIDA, PHD

INTELLIGENCE ANALYSIS

Abstract

In this brief study the author – who teaches the intelligence analysis at the National University of Public Service – elaborates the basics of intelligence analysis, and gives an overview of the analysing activity. The study concludes that the intelligence analysis is a science-based assessment of a theoretical activity, and the problem solving is in its focus point.

Keywords: intelligence, intelligence analysis, evaluation, theoretical methods, matrixes, intelligence reports, intelligence cycle, databases, procedures

The intelligence analysis is a complex system of activities. The information gathered by information collectors is processed systematically by analysis organizations with defined spheres of authority, and through procedures based on professional knowledge. Conclusions, assessments and predictions are conceptualized from the results. Therefore, the available data and information go through a positive, incremental, qualitative change through the analysis. The conclusions, assessments and predictions represent the value added. The process is similar when information collectors can only gather half-information, and it is the analyst officer's job to supplement it by using different procedures. Analytical work is a theoretical, conceptual system of activities, whose main aim is to solve the problem. Aside from their own procedures and theoretical methods, the analysts draw also on the results of other disciplines, like politics, law, history, statistics, economy, sociology, psychology and military science.

The analysis is a central element of the intelligence cycle, as their aim and purpose are the same: to provide the users[1] with analysed information to help them in decision-making and to uncover and define possible threats, risks and challenges posed to the state. Based on the intelligence cycle, the analysts receives the information requests from the users, control the data gathering activities pursued by the information collection services, process the data

[1] The users of intelligence are the leaders of the state, for example the government and the legislation, but military leaders and the leaders of law enforcement organizations also belong to this group.

obtained by collectors, analyse the information and inform the users about the required questions.

So the analysis work is executed within the frames of the intelligence and operates the intelligence cycle, based on defined methods and principles.

Fundamentally, intelligence analysis can be divided into six different spheres of action.

- analysing and assessing information;
- making reports;
- managing the databases of the analysing and assessing organization;
- dissemination;
- operating the intelligence cycle (helping the work of information collectors);
- supporting (intelligence and military) operations,

The above activities represent different stages in the analysis and assessment, because the operation of the intelligence cycle is going on during the whole process, while analysing and evaluating information, preparing reports and operating the informatory system are consecutive procedures, and the operation of intelligence databases only happens periodically.

It's important to emphasise that analysis doesn't only include the preparation of reports, because its main function is the analysis and evaluation of the information. Analysis work – similarly to the whole intelligence work – is not an autotelic activity, because its main objective is to provide the users with such information that helps them in making the right decision.

Information analysis and assessment

The complex analysis of the available information takes place during the analytical-evaluative work. In the course of this process, with the use of different analytical-evaluative procedures, the information goes through a qualitative change. The person who does analytical-evaluative work first places the information in space (location), time and (network of) occurrences (processes), establishes causal connections and draws up predictions, conclusions and possible scenarios. During the process, the value of the information rises significantly, because of the value added by the analytical-evaluative procedures and the expertise of the analytical-evaluative specialists. In order to produce a significant added value, the analysts can use basically the following procedures:

- simple formal logical procedures

- fixed analytical-evaluative procedures
- complex analytical-evaluative models and methods

The analysis and assessment based on **simple logical procedures** is the most common method, because this method is extremely effective when it comes to examining the circumstances, effects and consequences of an event that has already occurred. The logical procedures – the deductive[2], inductive[3] and abductive[4] – start with formal logical thinking methods.

In this respect, we can also mention:

- the observation (empirical understanding of reality);
- trial (inquiry of a consciously elicited event);
- analysis (dividing the whole system in its components and examining each component);
- synthesis (examining the connection between the components by arranging them into a logical system)
- abstraction (getting rid of the unnecessary components)
- generalization (drawing conclusions from certain events that may apply to the whole process)
- comparison (exploration of the differences and similarities between the occurrences)
- analogy (drawing conclusions from the similarities of distinctive features and characteristics)

Unlike others, analytical-evaluative experts use these methods consciously, not instinctively. Aside from the above methods, numerous other simple procedures can be distinguished, such as the following:[5]

[2] In the course of deductive thinking, one draws conclusions about an individual based on generalization, so one reaches the individual from the general. According to deductive thinking, „Something must be true!"

[3] In the course of inductive thinking, one reaches the general from an individual, so one gets to the full picture through the parts of it. This method might have a number of different results. According to inductive thinking, „Something is likely to be true!"

[4] In the course of abductive thinking, one makes conclusions about the reasons behind a certain event based on its consequences, so the method offers an explanation to the events. According to abductive thinking, „Something is believably true!"

[5] The intelligence services of the United States currently use around 160 simple analytical-evaluative methods.

- **comparative method** (a quite usable method of creating models, it doesn't require computer simulations yet, it's mostly used for the analysis of devices, objects and processes; it can be a very good method of analysing the development of the target object /country/, because it's comparable with the development of their own system; in this case, their own system and technology can be the basis of the comparison);

- **graphic model** (the model is based on the analysis of the given topic, using one or more variables (mostly plotted against time); it examines the changes that the topic goes through; however the model simplifies the results quite a lot, because it ignores other factors that influence the topic and are not contained in the coordinate system; analytical-evaluative experts can use this model to summarize the results of the analysis; the graphic model has different types, for example the exponentially increasing one, the one converting to a given value or the bell-shaped curve; these graphs depict the changes from which conclusions for the future can be drawn);

- **application of patterns** (in this model the analyst examines the previous repeating events and processes; the problem with the pattern is how much the route indicated by the pattern differs from the previous experiences, and whether the difference is significant enough to be noted; there are statistical, chronological and spatial patterns for the different pattern models);

- **enumeration** (the simplest model, which is based on listing the characteristics of the given topics and the arguments about it; these arguments can be negative or positive and can either support or contradict the topic; the next step is to delete the similar arguments on both sides and draw conclusions based on what is left, the other name of this model is the parallel list);

- **connection network** (inquires the system of connection between entities – people, places, organizations, objects, events –; the models that explore the hierarchy, the connections, the matrix and the network are all different types of connection models);

- **the process model** (describes the order of the events or the actions related to the topics, and with the use of this information, the possible future actions are predictable; the feedbacks are an important part of the process, the system of loops and lines describing the process defines the connection between the input and output, while the feedbacks are controlling elements);

- **profiling** (it is used to model people; the aim of creating profiles is to help to analyse the actions of a person and to predict his future actions, and also to determine his expectable behaviour/reaction to a certain event);

- **simulation model** (describes the interactions through a mathematical method, so it can determine the behaviour of the system).

The choice among the procedures depends on the contents of the given information and the aim of the inquiry, but there are cases where the personality of the analytical-evaluative expert influences which simple logical procedure he chooses to analyse the available pile of information. The results of the procedures usually contain only preliminary information for the conclusions, because these must be attained through further logical procedures by the analytical-evaluative experts, who also have to use their own expertise and knowledge. However, simple logical procedures also provide an opportunity to make predictions for the future.

The **fixed analytical-evaluative procedures** are special methods of analytical-evaluative work during which a given event, process or person is processed in a similar fashion every time, just as they were filling out a „form" with analysed-evaluated data. For example risk calculations, budget analysis and biographies are these kinds of procedures. When filling out the „form", the analytical-evaluative expert may use simple analytical-evaluative procedures as well. Among logical procedures mathematical and statistical methods are the most prominent ones. During the procedure it is important to pick out only the most necessary information, so the exhaustive, detailed analysis and evaluation of information falls into the background. In this case, the results of analytical-evaluative work – conclusions, the hypothesis, estimates and the results of mathematical procedures – cannot be substituted by the most necessary information. The missing information cannot be replaced with the analysis and evaluation of the available data; instead they need to be collected by the information collectors.

Thanks to fixed analytical-evaluative procedures, when it comes to identical subject matters, the users can get the same type of reports, which increases the efficiency of the information dissemination.

The **complex analytical-evaluative models** are very rarely used by the intelligence services, because they are more time-consuming and require a higher level of expertise. But at the same time, they ensure the determination of conclusions and predictions that are essential to users when it comes to making decisions. Most complex analytical-evaluative models are methods of different disciples that are transplanted into the intelligence work.

The complex models include:

- **complex matrixes** (using a few chosen characteristics, the complex inquiry of the systems can be done with the matrixes, and on the different levels of these chosen characteristics the factors influencing the operation of the system can be determined);

- **game theory** (examining the actors' behaviour in situations where every participant's actions are influenced by the possible reaction of the others; in this way strategic problems can be modelled);

- **space-time model** (models the changes that occur to an event and a process in different places and times);

- **geographic model** (makes it possible the placement of a certain event or process in time and space and the complex examination of the changes);

- **analysis of trends** (suitable for the description of processes and tendencies; helps to predict forecoming events);

- **models of security theories** (numerous procedures have been developed in security theories and IR theories that define and establish complex security, some of which can be used for analytical-evaluative work).

Based on the above descriptions, the analysis and assessment work uses the analytical procedures of different scientific fields in order to achieve the most accurate results when examining intelligence information. Experiences show that analytical-evaluative work mostly uses the methods of IR theories and security theories. One of these is the theory of regional security complex[6], which examines regional security systems based on the interdependency among states.

Drawing conclusions, developing evaluations, predictions and sometimes drafting scenarios are parts of the analytical-evaluative process. The above models help to draw conclusions and develop evaluations based on the available information. The evaluations are useful to the users because they refer to the background, the causal connection and the impact of certain events that occurred, while conclusions might include the possible consequences and the way forward as well. The preparation of predictions is one of the most important aims of analytical-evaluative services, because this is the best way to support users. Predictions have different types, ranging from simple statements to complex systems. Scenarios are one of the keys to complex systems.

Probable future occurrences are detailed in these scenarios. When preparing them, they analyse how and in which way the current situation might develop, so in a few words, what kind of situation might emerge in the future, and they set up hypothesises that model the ways in which the changes could happen. It's impossible to predict what will happen exactly, but the probability of future scenarios can be – more or less precisely – determined. In the case of scenarios prepared by analytical-evaluative services, it is extremely important to define the probability of certain events in the reports, because it helps users making a decision.

Basically, four types of scenarios can be distinguished:

- **demonstrative scenario;**
- **propelling scenario;**
- **scenario of political transformation;**
- **time-slice scenario.**

[6] The Theory of Regional Security Complex by Barry Buzan and Ole Weaver. Barry BUZAN – Ole WEAVER: Regions and Powers: The Structure of International Security. Cambridge, 2003

Disseminating information, preparing reports

When the analysis and evaluation of information is done, the preparation of responses to the users' information requests – which means writing informatory reports – can begin. This could be viewed as the second element of the analytical-evaluative work, however, the preparation of a report isn't always part of the process, because during the analysis and assessment, it might become clear that the information collected for a specific topic isn't satisfactory or is irrelevant to the users, so it is unnecessary to inform them about it. If further information is needed – and the information requests of the users are still relevant –, then the analytical-evaluative service or person files a supplementary (repeated) request of information to the information collectors.

Thus, at this stage, the preparation and elaboration of information takes place. In the case of information, punctuality, precision and uniformity are of heightened importance as users only trust intelligence reports that always contain truthful information.

The preparation of information is always based on the users' requests and the regulations of public acts (a system of duties for intelligence services determined by the law), during which users or public acts define the subject matter or the exact topic of the information.

Information can be written or verbal. Written information is in the form of reports, and for verbal ones, presentations are held. Nowadays, written reports are not only written on paper, but different documents on the computer belong to this group as well. Aside from that, information can be distinguished in numerous ways, but the process of preparation and the contents are more or less homogenous, as all of them must meet the contextual and formal requirements of intelligence information. The extent, the level of elaboration, clear, understandable wording, punctuality, uniformity, completeness and the separation of information and evaluation (conclusions) all belong to the contextual requirements.

The **extent** is important because users may have a limited time to read a report, so when reading (or maybe just glancing through) a long document, the most important points could be missed, while if the report is too short, it cannot give a satisfactory answer to the information request, and as a result, further questions might emerge.

Ensuring a high **level of elaboration** is the duty of the analytical-evaluative personnel, which means that they have to prepare informatory reports that do not contain half

information or indications, but information and evaluations are shown through a defined track of thought or an elaborated system.

Clear wording makes it easier for the user to understand the report. Reports written with difficult, long, compound-complex sentences won't reach their goals of informing the users properly, because they are hard to read and understand.

As for certain information, **punctuality** is very important, because approximate data and inaccuracies only strengthen the generality of the report, so the user won't get the necessary support.

Uniformity is a characteristic of reports that can be observed in the unified interpretation and usage of definitions, names and descriptions of activities. However, at the same time, the structure of reports is uniform too, so users get what they expect from intelligence reports.

Completeness determines the quality of the informatory report, because the user expects a report that answers all of their questions, otherwise they will feel like something is missing or further questions will emerge.

The **separation of information and evaluation (**assessment**,** conclusions and predictions) in informatory reports is extremely important because the user has to be able to differentiate between the information gathered by the intelligence and the evaluations, conclusions and predictions of the analytical-evaluative personnel.

Reports have definite formal requirements, for example they must have certain obligatory elements (title, résumé, summary for the leader, elaborated information, evaluation, the level of protection of the information (classification), the date of estreatment, the person who estreated the document etc.), the text should be readable, if necessary, it should contain footnotes (comments), and it should use Hungarian language in a precise, grammatically correct way. The formal requirements for reports – except for references[7] – are exactly the same as those for scientific publications. Documents of the intelligence must be free of grammatical errors and mistypings, as these errors question the punctuality of the report and its writers (and the estreaters as well).

[7] Leaving the references out is important because of the protection of intelligence sources. At the same time, the intelligence service itself is the safeguard that guarantees the usage of exact and relevant data for its information [report].

Because of their uniformity, the structure of the information is always pre-defined. The title at any time must include the subject and the field the information deals with. A résumé, which offers a quick orientation for the users, is often part of the information as well. The content is mostly elaborated in the text, and to make it more understandable, should/could be supplemented by pictures, graphs, tabs and sketch maps. The information must be stated first, and later on, it has to be followed by the evaluation. The informatory report should be closed by the name of the estreater and the date of estreatment, which also serves to verify the document.

The preparation of information starts with the collection and organization of available information and data, and the execution of the chosen analytical-evaluative procedure. In the meantime, the information that is planned to be included in the report (names, events, definitions, activities) is corrected. After that, the synopsis of the informatory report should be put together, during which the hypothesises are defined as well. The structure of the synopsis must meet two requirements: first, it must have an understandable train of thought, and second, it must include the main message of the informatory report. The train of thought is a well-structured process with points of junction. The main message is a determinant piece of information that the user won't forget on the long run. When composing the the text, simple, short sentences should be used. The usage of difficult, compound-complex sentences isn't beneficial. Using too many foreign words counts as a mistake as well – and that includes not only the words adopted from, for example, Latin language. English expressions and names should be avoided as well. The informatory report – if not stated otherwise – should be written in Hungarian, as it cannot be expected of the user to understand a language other than their mother tongue. The elaboration of the information could be followed by the evaluation, which is prepared after the analytical-evaluative procedures. The evaluation has to be clear and unambiguous.

Verbal reports should be prepared and organized in a similar way to written ones. If it is possible, verbal reports should be elaborated in writing, too, so they have a written (textual) version as well. This is important firstly because the service has to keep track of what kind of information did it share with whom. Secondly, it is useful to prepare presentation material (drafts) so that the oral presentations are easier to understand. It is also possible that after the oral report, the user will ask for the content of the presentation in a written form.

In the course of the preparation of information, the system of supervision and feedback – in which the leaders of analytical-evaluative organizations play a key role – is extremely important for national security services. The supervision guarantees that the intelligence information always contains real information and remains absolutely neutral politically.

Analysis-assessment databases

Databases are integral parts of the analytical-evaluative process, because they contain all pieces of information necessary for the execution of analysis and evaluation and the praparation of informatory reports for the users. Fundamentally, databases have two main parts. One contains every information gathered by the collectors, while the other has tematical database filled with information about a given target area, person or object. (For example, databases of names or organizations, or technical databases belong to this group). Aside from these, analytical-evaluative personnel can use other, external databases as well. These are operated by other organizations. These databases need to be examined and their credibility must be verified, because intelligence services can only use credible, reliable databases. These external databases can be commercial OSINT databases purchased by national security services.

Informatory system

Informing the users is the most important stage of the intelligence cycle, because this is the part when it becomes clear whether the intelligence was useful for the users. At this time, the whole process is evaluated as the users decide whether the products of the intelligence were useful to them. Intelligence services develop their informatory system based on this. In the system, there are different, predetermined types of information.

Information can be distinguished based on their periodicity, subject, extent, level of procession and urgency. As for periodicity, there are daily, immediate, periodical (weekly, monthly, yearly etc.) and ad hoc information. The subject is mainly determined by the information requests of the users, but certain information might cover more than one subject, and can offer a full, global-scale review about a given question. The extent of reports can be quite varied, but they should never be too long, because users have a limited time to read intelligence reports. The level of procession is defined by the nature of intelligence, which was already discussed before in the chapter about analysis and evaluation. Aside from that, the aim of the information also influences how deeply the user should be informed. The

urgency is defined by the content of the information. It means how urgent it is for the user to receive the information necessary to make a decision.

Aside from informing the users, intelligence services have obligations to supply information, which is also part of the informatory system. They send certain reports not directly to the end-users, but to the state organizations obliged to cooperate with each other. Instead of analysed-evaluated material, piles of information are sent to these organizations. However, this process needs some analytical-evaluative work, too: the data need to be systematized, classified and supplemented. The format of reports (supply of data) is not defined by the intelligence service, but the user (a.k.a the state organization with an obligation to cooperate).

Operation of the intelligence cycle

Analytical-evaluative organizations might have a heightened role within the intelligence cycle if the management of information is one of their duties, because if that is the case, they are present at every stage of the cycle. Looking at the cycle from an analytical-evaluative point of view, the process – whose aim is to, naturally, meet the information requests of the user –, happens in a way that is beneficial to the analytical-evaluative organization, which means it will be able to prepare informatory reports that support the decisions of the users to a satisfactory degree.

Five different stages of the classic intelligence cycle can be differentiated: receiving information requests, collecting information, processing and systematizing the collected data, analysing the topic and finally informing the users.

Analysing organizations take part in the acceptance of information requests. At this stage, after the questions of the users are received, analytical-evaluative personnel plan and organize the intelligence process as long as there are no specific bodies appointed to coordinate and control the collection of information. After that, the analytical-evaluative organization checks whether the answers are already available in the analytical-evaluative databases. If they aren't, the analyst organizations start the second stage of the cycle, which means they tell information collectors to gather the missing data. In the stage of information collection, analytical-evaluative organizations control the information collection activity through the system of feedbacks. In the stage of processing and evaluation, transformation of data happens in a way that the analytical-evaluative organizations can use the information. In

the analytical-evaluative stage of the cycle, analytical-evaluative personnel analyse and evaluate the information and prepare the informatory reports containing the answers for the users. The process of information is also based on the analysed and evaluated material prepared by the analyst organizations.

Conclusions

From national secrutiy standpoint, the intelligence analysis is becoming ever more complicated and – perhaps – ever more important. Within the intelligence cycle, it is the analysis and assessment activity that crowns all the intelligence process, because it is this activity that makes it possible for the intelligence service to provide the interested politicl and military leaders with the indispensable information necessary for their decisions.

The analysis and assessment are pursued with predetermined, sophisticated methods, from among which the most important are: the comperative, the graphic, the profiling and the simulation models. The so-called complex analytical models are very rarely used by the intelligence services, because they are rather time-consuming and require special expertise.

The intelligence reports to be disseminated have certain indispensable requirements, such as their appropriate extent, level of elaboration, clear wording, punctuality, uniformity, completeness and separation of information from evaluation.

The analyzing and assessing organizations have to follow through the whole intelligence cycle; beginning with setting the tasks for the organs collecting the information; and ending the intelligence process with disseminating the results (the reports) of the cycle among the decision-makers.

References

- Dr. KOBOLKA István (szerk.): Nemzetbiztonsági alapismeretek.
  Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. ISBN 978 615 5344 32 9
- Mark M. LOWENTHAL: Intelligence from secrets to policy.
  CQ Press, Washington D.C., 2012. ISBN 9781608716753
- Richards J. HEUER – Randolph H. PHERSON:
  Structured analytic techniques for intelligence analysis.
  CQ Press, Washington DC, 2011. ISBN 9781608710188
- Robert M. CLARK: Intelligence analysis: A Target-Centric Approach.
  CQ Press, Washington D.C., 2010. ISBN 9781604265439
- Washington PLATT: Strategic Intelligence Production: Basic Principles.
  Praeger, New York, 1957.
- ZNEHKNB5140: „Információk elemzése és értékelése" című
  MSc tantárgy előadásainak anyagai – készítette: Dr. VIDA Csaba, NKE, 2012.

LT. COL. CSABA VIDA, PhD

DOES THE INTELLIGENCE CYCLE STILL EXIST? (WHAT IS INTELLIGENCE ABOUT?)

Abstract

The author of this study has been dealing with this topic for several years. He raises the following right questions: does the intelligence cycle still exist, how did the intelligence cycle develop and change, what are the real elements of this cycle, which is the content of the request for information (RFI), what are the reasons for the rivalry between the information collectors and the analysts, who are the main critics of the intelligence cycle, what is the essence of their criticism, what are the contradictions between the political decision makers and the analysts. The author answers all these questions and draws the final conclusion that although the intelligence cycle functions in a different way in theory and in practice, there is still a need for the cycle to produce good intelligence products and provide the personnel with an efficient intelligence training.

Keywords: intelligence cycle, data collection, analyses and assessment, policy makers and analysts, criticisms of the cycle, main elements of the cycle, evolution of the cycle, request for information (RFI), further need for the cycle.

In the Hungarian society and scientific circles there is a lot of misunderstandings about the function of the national security system; and the cause of this should be examined from two viewpoints. First, the society identifies the national security system with the scandals and the abuses of the last decades, and with the activities of the state security services of the pre-1989 regime, because the media can only hammer this in the minds of people, due to the mysteriousness that surrounds the national security services. Second, the domestic literature available for everyone is extremely insufficient. This also applies to the theoretical bases of national security intelligence and counter-intelligence activities.

Regarding the theory of intelligence, especially the analysis and assessment activities, I have already pointed out this insufficiency in my study[1] entitled *Művészet vagy tudomány:*

* The author wrote his study under the support of the MTA Bolyai János Kutatási Ösztöndíj (János Bolyai Research Scholarship of the Hungarian Academy of Sciences)

Gondolatok a hírszerző elemzés-értékelésről (*Art or Science: Thoughts about Intelligence Analysis and Assessment)* [Felderítő Szemle (Intelligence Review), 2012/3-4.].

After the publication of the article, based on my research about the theory of national security intelligence, I had to state that there are some similarities not only in the case of analysis and assessment, but also in the case of the theory of national security intelligence itself. This is supported by the fact that one of the well-known search engines[2] on the Internet found only nine Hungarian results when searching for "intelligence cycle" as the description of the process of intelligence, while in English[3] there are 427,000 results for the same term[4]. Among the Hungarian results, there was only one that had the intelligence cycle as its main topic, which was published by Dr. Péter Fenyves[5], under the title *A hírszerző ciklus* (*The Intelligence Cycle*)[6].

In this study the author examined the elements of the intelligence cycle in the case of different foreign national security services, and in the end, he introduced his own version of the intelligence cycle. The author undertook only the task to introduce shortly the cycle, and he did not analyse its particulars or potential problems. The other results only touched upon the notion of intelligence cycle, but did not describe in detail its real meaning. Despite the insufficient literature, several higher education institutions teach the intelligence cycle[7].

Based on the scientific journals and magazines[8], it can be stated that in open sources, most of those who deals with the theory of national security intelligence are representatives of the military sciences. In Hungary, there is scientific literature for the theory of intelligence besides the open sources, because the national security services do have their own broad scientific description of their activity systems. However, these texts are still considered confidential information, despite the fact that in the international literature the theoretical questions can be easily found.

---

[1] Dr. Csaba Vida: *Művészet vagy tudomány: Gondolatok a hírszerző elemzés-értékelésről (Art or Science: Thoughts about Intelligence Analysis and Assessment)* pp. 140-141
[2] Google Search Engine, www.google.hu
[3] Term searched for in Hungarian: „hírszerzési ciklus", in English: „intelligence cycle"
[4] Date of access: Aug 1, 2013
[5] Retired Colonel Dr. Péter Fenyves, who has CSc in military science, expert at the Hungarian Association of Military Science, former associate at the Hungarian Military Intelligence Office, former defense, military and air attaché in Ankara.
[6] Colonel Dr. Péter Fenyves: *A hírszerző ciklus* (*The Intelligence Cycle*), pp. 66-75.
[7] Dr. Csaba Vida: *Művészet vagy tudomány: Gondolatok a hírszerző elemzés-értékelésről,* p. 147.
[8] Periodicals considered scientific by the different committees of the MTA (Hungarian Academy of Sciences). In military sciences these are the following: Hadtudomány, Új Honvédségi Szemle, Felderítő Szemle, Szakmai Szemle, Hadtudományi Szemle, Belügyi Szemle, etc.

In contrast with the Hungarian literature, the international, especially the English literature is extremely broad, and in the last decade a significant number of studies have been published in connection with the national security activity. These precisely elaborate on the theories of national security and the factors connected to the intelligence cycle as well. Based on these, the scientific debates surrounding the national security intelligence can be kept track of, as well as the debates about the intelligence cycle.

The Evolution of the Intelligence Cycle

The intelligence cycle describes the process of national security intelligence activities, which is present at every organization (government institutions and private companies) where people gather information. Despite this, the system of the intelligence cycle only took shape by the mid-20th century. The definition of the elements of military intelligence appeared in U.S. regulations around WWI[9], which defined the tasks of data collection, comparison and dissemination. After WWI, four elements of intelligence were identified: requests for information (RFI), collection of data, analysis and dissemination. The full system of intelligence emerged during WWII, which is well supported by the fact that after the war, the theory of the intelligence cycle was formulated and published by Robert Rigby Glass and Phillip B. Davidson in 1948 in their book entitled *Intelligence is For Commanders*[10]. They described the intelligence cycle as a cyclical process, in which the mission (cycle) has four elements: directing data collection efforts, gathering information, analysing information and utilizing the products of intelligence. When examining the origins of the intelligence cycle, Michael Warner[11] stated that the formation of the concept should be basically sought at the points of contact between military sciences and psychology, but in any case it originates from social sciences. After the description and definition of the cycle, the concept quickly spread among the international intelligence community, and thus it became the generally accepted model of intelligence. This is supported by the fact that this is also the base for intelligence[12] at the renowned intelligence services[13]. The system of the intelligence cycle solidified at the end of the 1940s and at the beginning of the 1950s, and it is still considered the classical version.

[9] Kristan J. Wheaton: *Let's Kill the Intelligence Cycle*. http://sourcesandmethods.blogspot.hu/2011/05/lets-kill-intelligence-cycle-original.html, date of access: 14 July, 2013.
[10] Robert R. Glass – Phillip B. Davidson: *Intelligence is for Commanders*.
[11] Michael Warner was a formal associate of the Central Intelligence Agency (CIA), who worked at the processing and analysing institution of the CIA, and later he engaged in the history of CIA.
[12] Colonel Dr. Péter Fenyves: *A hírszerző ciklus* pp. 66-75.
[13] American, British, German and French.

The cycle went though smaller changes in the last decades as a result of the development in information technology and information society, which manifested mainly in the breaking up of the working process. In the beginning of the 21st century, some representatives of the national security theory consider the intelligence cycle a "Cyclops"[14], because they think that nowadays it describes the process of intelligence defectively. Among the circles of the U.S. national security theories, a scientific debate developed in 2006 and 2007[15] in connection with the intelligence cycle. The leader of this debate was Arthur S. Hulnick[16], who wrote that "the description of the process is not good, based on which the intelligence process is working"[17]. Presenting the opinion of American intelligence officers, Robert M. Clark[18] in his 2010 study[19] explains that "…the intelligence cycle has become only a theoretical concept … Many intelligence officers admit that the intelligence process 'in reality, does not work like that.' In other words, effective intelligence efforts are not cycles."[20] Mark M. Lowenthal[21] analyses the system of the intelligence cycle in the fourth chapter of his book entitled *Intelligence: From Secret to Policy*[22], and points out that in his opinion, the process of intelligence is not a cycle, but a linear process realising on different levels as a result of constant feedback. Experts[23] participating in the relevant scientific debate also formulated several arguments against the intelligence cycle, claiming that it does not cover the whole process of intelligence.

Description of the Intelligence Cycle

After analysing the defects of the intelligence cycle, we need to discuss what the cycle in fact is. The cycle is a complex description of the intelligence activity, which includes the

[14] Kristan J. Wheaton: *Let's Kill the Intelligence Cycle*. http://sourcesandmethods.blogspot.hu/2011/05/lets-kill-intelligence-cycle-original.html, date of access: 14 July, 2013.
[15] The source of the debate was a 2006 study by Arthur S. Hulnick entitled *What's Wrong with the Intelligence Cycle?*
[16] Arthur S. Hulnick spent 35 years in the profession of intelligence, worked as an intelligence officer in the U.S. Air Force and for the CIA. Since 1989 he has been working at the University of Boston. His main research topic is strategic intelligence.
[17] Julian Richards: *The Art and Science of Intelligence Analysis*, p. 9.
[18] Robert M. Clark served at the U.S. Air Force, and then worked for different intelligence services for 42 years. He is currently a professor of the University of Maryland and the Intelligence and Security Academy.
[19] Robert M. Clark: *Intelligence Analysis: A Target-centric Approach*.
[20] Robert M. Clark: *Intelligence Analysis: A Target-centric Approach*, p. 11.
[21] Mark M. Lowenthal was the professor of John Hopkins University and the University of Columbia, previously worked for 36 years for different intelligence services, and worked as an expert for Congress.
[22] Mark M. Lowenthal: *Intelligence: From Secret to Policy*, pp. 57-70.
[23] Besides the above mentioned persons, Geraint Evans (intelligence officer of the British army), Lisa M. Palmieri (associate of the U.S. Department of Homeland Security), Julian Richards (professor of the University of Buckingham), among others.

process and system of information gathering, and the main aim of these is to support policy makers (users[24]) with information. Furthermore, it has early warning and forecasting tasks in certain security issues defined by the decision makers.

Currently, there are several versions of the intelligence cycle, which usually differ in the number or in the names of the stages of the cycle. The literature considers the five-element system as the classical version, which consists of the acceptance of requests for information (1), the data collection (2), the data processing (3), the analysis and assessment (4) and the dissemination (5).

The **acceptance of requests for information** stage is a much more complex element of the process than its name suggests, because this stage starts at the users' level[25], when they determine their requests for information and send it to the competent intelligence organization. At the intelligence agencies, these requests are interpreted first, then intelligence is designed and organized, and the data collecting organizations are tasked and directed. User's requests for information must be interpreted first from the intelligence point of view, because the users (mainly politicians, who are not experts at intelligence) do not formulate their questions in the language of intelligence. As a result, these have to be "translated", so that the data collectors and processors and sometimes the analysts can convert them into their own task systems**.** After identifying the questions, the competent organization plans and organizes the fulfilment of the RFI and examines whether the required information is already in the hands of the intelligence service, or it should be collected by the data collectors. If new data is needed, those data collectors are selected, who can collect the required data based on their skills and characteristics. However, it should be kept in mind during the organisation of intelligence work that even the biggest services[26] have limited capabilities, thus the RFIs must be prioritised. During this process, the importance of the original user (in case of governmental services, the position that the user holds in the government), the significance of the required data and the probability of the collection of the data must be considered. Obviously, intelligence services want to fulfil every information demand, but their capabilities limit this ambition.

[24] On the governmental level, the users are the members of the government, the heads of legislation, the directors of the central government offices and the commanders of the military and law enforcement organizations. In business intelligence, the users are the customers, who are usually the directors of different companies.
[25] Users of the information include political and military leaders and the directors of the central government organizations.
[26] For instance, the CIA and the Russian Foreign Intelligence Service employ thousands or tens of thousands of people.

In order to successfully collect the required information, during the planning and organization process, it is necessary to designate the most appropriate data collector organisation. The aim of this is to increase the efficiency of intelligence, because every data collector organization has different information sources, thus they can collect different types of information. After the selection of the data collector organization, the actual **data collectio**n starts. Data collection can be complemented in different ways, differing in the tool, the method or the procedure used for gathering data. Based on this we differentiate the branches of intelligence, which have different capabilities and characteristics. According to Lowenthal, in the process of intelligence, the data collectors produce raw data and information[27], but these cannot be considered as the products of intelligence[28], because in most cases they are unintelligible for the users. The amount of raw information determines the success of intelligence. However, this does not mean that the data collectors have to collect as many data as possible, because it would lessen the probability of the successful fulfilment of the request for information. Too much and sometimes irrelevant information can hinder the success, because the data processors and analysts can only process and analyse limited amount of information. Data processors and analysts always have smaller capacities than data collectors, thus the data collectors can only feed information related to the defined topics into the process of intelligence. However, this narrowing constraint may define the success and efficiency of the services in every case. For the intelligence organization, only those data and information exist that was forwarded by the data collectors in the intelligence cycle, because those that were not forwarded cannot be included in the reports prepared for the users.

The next stage of the intelligence cycle is the **processing and systematisation** of the raw data and information. Processing of raw information is needed because the data collected through data collection, especially by technical means (signs, codes, pictures, measurement data) is not practicable for all-source analysis and assessment, and is not suitable for informing the users. Processing raw information might require special skills, for instance decryption capability, or knowledge of a special language. If the raw data is not processed, it is qualified as unusable in the intelligence process. During data processing, raw data gives birth to information, which needs to be systematized to duly support the analysis and

[27] Between data and information, the following distinction can be made: data is unintelligible for the analysts directly because it needs to be converted into information. Based on this, data can be signs, numerical data and measurement results collected from technical reconnaissance.
[28] Mark M. Lowenthal: *Intelligence: From Secret to Policy*, p. 57.

assessment. During the systematisation, information is recorded, grouped and selected, and the filling of intelligence data stores starts.

After the processing and the systematisation, the next stage is **analysis and assessment**, which basically consists of two parts. In the first part, information is analysed and assessed, during which process the analysts define the cause and effect relations between the pieces of information, draw a conclusion and draft the predictions. For this, they use different analysis and assessment methods, which have three different types: the simple, logical analysis and assessment methods, the bound analysis and assessment methods and the complex analysis and assessment methods.[29] In the course of analysis and assessment, some information is analysed and assessed not only from one source, but from all available sources; this is called all-source analysis and assessment. After the analysis and assessment, raw and processed information go under a qualitative change, and thus become suitable for informing the users. Therefore, analysts can start the preparation of reports, which answers the users' request for information. During the preparation of these reports, analysts take into consideration the original RFI to the largest possible extent.

After the reports (the products of intelligence) are prepared, the next stage is the **dissemination** of information, which can be written or oral. Intelligence services can produce a large number of intelligence products, which all serve the purpose of satisfying the users' requests for information to an adequate degree. These RFIs are worded differently towards the intelligence services. The grouping of intelligence products is based on time, according to which the reports can be grouped as immediate reports, permanent and temporary reports, or long-run predictions that can be prepared for years. The method of informing the users raises an extremely important question: what kind of relationship is between policy makers and intelligence services, and how big the responsibility of intelligence organizations is.[30]

The above-mentioned five stages are the components of the classical theory of the intelligence cycle, which is completed by the system of feedbacks. Feedbacks are present in every stage and between the stages as well. Their fundamental aim is to increase the efficiency of intelligence, and to provide the best possible answer for the users' requests of information.

---

[29] Find more information about analysis and assessment methods in my study entitled *Művészet vagy tudomány: Gondolatok a hírszerző elemzés-értékelésről (Art or Science: Thoughts about Intelligence Analysis and Assessment)*.

[30] Find more information on this topic in Hadtudomány 2013/1-2. in my report entitled *Korszerű elemző-értékelő eljárások alkalmazása a hírszerzésben (The Use of Modern Analysis and Assessment Methods in Intelligence)*.

After the overview of the elements of the classical intelligence cycle, we need to answer the following question: who or which organization does operate the cycle? There are significant differences between the national security intelligence services in this regard, because in the case of services employing large numbers of people and operating on huge financial resources, a separate structural element engages itself in Collection Coordination and Intelligence Requirements Management (CCIRM), which can be found in the U.S. and the NATO intelligence doctrines as well. In the case of intelligence organizations with a smaller number of employees and capabilities, two different methods can be distinguished. One solution is that the analysis and assessment organization defines the process of the intelligence cycle, because it is concerned in all the elements, and this intelligence organization knows what information is needed to answer the users' requests for information. The second solution is that the management of the intelligence services operates the cycle, as a result of which the data collector, the data processor and the analysis and assessment organizations have a smaller scope for action. In these two cases, there is no significant difference in the operation of the intelligence cycle; there is only a slight difference in the independence of the different stages. In my opinion, if there is no possibility of establishing a CCIRM organization, than the analysis and assessment organization is the best for fulfilling this task.

Criticism of the intelligence cycle

Critics of the intelligence cycle concluded from the mistakes of intelligence, from their own personal experiences and the statements and recollections of the current and former employees of intelligence services that today the intelligence cycle is not operating sufficiently, thus it is not suitable for describing the process of intelligence. Problems pointed out by the above-mentioned critics can be divided into four groups. The first negates the existence of the intelligence cycle because (according to representatives of this group), it does not represent the real process of intelligence. The second group, although it accepts that the cycle in part represents the process of intelligence, but says that it is not a real cycle. The third group of critics attack the stages of the intelligence cycle, because they think that the function of the stages does not realize. The fourth group of critics states that some elements are missing from the cycle.

In the followings I will present these accusations, and will try to highlight their relevancy and irrelevancy in the case of the intelligence cycle, and I will suggest types of complements and modernization that could be done.

Some tasks of intelligence are not executed within the intelligence cycle

Hulnick states based on his experiences at CIA[31] that the intelligence cycle does not cover the whole spectrum of activities of intelligence services, because in the case of counterintelligence and covert and clandestine actions, the activities of the service do not happen on the basis of the cycle. Geraint Evans also highlights this problem in his work entitled *Rethinking Military Intelligence Failure.*[32] The American school of the theory of intelligence considers counterintelligence a part of intelligence, thus does not differentiate it from intelligence itself. However, when examining the theoretical activity of counterintelligence, it can be stated that – in contrast to the American theory and practice – it cannot be considered as a part of intelligence, because it has a different aim and a different purpose, and applies different procedures. At the same time, there are some similarities, especially when the counterintelligence organization does information-collecting activities, during which it also applies the intelligence cycle. The difference of the counterintelligence service is also supported by the fact that in several European countries[33], intelligence and counterintelligence activities are managed by different organizations.

Covert and clandestine actions are considered intelligence operations by the classical theory of intelligence, which represent the special branches of intelligence, because these are not always carried out with the aim of collecting information, but to cause disadvantage and loss to the target country, so that the target cannot assert its own interests and cannot protect its own values. Nowadays these include air strikes carried out by U.S. drones in Yemen and Pakistan, which belong to the actions of U.S. intelligence. However, these should be considered military actions rather than intelligence ones, despite the fact that the organisational element, which carries out these actions, belongs to the intelligence. Intelligence actions launched in the framework of information collecting do fit into the intelligence cycle because the collection of the required information can take place in the form of covert action, which – as data collection – is a part of the intelligence cycle. Based on these it can be stated that Hulnick's viewpoint is only characteristic of some special tasks of the American intelligence services, while the intelligence cycle can describe their activities directly connected to intelligence or information collection, based on the classical theory of intelligence. Those that are not connected to information collection (as counterintelligence

[31] Arthur S. Hulnick: *What's Wrong with the Intelligence Cycle?* pp. 13-14.
[32] Geraint Evans: *Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle*, pp. 22-46.
[33] Great Britain, France, Poland, Austria, Croatia, the Czech Republic, etc.

and intelligence actions carried out not in order to gather information) cannot be connected to the basic activities of intelligence.

Policy makers do not draft requests for information (RFIs)

In one of his criticisms[34], Hulnick attacks the present practice of drafting RFIs, which starts the intelligence cycle, because he refutes that the users of intelligence, namely the policy makers formulate questions towards intelligence services. In his opinion, the leaders (managers) of the services launch the intelligence cycle based on their own intuitions and the ensuing events. In this case, the aim of the leaders is to draw the attention of policy makers to the security problems threatening the country. Hulnick acknowledges that sometimes policy makers do give signs to the leaders of intelligence that they need information, but in his opinion these do not manifest in concrete questions. This leads back to the question of the depth of relationship between the intelligence leaders and the policy makers, because Hulnick thinks that the leaders of intelligence and the policy makers need to be in such a close relationship that the leaders have to know the problems of the policy makers, because intelligence has to answer these problems. In their studies they mention that other researchers also mention the lack of RFIs. For instance, Lowenthal writes about the vacuum of requests for information, when he asserts that policy makers assume that intelligence services know their demands, so they know what to do, and there is no need to word these demands.

When examining the questions of the lack of RFIs, the notion of RFI has to be defined, because the solution to the problem worded as criticism also lies here. There are different types of requests for information, because it does not limit itself to the written or oral questions of policy makers. RFIs can be laws, decrees, orders or temporary tasks connected to intelligence services and their activities, issued by policy makers and the legislature. For instance, based on the Act on the National Security Services[35], one task of the national security services is to "uncover the efforts indicative of offensive intention against the country"[36], and this can be considered a request for information because the policy maker authorized by the legislature expects information in this topic from the intelligence services. Intelligence cycles launched by these laws are constantly present in the activities of the intelligence services, thus they operate as an independent cycle on their own. Besides the legal instruments, the public and private declarations by policy makers should be considered

[34] Arthur S. Hulnick: *What's Wrong with the Intelligence Cycle?* pp. 1-2.
[35] In Hungary, national security services, therein the activities of intelligence services are regulated by Act CXXV of 1995 on the National Security Services.
[36] Art. 6 (a) of Act CXXV of 1995.

also as RFIs, in which they outline the topics they engage themselves in. If these fit into the legal responsibilities of the given service, these requests need to be translated to the language of intelligence in the first stage of the intelligence cycle, and the intelligence cycle can start. Based on this, the leaders of the intelligence services not independently, but following the initiatives of the policy makers or the orders of law do they launch the cycle. Of course, the latter solution is not and ideal situation. To fully eliminate the problem, there can be only one solution: if the policy makers (within the legal framework) consciously use the intelligence services. Based on the above, policy makers formulate RFIs towards intelligence before every intelligence cycle, because if the cycle does not originate from the initiation of the policy makers, it questions the legality of the activities of the services.

Data collectors gather information independently

Hulnick's next criticism is that data collectors function independently, do not wait for direction or RFIs; they make an effort to fill the gaps in the databases of intelligence. He supports this with the fact that information sources in the different branches of intelligence are not flexible, since sometimes it takes months or years to find the suitable sources.

When examining the above-mentioned problem, it can be stated that data collecting organizations – especially their technical elements – do not stop their activities when they answer a request for information, but continue them. However, the data collectors' capabilities and sources are not formed independently, but on the basis of the fundamental tasks, so that the subsequent concrete RFIs can be satisfied. Obviously, some foresight is needed from the part of the leaders of data collectors, but they have to work in a fixed system and have to answer the fresh RFIs. Acquiring new data sources or changing the direction of data collection can also happen in connection to the RFIs. Based on this, data collection is not a self-contained activity; it can only operate efficiently as part of the intelligence cycle. If data collection operates independently from the cycle, it engages its capacities in collecting such information that does not serve the operation of the intelligence service. However, we must mention the race between data collectors and analysts because Hulnick formulated his criticism as a data collector, and tried to highlight the priority of data collection. But this is not a good direction because all elements of the intelligence cycle are equally important. The data collector cannot live without the analyst, and vice versa. Based on Hulnick's suggestions, we also have to mention the raw information, about which the data collectors (excluding the analysts) inform policy makers. This is mostly characteristic of information acquired through

human intelligence. Hulnick considers the procedure a faulty decision because a lot of raw data and information is incomplete, contradictory or defective. He regrets that in the case of certain services (countries) this procedure is inevitable because policy makers (with propagandistic aims) make prestige out of it. In my opinion, this significantly constrains the operation of the intelligence cycle, because if policy makers receive the given information at the same time as the analysts receive it, the latter get into a difficult situation, especially when the original information is not real.

The parallel activities of data collectors and analysts

Moving forward along the lines of the previous problem, Hulnick stated that the relationship between data collectors and analysts hinders the operation of the intelligence cycle because the two most important elements of the cycle do not operate in the defined stages of the cycle, but in parallel. This is the case indeed because the data collectors do not stop their sources because of the above-mentioned reasons, while after accepting the RFIs, the analysts start to prepare the answers, during which they first examine if the information is available in the data stores. According to Hulnick it can happen that there is no need for data collectors to elaborate an answer. However, this is a highly ideal case, but analysts can still turn to data collectors to verify, actualise or complete the previous information. Yet, the parallel work does not exclude the operation of the cycle.

The lack of the sharing of information

It was also Hulnick who worded the problems connected to the sharing of information, which is present within intelligence services. Data collectors often do not share all the information with the analysts because they are afraid that the analysts do not handle information suitably and might disclose their secret sources. Mistrust has mainly psychical reasons. According to Hulnick, this comes from the mistaken belief that the analysts are introverts, while operational data collectors are extroverts. This stereotype stuck so much in the minds of the two organizations during the years that it started to hinder the operation of the intelligence cycle.

In my opinion, the mistrust and the competition between data collectors and analysts hinder not the intelligence cycle, but the efficiency of intelligence services, because for the intelligence services the information that is not forwarded by data collectors towards the

analysts does not exist, even if the raw information is directly given to policy makers, because that cannot be considered the end product of intelligence.

Some intelligence products are not the results of the intelligence cycle

According to Hulnick, the most widespread and popular products of intelligence services are the daily intelligence reports. Every policy makers' day starts with these reports. These reports are usually news selections prepared with the use of the media, and are easily comprehensible, short and concentrate on the essence. Information included in these reports do not undergo analysis and assessment, thus these reports are not prepared on the basis of the intelligence cycle.

As for the daily intelligence reports, Hulnick is partly right, but there is some analysis and assessment work in these reports as well, because selection also takes place on the basis of the constant request for information of policy makers, and the analysis and assessment procedures also appear in the method of systematisation and selection of the pieces of information, because they place the information in space and time.

The intelligence cycle does not contain feedback

During the analysis of the intelligence cycle, Lowenthal asserts that an important element is missing from the classical version of the cycle: the system of feedbacks. This has to be present not only among the different structural elements of the intelligence service, but on the part of policy makers as well, because Lowenthal thinks (based on American examples) that there is no sufficient feedback from the part of politicians.

Although the classical intelligence cycle does not depict the system of feedbacks, but the system between the structural elements of intelligence would not work if there were no interaction between them. The direction of data collectors can also be viewed as feedback. As for the users (namely the policy makers) Lowenthal is right, because they react very rarely to the products of intelligence. Feedbacks are usually only negative. However, this problem does not hinder the operation of the intelligence cycle.

The intelligence process cannot be described by a simple cycle

According to Lowenthal, one of the main problems of the intelligence cycle is that it is too simplified and one-dimensional, and that the cycle does not ensure the system of feedbacks. Lowenthal thinks that as a result of feedbacks and intervention by policy makers,

intelligence is a multi-dimensional, complex, and not a cyclical, but linear process, consisting of defined stages. Peter Gill and Mark Phythian worded their own point of view in connection with this, which viewpoint aimed at demolishing the barriers of the intelligence cycle. According to the two authors, several factors (they called them challenges) have to be taken into consideration that the intelligence cycle cannot manage, for instance the risk-based approach, the bureaucratic political system, the interactivity, the comparative analysis, the covert and clandestine actions, the technological development and the supervision of intelligence. After analysing the factors, Gill and Phythian suggests the move towards the direction of a more complex, web-based intelligence. In his study, Hulnick focuses on the description of the intelligence process as a matrix-based model.

In my opinion, the exaggerated (matrix-based or web-based) intelligence cycle would have a result that the cycle would no longer be a general theory, but a method specialised for the given activity system of an intelligence service. However, critics are right in stating that the intelligence cycle is a simplified model of the process of intelligence.

As technology developed, the process of intelligence became much more complex

Julian Richard formulated the suggestion that also appeared on the part of Warner, Gill and Phythian, that the exponential development of technology, as an effect of information society, is much more perceptible in the case of intelligence, because the basis of intelligence is information. Technological development affected the flow of information and resulted in the rearrangement of the disciplines of intelligence. The role of open source intelligence (OSINT) became more important, and the cyber intelligence (CYBINT) also appeared, and the intelligence services still do not know what to do with the latter. Aaron Brantly[37] also draws attention to cyberspace when examining the intelligence cycle, because he thinks the cycle cannot operate sufficiently in this field. In cyberspace, quick actions and reflections against attacks have a significant role.

In my opinion, as an old discipline of intelligence, OSINT is an integrated part of the data collection stage of the intelligence cycle, although it received a bigger emphasis than before, and sometimes it is able to ensure the required data alone. However, in the case of OSINT, one must be careful not to let intelligence become one-sided, since there is still a need for the data and the information collected by the other disciplines of intelligence to

[37] Aaron Bartley earned his PhD at the University of Georgia, where he engaged himself in international relations. He served at the United States Peace Corps in Ukraine, then worked as a consultant at the organization during the Arab Spring.

maintain an efficient and productive work. However, the case of CYBINT is different, because it is essentially not an information gathering discipline of intelligence; as for its function, it can rather be compared to covert and clandestine actions.

The five elements of the cycle do not cover the process of intelligence because some elements are missing.

Kristan Wheaton[38] examined the stages of the intelligence cycle and their content in the different strategies, doctrines and educational materials of different intelligence services. He found that in U.S. literature, the intelligence cycle consists of four-six stages, and these have altogether 19 different elements. Only the stage of data collection was present in every version. However, these elements can be compared to the five stages of the classical intelligence cycle. The first stage is characterised by requests, needs, control and design. The second stage unanimously consists of data collection. The third stage is characterised by processing, evaluation, summarising and explanation. The fourth stage consists of analysis and the preparation of reports, while the fifth can be characterised by dissemination, utilization, integration and feedback.

In the literature, besides the fundamental concepts, new elements or stages occur in the intelligence cycle, which did not form parts of the classical version. These include the filling of the data stores and databases, utilization and application, and the execution of action. When examining the content of the new stages, one finds that these all have been parts of the intelligence cycle, where they have been a part of one of the stages. For instance, the filling of data stores and databases takes place in the stage of data processing and systematisation, while utilization, application and the execution of action can be connected to dissemination, but these do not directly form a part of the intelligence cycle because they depend on the decision of the user.

[38] Kristan J. Wheaton is an associate professor at Mercyhurst University in Erie, Pennsylvania, where he teaches intelligence studies. He served in the U.S. Army, where he specialized in security problems, analysis and assessment methods and game theory. He was a military attaché in Europe, and worked for the intelligence departments of the U.S. forces stationed in Europe.

Conclusions

The researchers of the theory of intelligence consider the above-mentioned ten problems as the criticism of the intelligence cycle. Most of the critics deal with the practice of intelligence, because they do not criticise fundamental theoretical questions. It might seem from my answers to these criticisms that I would like to protect the intelligence cycle, but this is not the case, because I agree that it does not cover fully the practice. However, I think that the cycle is a theoretical reflection of the intelligence process, and not its practical realisation. In this regard, I partly agree with Robert M. Clark, who said that the intelligence cycle became rather a theoretical concept than a practical tool. However, Clark thinks that the gap between the theory and the practice is growing, but in my opinion, the theory and the practice should be examined from different viewpoints. For instance, in the case of practice, it is the problems, the mistakes, the errors and the characteristics within intelligence that cause the deviation from the intelligence cycle. When examining the mistakes in intelligence [as I elaborated on the topic in my study entitled *Korszerű elemző-értékelő eljárások alkalmazása a hírszerzésben (The Use of Modern Analysis and Assessment Methods in Intelligence)*[1]], it can be stated that most of the mistakes of intelligence is caused by the deviation from the intelligence cycle; for instance, the lack of the sharing of information. As for the intelligence cycle, one can state that on the theoretical level, the intelligence services still operate along the lines of this method. The difference between the theory and the practice is that the theory provides a framework for the efficient and productive operation of a given intelligence service, but during the practice, the possibilities, the capabilities and the situation of the service have to be taken into consideration, because the activities of an intelligence service employing thousands of people cannot be compared to that of a service employing a few hundred employees. The activity systems of intelligence services, and within that, the elements of the process and the relationship of the structural elements evolved through several decades, thus they can only be altered when some paradigm changes take place in the intelligence services.

In my opinion, the intelligence cycle continues to provide a sufficient theoretical support to the professional activities of intelligence services, thus it remains a key element of efficiently training the intelligence personnel. However, I think that it is necessary to further analyse the above problems to improve the Hungarian theory of intelligence.

[1] Dr. Csaba Vida: *Korszerű elemző-értékelő eljárások alkalmazása a hírszerzésben*, pp. 77-86.

References

- Dr. CSABA VIDA: Művészet vagy tudomány: Gondolatok a hírszerző elemzés-értékelésről (Art or Science: Thoughts about Intelligence Analysis and Assessment)
- KRISTAN J. WHEATON: Let's Kill the Intelligence Cycle.
- ROBERT R. GLASS – PHILLIP B. DAVIDSON: Intelligence is for Commanders
- ROBERT M. CLARK: Intelligence Analysis: A Target-centric Approach
- MARK M. LOWENTHAL: Intelligence: From Secret to Policy
- ARTHUR S. HULNICK: What's Wrong with the Intelligence Cycle?

GEOPOLITICS

DR. ZOLTÁN BÁCS

1815-2015: TWO HUNDRED YEARS OF DIFFERENCES IN CERTAIN IDEOLOGICAL AND POLITICAL TERMINOLOGIES AND POLITICAL INSTITUTIONS BETWEEN EUROPE AND LATIN-AMERICA

Abstract

In the political historiography based upon the European parliamentarian system, it is a permanent problem how to identify the political movements, tendencies and parties of Latin America; how to compare them with the existing European prototypes; and what can be the basis for their classification? What is the role of the Spanish and the Portuguese colonial traditions in Latin America? Is it true that the liberalism constitutes an obstacle to political and economic development in the ex-colonial countries?

Keywords: reaching independence, European models, North American and Latin-American democracy, military and civilian governments, right and left, central right and left, radical and liberal

The conditions and circumstances of achieving independence and choosing a proper way of development, as well as the partial and selective refusal of the political traditions of the European colonizers in the period of setting up the new legislative and institutional basis – in accordance with the traditions and culture of the given local community – exclude the full compatibility with the old European models, but preserve their certain elements in the new local institutions. If we accept this partial incompatibility both in theory and practice, we have to agree that the European basic categories like right or left, central left, central right, radical and liberal are not fully applicable in the Latin American, Asian and African countries, or at least not in the traditional sense.

Where does this incompatibility come from? How can it be explained and what kind of consequences it has? Is it possible to draw any concrete conclusion applicable to the region or to a major number of countries? This paper is trying to give answers to these questions.

In the case of some mostly mono-national European states or states with some national minorities of European origin, the achievement of independence never emerged as a permanent fundamental question. These states have been independent since the beginning of their statehood, or occupied partially or entirely by foreign powers only in a certain period of their history.

In the case of other European states the creation of the institutional and legal base of the state became possible after having conquered the political, economic and military independence by leaving a major regional or sub-regional power.

The ways of smaller homogenous national states or states with some national minorities on their territory leading to independence have been different. The independence has been the result of activities and struggle of smaller or larger popular groups. These struggles affected the larger part of the society only peripherally. The masses did not participate actively in the political struggle or in the armed clashes, they gave only a passive support or remained inactive or became victims of the collateral atrocities.

The ways of Latin American, Asian and African countries leading to independence have been more complicated. While under the circumstances of the feudalism in Europe, the independence was achieved in a struggle against the squires, in Latin America, Asia and Africa it was conquered by the separation of the colonies from the colonizers. We should not forget that while the independence wars against the feudalism were going on in Latin America, in Europe the bourgeoisie had already established its firm dominance.

The independence of the colonies was achieved by different ways. In general, the independence of Venezuela, Uruguay, Argentina, Chile and other countries in Latin America was conquered in an armed struggle against the colonial Spain, which led to the immediate change of the form of government in these countries. It is also obvious how important was the influence of the Declaration of Independence of the United States, when the forming of the institutions of these new-born republics was in progress. The exception was the case of Brazil, where the independence was conceded by the king of the colonial Portugal.

The royal decree of John the Sixth, King of Portugal proclaiming his son Peter the first sovereign of the overseas colonies meant only the creation of the legal frames and the legalization of an already existing situation. Neither the social situation nor the influence of the rich landowners – who were interested in the separation from the motherland – were

changed; they remained the most powerful and important stratum of the society. The absence of new antagonisms after achieving the independence created a specific situation, where the new state could apply the old political structure with its system of institutions and the form of administration used in Portugal.

In Asia and Africa, the new order emerged as result of a long process of struggle of wide popular movements with the active participation of the majority of the social strata against the motherland and her institutions installed on the colonies. After achieving the independence during the period of consolidation of public administration in the three continents, the influence of social movements, groups and strata which played an important role in the liberation remained significant, even determinant over the newly created political institutions and the structure of power. This influence could have been the origin of the national character of the political life of every country; however, the forms and appearance of this national or nationalist approach in the institutions and the political establishment are different in each country. This general historical heritage is the explanation why all the political forces including those which fought for the changes and even those which fought against them define themselves as political successors of the freedom fighters who achieved the independence. The reminiscences of the independence war i.e. the historical roots of the political heritage are more than frequently referred to by political or social reasons, when an urgent need to manipulate the masses emerges. These traditions are a massive obstacle for ideological groups and parties formed under foreign influence as alien body in these countries. Sooner or later every society rejects these political ideological creatures as something incompatible with local traditions and customs.

During the formation of their system of political institutions, many Latin American countries opted for the model of the most powerful rival of their ex colonial country – Spain – , but they tailored it to their own conditions. The institutions of the North American democracy as the division of power, the two chambers' system of legislation and the control over the executive power have been integrated into the institutions of the Latin American republics.

The conflict between using European institutional models by the Latin American countries and the inability of the traditional European political terminology to describe local political and social tendencies in Latin America is imminent. In the classic democratic institutional models, the division of powers is determined by the Constitution and the legal

status and the competences of every power branch are regulated by legal documents of inferior rank, generally by laws. The exact and clear regulation of the competences of the power branches helps to avoid the counter-democratic concentration of power by abusing the democratic principles and electoral practices on behalf of any interested group.

In Latin America – despite of the formally separated power branches – the branches' efficiency is very low, due to the failures of the legislation regulating their status and functions. In many cases, there are not legislative acts sanctioning the abuse or overpass of the juridical frames. The respect and the nimbus of the leader in the presidential republics constitute a tradition since the independence wars. It makes easier that a leader of a political group – elected or appointed – abuses of the power received as a result of the democratic elections. In such a case, the leader can use the weaknesses of the controlling mechanism of the legislation over the executive power, which can lead to obtaining a majority in the Parliament, guaranteeing him almost unlimited power, in violation of the democratic principles. Once having this power, the leader is in a position of controlling the legislation and influencing on the system of justice. Thus, the political elite will be able to consolidate its might and power in economy and politics, and will be able to manipulate the media and the masses, to increase its own acceptance amongst the voters, and at the same time, will have the tools to keep the opposition as far as possible from the media and the economic and financial resources. The political elite can ignore the objective economic and financial principles when takes politically motivated tactical decisions that may be harmful for the strategic goals. Here are some examples of the strategically counterproductive, politically motivated tactical decisions: the course of the Argentinean peso had been kept artificially high against the US Dollar at the beginning of the first years of the 21st century, giving a chance to finance large scale state investments by unsecured bonds. During this period, the market prices had been regulated by governmental decrees. These methods are the best known ones used frequently by the representatives of the Latin American populism and the contemporary state capitalism.

Another typical Latin American phenomenon hardly understandable for the Europeans is the systematic return of populism. This topic has been analyzed in many publications so I do not consider it is necessary to develop this topic in the present article.

It is also interesting to observe that the hierarchical attitude – surviving since the colonial times and the period of the independence wars – has been preserved even in the times of the democratic governments. The numerous negative examples of military governments

encouraged on one hand the strengthening of the popular wish for lawfulness and efficient democratic institutions, on the other hand they led to significantly diminishing the prestige of the military and the armed forces in general. The civilian governments which came to power after the military ones – instead of strengthening the lawfulness by creating a smaller number of new and more efficient laws or by introducing a multilevel regulation – approved a huge number of laws**.** If the laws were violated a lower level regulation act could have been sufficient. The same happened in Argentina where laws had been created to set up mixed intergovernmental commissions or to sign an intergovernmental treaty in the fields where it could have been sufficient to sign an agreement between ministries.

Another frequently met phenomenon in Latin America is the refusal of liberalism as an ideology. The reasons for this could be a good object for further investigation. While the European mentality considers the liberalism as a boosting factor for economic, social, political, juridical and cultural development of the widest social strata, in Latin America the liberalism is seen as the opposite of this. It is identified as the obstacle to the national social and economic development, it is an alien body; it is the ideology of the US penetration of the twentieth and the twenty first centuries into the continent. It was almost emblematic how vehemently the Argentinean President of that time, Néstor C. Kirchner had been criticizing this ideology during his presidential campaign of 2007. One of the possible reasons for the refusal of liberalism in Latin America can be that there has always been an antagonism between the theory of centralized Latin-American governance and the ideology of liberalism. With other words: while the liberalism applied in Europe and the United States has contributed to social and economic development under the conditions of wide social pluralism and internal and external prosperity, under the conditions of Latin America this pluralism has been a powerful menace to the elite interested in keeping the power in their hands and in preserving the hierarchical national system of governing. It is really strange: the Kirchner – Fernández governments identified several times by European political analysts as governments of the left, definitely refused the liberalism. The conclusion confirms the hypothesis at the beginning of this article: the European political terminology is incompatible in many cases with the political processes going on in Latin America, it does not serve at all or it serves with strong limitations only to describe and identify the processes and tendencies there.

The interest to concentrate the power – regardless of the geographic situation of the country – is in obvious contradiction with the traditional democratic principles of governance based on pluralism i.e. the rotation of governments of different ideologies from the right to the left always within the frames of parliamentary democracy. If we accept this affirmation, it seems to be inappropriate the ideological division of conservative vs. left, because the elite already in power is not entirely motivated to take decisions upon the electoral and governmental programs influenced by and elaborated in harmony with the ideological background of the dominant party or by the wish to represent trustworthily the interests of the voters. The real motivation is to achieve and keep the plenty of power from the highest level of the federal or central government down to the local administrations. The references to the historic and national traditions and the use of slogans full of ideological revelations are the compulsory elements of the show in the struggle for power. The real question is: from which social stratum, from which class the elite chooses its allies in order to implement the tactical and strategic goals, how long this alliance will persist, will the elite involve its ally into the real political cooperation or it will use this alliance only to maintain its power and influence its ally? The definition of the national and international context and the group of countries, the international political, economic and financial organizations and institutions which will be invited or approached to help to implement the aims of the elite in power is much more important than to define any ideological attribute.

Conclusions

Based on the above described situation, it seems that the concentration of power and the strongly centralized governance – besides being a permanent feature of the governing elite in many Latin American countries – is one of the factors which provoke the new rounds of the economic and financial crisis cyclically hitting the economy of many Latin American countries. This political practice cannot be identified as left or conservative; it has nothing to do with the traditional European classification of parliamentary parties or ideologies, and the least with liberalism.

INFORMATION AND COMMUNICATION SECURITY

DANIEL TOKODY, DÓRA MAROS, GYÖRGY SCHUSTER, ZSOLT TISZAVÖLGYI

COMMUNICATION-BASED INTELLIGENT RAILWAY IMPLEMENTATION OF GSM-R SYSTEM IN HUNGARY

Abstract

The GSM-R system, which is not yet fully implemented in Hungary, will undoubtedly bring about significant changes in the Hungarian railway. These changes give rise to numerous questions – even to the specialists – in connection with its future operation. The purpose of this article is to assess the present state of the implementation of the system, to outline the existing and the pre-planned GSM-R systems in Europe, and to present the international regulations and requirements, ensuring the reliable operation of the system and its interoperability between countries.

Keywords: intelligent transport system, telematics, primary and secondary communication, vehicle to vehicle communications, GPS, interoperability, RTMS, uniform radio system, redundancies, quality requirements, the state of the Hungarian railway network

Introduction of the Intelligent railway system

At present, the communication used on railway networks is based on rather inhomogeneous technical solutions and systems in Hungary and abroad, too. Meanwhile, international trends and requirements are oriented towards the implementation of intelligent transport systems, as defined in the European Union Directive 2010/40. “Intelligent Transport Systems (ITS) are advanced applications which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and ‘smarter’ use of transport networks.” [1]

The basic principle of the directive is the need to develop a system that ensures the interoperability of the railway communication systems in Europe. In the years since 2010, the conception of ITS has been further developed, and the uniform GSM-R communication

system, which is already operational in many European countries, and which is being implemented in Hungary, will bring significant and progressive changes in the reliability of railway transport.

Traditional railway systems are unable to help users perform their work in a better and more reliable way. At present, the solution of rather complex processes is based on human knowledge and experience, even though, in many cases, the learning of these processes and certain decision-making abilities could be taken over by modern info-communication systems.

Intelligence-based communication systems are used in modern networks, because highly complex processes, which would require significant human resources, can be made safer and more efficient this way. Human decisions are often based on experience and, many times, on intuition, without analysing the situation in full detail or considering all aspects in the decision making process. In many cases, the decision making is affected by instantaneous human behaviour, tiredness or poor concentration. Intuition might be too much to expect from intelligent railway systems, but there is a practical possibility of the heuristic approach to its processes. “Intelligence needs to be used in process controlling systems, when at least one of the controlling tasks requires intelligent problem-solving. In this case we can talk about an intelligent controlling system.” [2]

Telecommunication and informatics, or the solutions of telematics form an indisputable part of today’s railway networks. The basic components of these systems are telecommunication and the related technologies and protocols, such as GSM-R. The use of wireless technologies – due to their mobility - can now be regarded as a basic solution in case of railway communication systems. The following figure shows the relationship between telematics and intelligent transportation systems.

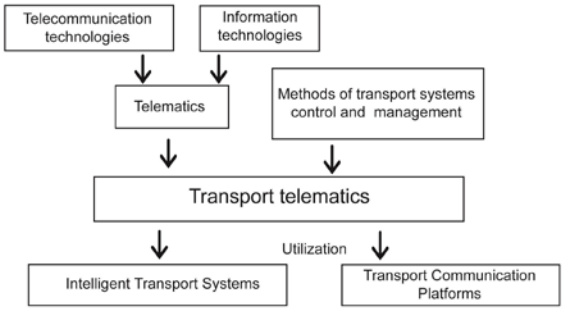

Figure 1.

The relationship between telematics and intelligent transportation systems [3]

By using sensors and various controlling and regulating elements, intelligent railway systems achieve automatic (without human intervention) and agile resource management in a large and complex system. Therefore, "The concept of intelligent railway includes the advanced automation systems, the continuous monitoring of the railway rolling stock in terms of all locomotives and wagons, the self-explanatory visual and acoustic passenger information service both on board and at the station. The selection of the location of a station and the designing of station buildings is also an important part of the intelligent systems. A system can include any theories, tools or developments that aim to implement an intelligent rail system." [4]

Communication is, of course, essential for the operation of intelligent systems, but to ensure operational security and continuity in most of the cases, it is necessary to establish a primary, and, in case it fails, a secondary communication network. In order to ensure maximum security, the two systems should have as many different features as possible, and they should be largely independent of each other. With regard to railway, the uniform GSM-R system can be mentioned as primary communication, while secondary communication may be ensured by those solutions that can be best adapted to the technology, such as the WLAN, Zigbee, IR and RF communication.

In the case of intelligent transportation systems, Vehicle to Vehicle (V2V) communication can also be achieved. By using this technology, the number of vehicle collisions can be minimised, and it will be possible to share any detected incidents that might endanger traffic. V2V communication can be achieved by different solutions, for example by the so-called ad hoc, i.e. self-organising, mobile networks.

Communication within the vehicles is also an important part of information exchange in ITS. Today railway vehicles are equipped with special sensors, such as thermometers, humidity gauges, odometers, tachometers, etc. Strain gauges are used for diagnosing the critical points of strain in the vehicles, or for dynamically estimating the utilisation of railway carriages or wagons. In many cases, communication of these sensor networks is ensured by wireless solutions, such as the communication interface of Zigbee.

A further advantage of intelligent transportation systems is that they can communicate with the global positioning system (GPS), or other systems of geo-informatics and digital topography. Nowadays, increasingly interconnected and, from the point of information

sharing, more and more dynamic communication systems are needed in the entire range of transport in order to achieve the final goal of creating an intelligent environment for everybody.

Background of the implementation of the GSM-R system in Hungary

In recent decades, the countries of the European Union have forged stronger economic ties with each other. These commercial changes have shown the direction for the development of a more open and interoperable railway system, and for the unification of various transport systems. Because of the different telecommunication, controlling and technical systems in the countries, the railway sector in Europe is not efficient enough to compete with other forms of transportation, especially with road transport, therefore the European Union appointed various organisations to issue common directives in order to ensure interoperability through the development of the European Rail Traffic Management System (ERTMS).

The bases of the development of the ERTMS can be originated back to 1995, when the International Telecommunication Union (ITU) allocated new frequency bands for railway communication in the GSM frequency range between 876-880 MHz and 921-925 MHz on 19 channels. The EIRENE (European Integrated Radio Enhanced Network) and MORANE (MObile radio for Railway Networks in Europe) documents were issued between 1995 and 2000 in order to set the technical requirements of the new system. In 1997, a memorandum of understanding was signed by 32 European railway administrations to develop the GSM-R system as part of the ERTMS. The European Parliament and the Council passed Directive 2008/57/EC on the interoperability of the railway system within the Community in 2008, and then in 2012 Decision 2012/88/EU was taken by the European Commission on the technical specifications for interoperability relating to the control-command and signalling subsystems.

The ERTMS consists of three basic components:

ETCS – European Train Control System – includes the control of train traffic, the management of movement permits, automatic train protection and interfaces to the security equipment.

GSM-R - Global System for Mobile Communications – Railway – The "communication element" of the system, which enables speech transmission between the controllers, trains and the members of the operating staff, and provides bearer capability for

ETCS L2 or higher level data transmission to ensure wireless communication between the trains and the central elements of the ETCS.

ETML – European Traffic Management Layer – standardises the operational levels that are necessary to maintain train traffic, and controls the management of the data related to railway schedules and train traffic.

The conference organised by the UIC - International Union of Railways – in Istanbul in April 2014 gave an overall picture of the already operational and the planned GSM-R networks in the world. According to reports, the railway networks of thirteen European countries connected to the international GSM-R roaming network in 2014 were Austria, Belgium, Switzerland, the Czech Republic, Germany, Denmark, Spain, France, Italy, Norway, the Netherlands, Sweden and Slovakia. At present, the introduction of the GSM-R systems is in the implementation or planning phase in many other European countries.

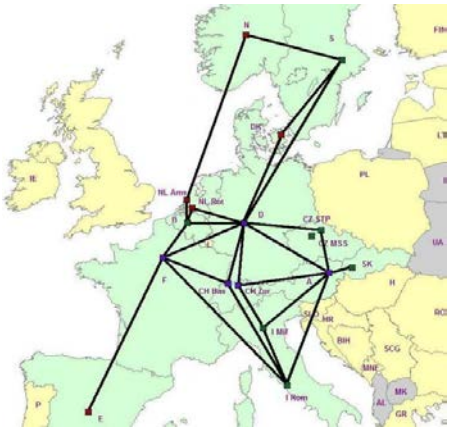

Figure 2.

Connections of the European GSM-R systems at present [7]

According to the latest reports, in the period between 2010 and 2014 the length of railway lines equipped with the ERTMS almost doubled, while the number of vehicles using devices that are compatible with the system increased by approximately two thirds.

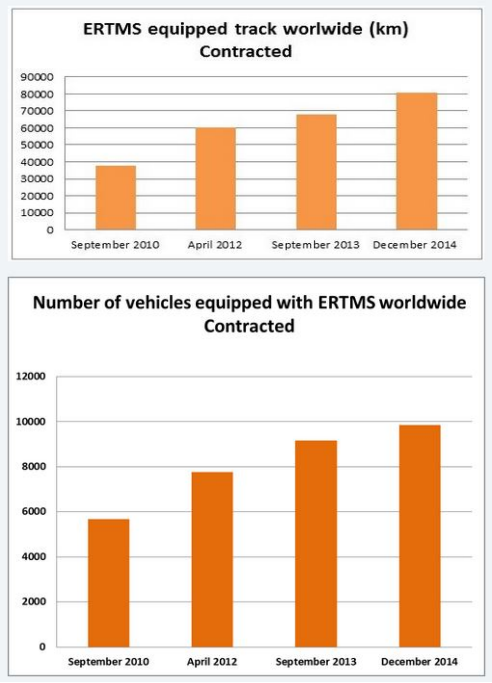

Figure 3.

The number of railway sections and vehicles using the ERTMS [8]

The GSM-R roaming operates similarly to the traditional GSM network roaming. As all railcars have been equipped with GSM-R compatible devices, communication on cross-border railway lines has become continuous, uniform and, due to the redundant network implementations, more reliable than the formerly used, mostly analogue solutions. The continuous operation and the uniform display and communication interfaces of on-board radios provide full IT support for train drivers.

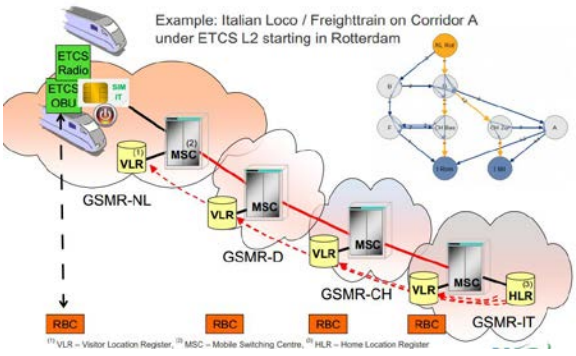

Figure 4.

Roaming situation in GSM-R [7]

In the above example a train set, which is in Italian ownership, travels from the Netherlands through Germany and Switzerland to the Italian destination. Between the GSM-R systems implemented in each country according to uniform technical requirements, the roaming contracts ensure the seamless connection on the entire route.

Changes in the technological background of railway telecommunication might seem to be rather slow, considering that new standards and recommendations are being implemented continuously. At the introduction of the new systems, the service level and the planned life cycle of the systems presently in operation must also be examined. In Hungary, the currently operating rail line radio systems are 25-30 years old, manufacturer support is no longer provided for the fixed network, and the maintenance of radio centres is becoming more and more difficult. The analogue radio system operating in the eastern part of the country can be accessed by anyone, and it is not interoperable with the international systems. The 450 MHz radio system, which was introduced in accordance with the recommendation UIC 751-3, already adopted the international principles, but it could not become internationally uniform because different supplementary operating modes were used in each country.

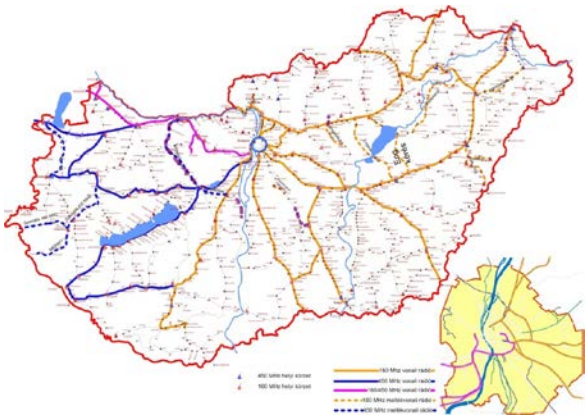

Figure 5.

The present analogue radio systems of MÁV

Over the last years, the GSM-R system has gradually gained ground in the neighbouring countries. Only vehicles equipped with GSM-R train radios are allowed to enter the territory of Germany and Austria. It was the result of these external circumstances that the multi-norm train radio, which can operate both in analogue and in the GSM-R band, had become a basic requirement, even before the tender for the implementation of the GSM-R network was called.

Phases of the GSM-R implementation

According to the plans, the project for system implementation divides the development of the GSM-R network into two phases.

In the first implementation phase (first phase) the Hungarian GSM-R system covers five railway line sections of altogether 905 km by the end of 2015.

1st line: Budapest – Székesfehérvár, length: 117 km,

2nd line: Budapest – Lökösháza and Szajol – Püspökladány, length: 292 km,

3rd line: Győr - Bajánsenye, length: 184 km,

4th line: Budapest – Hegyeshalom, length: 187 km,

5th line: Sopron – Szentgotthárd, length: 125 km.

The first implementation phase focuses on the international transport corridors which should be equipped with ERTMS in order to ensure interoperability, as set in Decision 2012/88/EU, also covering the related main railway lines. All networking, connecting and operating subsystem elements needed for the support of the GSM-R network, as well as all telecommunication infrastructure required to ensure the radio coverage of the selected railway line sections and the central controlling equipment (the base station subsystem, approximately 137 antenna towers, optical cabling, transmission technology, power supply, protection of property and the dispatching system) is implemented in this phase.

In order to help migration to the GSM-R network, the following mobile terminal equipment will be purchased in the first phase: 1280 (shunting – OPS, operating – OPH, general purpose – GPH) hand radios, 100 two-norm (UIC-751-3 450MHz and GSM-R system) train radios and 74 desktop fixed radios.

In terms of coverage and the number of mobile and fixed terminals, the first phase will not bring the complete change of the analogue radio systems, as, in order to take full advantage of the GSM-R system, it is necessary to equip all the vehicles operating on the line sections with GSM-R train radios, and to integrate the services provided by the system with the communication technologies of the Hungarian railway companies. The Hungarian GSM-R system is expected to follow the international experience, which shows that migration to the GSM-R systems implemented after 2010 lasts 3-5 years on average, therefore, this amount of

time is required for the complete transition to the new communication system. The first phase was completed by the end of 2015.

In the second phase of the GSM-R implementation, approximately 2150 km of line sections will be covered.

Figure 6.

Development of the A GSM-R network between 2014 and 2020 [5]

With the geographical expansion of the GSM-R coverage, which is expected to take place in the second phase, the question will arise: What should happen to the analogue radio systems?

The analogue radio systems of MÁV will only change, if the existing networks are replaced by GSM-R equipment in geographical coverage and functionally, both on the sides of fixed radio operators and mobile train radios. There are different migration strategies for the replacement of analogue railway radio networks with the GSM-R system.

Network-oriented migration (double infrastructure) – In this case migration can only be started when the GSM-R implementation has fully covered the analogue radio systems. At the maintenance of the vehicles, the existing analogue train radios must be replaced with GSM-R train radios, so the analogue and GSM-R radio systems will operate in parallel until the last train radio is replaced.

Mobile-oriented migration (with multi-mode train radio) – The most important element of this solution is that all locomotives be equipped with multi-mode train radios,

which support both the analogue and the GSM-R radio systems. In case of the mobile-oriented solution, the time of migration depends on the pace of the installation of the multi-mode train radios in the rolling stock. Ideally, if all vehicles are equipped with train radios that support both the analogue and the GSM-R modes, the GSM-R system sections can be put into operation continuously, and the analogue radio systems can be switched off by sections. When scheduling the installation of the new train radios, priority is given to the vehicles which operate mainly on the sections covered by the GSM-R. At the end of the second GSM-R phase, the analogue systems of the main lines are expected to be switched off.

The GSM-R shunting function needs special attention, as it is substantially different from the traditional analogue solutions used locally, therefore multiple tests and examinations must be carried out in accordance with international standards, before it can gain permission for railway operation. Furthermore, the radio installation is also problematic on the line sections (branch lines) that are not covered by the GSM-R system. Should the tried-and-tested 450 MHz system be installed, or should a new national roaming contract be made with a public GSM service provider in order to take advantage of the newly purchased GSM-R train radios and mobile devices? In this latter case, however, it is not sure to what extent the public system will be able to support certain railway specific services.

Coverage requirements

The GSM-R network development is based on the European requirements, which must be strictly followed in order to achieve uniform interoperability all around Europe. The most important technical requirements are described in the EIRENE Functional Requirements Specification Version 7.3.0 and the EIRENE System Requirements Specifications Version 15.3.0. The requirements define several types of coverage, depending on what traffic and technological needs may arise in the given area or line section in the near future. The FRS 15.3.0, for example, defines, among others, the requirements of the minimum received signal levels for different coverage solutions.

Radio layer redundancy

Single coverage will be provided on the lines marked as L1. These are the lines on which the ETCS, which requires double coverage, will be implemented in a later project. Therefore, the present phase only prepares for the future infrastructure, but later this

infrastructure can be expanded for the implementation of the second layer without replacement or restructuring.

The ETCS system requires a fault-tolerant and high-availability (99.98 %) telecommunication network. In the case of a line section equipped for ETCS L2, the L2 or double-layer radio coverage-must be applied. In this case there are two parallel layers, where layer ‘A’ can fulfil the radio coverage requirements on its own, but a redundant layer, layer ‘B’, has also been added with the same coverage parameters. If there is an outage of cell service on layer ’A’, the cell of layer ‘B’ takes over the traffic (Figure 3). In case of handovers (radio cell switch during speech connections or at the signal exchange for establishing or breaking down speech connections) and cell resets, the mobile devices give priority to the neighbouring cells of layer ‘A’. According to the network configuration, the device stays on layer ‘B’ only until the cell of layer ‘A’ starts operating again. In order to ensure the independence of the two layers, two outdoor cabinets are deployed, which follow a uniform design in order to make the installation and the future operation easier.

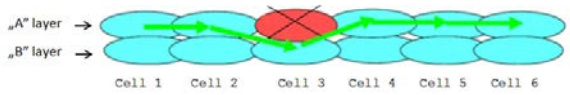

Figure 7.

The concept of two-layer (L2) coverage

A system complying with the above parameters must be developed on the 19 frequencies that are available in the GSM-R frequency band, where it is easier to achieve the required coverage than the quality, which is determined by interference. In this term, the Budapest environment causes the biggest problem, because of the high density of the cell network.

In the areas of bigger stations, further capacity cells must be used to serve the predicted traffic. These antennae are generally shorter than the antennae of the main line cells, so that the coverage and the caused interference can be kept at the appropriate level. In order to increase redundancy, each radio layer must be served by a separate antenna system.

Redundancy of network elements

The base stations connect to the base station controllers (BSCs) through redundant transmission routes. The two BSCs operate by load sharing, but if any failure occurs in one of the BSCs, the other can take over its traffic. In case of double coverage, the stations of the individual layers are separated according to the BSCs, and the base stations of two parallel layers can only be controlled by the same BSC, if the other BSC fails to operate.

At the location of a base station the two layers are served by separate antenna systems.

In the GSM-R network, redundancy is ensured on multiple layers, and it has two types. Physical redundancy includes double coverage, the use of an optical ring network or the system element specific concept of 1+1 or N+P element level redundancy, where the redundant elements fully take over the task of the default unit without causing interruption in the operation of the whole system or in a sub-system. The other type of redundancy is logical redundancy, which means the redundancy of running control processes, applied data bases and route sets.

Redundancy must be ensured not only on the level of system elements, but also in the form of geo-redundancy, which means that the central network elements must be stored in separate locations, in order to ensure the full service of the system, in case an unexpected event (e.g. natural disaster) happens at one of the locations. This is achieved by building two core networks, one in Budapest (location M1) and the other one in Székesfehérvár (location M2), which also enables the simultaneous and redundant functioning of group calls and their recording. The unique user identifications and other data that are necessary for the management of calls are stored in the Home Location Registers (HLR), which can also be found at the above-mentioned locations. The HLRs contain the entire user database, but the users are divided in a way that in normal operation one of the HRLs provides information about one half of the users, while the other HLR about the other half of the users when making connections. If one of the HLRs fails, the whole database is activated in the other HLR, in order to prevent any disruption in the connection between the network and the terminal device, which may be caused by lack of information.

Quality requirements of the GSM-R network operation

The Decision 2010/713/EU of the European Commission describes the modules for the procedures for assessment of conformity, suitability for use and the EC verification to be

used in the technical specifications for interoperability adopted under Directive 2008/57/EC of the European Parliament and of the Council.

In accordance with Article 18 (4) of the directive on interoperability, only an internationally registered certifying organisation (Notifed Body, NoBo) may issue an "EC Certificate of Conformity" on the compliance with the quality requirements defined in the mandatory normative documents, which cover the quality assessment of the individual sections, the related subsystems and, after implementation, the entire network. The present certification activities include, among other areas, the GSM-R system for both speech and data communication, in a way that allows the future development of the ETCS L2 system without any modification or further certification of the GSM-R network.

According to the SH1 module defined in the Decision, the certification activities include three basic areas: assessment of the quality control system, design examination and the verification/certification of subsystem testing.

During the certification process special attention must be paid to the testing of operational parameters of the network. The quality requirements are defined in the above-mentioned EIRENE and MORANE documents, as well as in the specifications of the European Telecommunications Standards Institute (ETSI) and the International Union of Railways (UIC). The test plans are prepared by the experts of the implementing partner, and a special measuring wagon is used for the purpose of testing the GSM-R-based IT services on the railway lines. The prior technical setting of the test environment must be done in a way that it should not change during the tests either in terms of radio coverage or in the related network services and network elements. This is strictly required in order that the NoBo accept the validity of the measured parameters and, in case of compliance, issue a certificate for the individual subsystems as well as for the entire system. With regard to the hundreds of technical parameters defined in the normative documents, the testing process is the most complicated and most resource-consuming (time, money, experts) part of the certification procedure. Specific international requirements are defined for test procedures, for the measuring environment and for the number of measurements; therefore the acceptance of test plans is also a part of the certification procedure. The certificates issued by the NoBo ensure the compliance of the GSM-R system with the European standards, the flawless operation and high reliability of the system from all technical aspects, and the conditions of interoperability.

Conclusions

The standards of the European Union have brought the necessary changes in the international and the Hungarian railway communication. The first phase of the Hungarian GSM-R network was expected to be completed by the end of 2015, which will bring a new modern era in the Hungarian railway communication. The present article has outlined the features of the connected lines that are already operational at international level, the phases of implementation, and the state of the Hungarian network, its quality requirements and its future prospects. Without aiming to give a complete overview, the present article has also described some solutions to the quality assurance of network operation and some issues of complying with the technical requirements.

References

[1] "ITS Directive 2010/40/EU, DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010 on the field of road transport and for interfaces with other modes of transport", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF

[2] Lakner Rozália, Hangos Katalin, Gerzson Miklós, „Intelligens Irányító Rendszerek", ISBN 978-963-279-511-9, Veszprém, University of Pannonia, 2011. p. 10.

[3] Mirosław Siergiejczyk, "Communication Architecture in the Chosen Telematics Transport Systems", http://cdn.intechopen.com/pdfs-wm/37575.pdf

[4] Tokodi Dániel, Dr. Schuster György, Ihász Jácint. "SMART Rail technológiák lehetőségei, az intelligens vasúti hálózatok kialakításának kérdései", Vezetékek Világa 2014/2. pp. 11-15.

[5] Csilling László. "Kormányzati Informatikai Fejlesztési Ügynökség, GSM-R a 160 km/órás vasútért" slide show presentation, 2013.11.07. Infotér konferencia.

[6] Achim Vrielink, Dirk Brucks. "GSM - R Interconnection & Roaming situation, Future plans", 2014. http://www.ertms-conference2014.com/assets/SESSION-RESENTATIONS/S6/20140304UIC-ERTMS-World-Conference-2014.pdf

[7] Unife - the european rail industry, "ERTMS Deployment Statistics – Overview. 2010 – 2014." http://www.ertms.net/?page_id=58

[8] Fregan Beatrix - Fábián Éva: The special relationship for European integration, In: Fekete Károly: Kommunikáció 2010. 397 p. (ISBN:978-963-7060-21-2)

[9] Fregan Beatrix: Un personnage éminent de l'historie de la Défense Hongroise, HÍRVILLÁM = SIGNAL BADGE (ISSN: 2061-9499) I: (1) pp. 302-304. (2010)

[10] Rajnai Zoltán Bleier Attila: Structural problems in the fixed communication systems of the Hungarian Army In: Fekete Károly: Kommunikáció 2009. 346 p ISBN

[11] Rajnai Zoltán: Les radios de l'avenir pour les armées In: Fekete Károly: Kommunikáció 2004, pp. 269-273

GERGELY KRISZTIÁN HORVÁT

LEVERAGING IFORMATION SECURITY STANDADS TO COMPLY WITH HUNGARIAN L. Act 2013

Abstract

In this article, the problem of setting up of an information security control framework in a government or municipal organization is discussed from compliance and management perspectives. There are generally accepted information security control frameworks which can be the foundation of own control framework. Every organization is different in size, budget, the relevant legal and regulatory requirements, and risk apptetite. The role of the information security officer is to take these into account, prepare a detailed risk analysis and design a work plan to keep the risk at an acceptable level, have the plan approved by the head of the organization and implement the plan; ideally using an accepted information security control framework or even more frameworks. A method to leverage more frameworks to comply with Hungarian L. Act 2013 is presented in this article.

Keywords: information security; compliance; ISO/IEC 27001; NIST SP-800-53; Cobit 5 for Information Security; compliance requirement mapping;

1 Information Security Compliance

1.1 Information Security Regulations

Information is processed using partly or fully automated information systems in digital government systems. Dependence on information automated information systems is high. Governments and authorities around the world have decided to mitigate these risks via setting explicit rules, issuing laws and baseline information security requirements.

Development of the regulations and the different security control frameworks have evolved in parallel. In some countries regulations preceded the control frameworks, but in many countries the best practice control frameworks are referenced by laws and regulations.

The importance of timely, accurate and reliable information is increasing in the Hungarian governmental and municipal sector as well. This alone would justify that the Hungarian Parliament issued separate law on electronic information security on April 15th in 2013. The fact that a number of significant cyber security incidents occurred even within the

doors of ministries in recent years speeded up the legislation process. Exact timing and impact of these incidents constitute confidential information.

The goal of the law is to prescribe a baseline of controls at every security level and to make governmental and municipal organization aware of the electronic information security risks they face and prevent the risks of losing the confidentiality, integrity or availability of their information and their information systems.

1.2 Information Security Risk Management and Compliance

Laws and regulations are by definition developed at a governance level, setting the goals of the legislators, or the regulators regarding what has to happen at federal, national or at organizational level.

The task of management of an organization regarding compliance is how to make it happen what must happen. This is left to the subjects of the laws and the regulations, namely the public and private organizations, or more precisely the CISOs or information security officers of these organizations.

Information security controls requirements derived from laws and the regulations are compulsory for the organization. However, a CISO would not be successful in terms of effective risk reduction if he / she focuses only on reaching compliance. Oftentimes, there are higher information security risks in an organization for the information security officer to mitigate than a non-compliance issue. After all, there is no use worrying about a regulatory fine while fighting a DoS attack or while trying to cope with a ransom ware.

An information security officer has to have his priorities in line with real life requirements: saving lives, handling major information security incidents, stopping imminent risks from happening and solving non-compliance issues. In Hungarian governmental organizations, according to the author's experience, priorities often follow different order in this priority list if the information security officer is not a trusted advisor of the senior management or if he / she does not have a full picture of the information security risks.

An information security officer has to know first why he / she is entrusted to protect the organizations' information assets that are to protect confidentiality, availability and integrity of information and information processing facilities. It is also his job profile requirement to comply with all relevant requirements, but it is only a secondary goal.

According to the author's experience, an information security officer can take advantage of compliance requirements while achieving his / her primary professional goal. In this article a Hungarian example of using international information security control standards and guides to comply with national regulatory compliance requirements is discussed.

2 Information Security Control Frameworks

2.1 Information Security Control frameworks

Control frameworks are generally accepted as national (f.e. NIST) or international standards (f.e. ISO/IEC), or published by professional organizations (f.e. ISACA, ISF).

They collect the experiences of the professional "crowd" that synthesized it. Standards and guide become a popular way to comply with the laws, regulations and contractual requirements.

Information security standards and control frameworks become valuable tools to ensure that security is planned, organized, implemented, tested and monitored. The standards and control frameworks became the lingua franca or common language. For an information security officer it is important to have a good command of these languages.

In this section, three of the most well known information security languages are discussed. These are those that the author found helpful to set up an information security framework, which is compliant with Hungarian L. Act of 2013.

2.2 ISO/IEC 27001:2013

ISO 27000 is the family of security techniques standards within the information technology field that focuses on Information Security Management Systems (ISMS). ISMS, according to ISO, "an ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process [2]."

This standard has its roots from the practices of the UK Government, the Department of Trade and Industry (DTI). First published as British Standard BS 7799:2 from 1995 and improved in 2002 to include the PDCA cycle.

It was included as an ISO standard later as ISO 27001:2005 when ISO adopted it. In 2013, the standard was revised and publishes as ISO/IEC 27001:2013, adopted by the Hungarian Standards Institute one year later as MSZ ISO/IEC 27001:2014.

ISO/IEC 27001:2013 standard specifies the requirements for continually improvable information security lifecycle based management system [3].

It is harmonized with other ISO management systems standards, including quality, environment, and information service management standards. It is designed to be generic such that it is applicable to most organizations.

The main book of the international information security standards ISO/IEC 27001:2013 sets the requirements for the information security framework of an organization, the information security risk management practices, and recommends controls to manage information security risks in Annex A. In Annex A, the controls are grouped into 14 sections covering logical, physical and human security as well as compliance.

An advantage compared to other information security best practices is that ISO/IEC 27001:2013 standard is certifiable; meaning that certification to the standard is an option. In addition to benefiting from the implementation of best practice information security controls, an organization which implemented the ISO 27001 ISMS may order a certification audit from an accredited certification body.

Certifications provide assurance to the customers and clients of the certified organization that relevant standards' recommendations have been followed. In certain occasions, certification is also a compliance requirement for an organization to provide special services. In Hungary this is the case for a few governmental organizations: including the Agricultural and Rural Development Agency (ARDA), which processes and pays out European Agricultural Guarantee Fund (EAGF) and European Agricultural Fund for Rural Development (EAFRD), and for special service providers licensed by the government, including electronic signature service providers, and lately the unified eID card framework service providers (based on Law LXXXIII. 2014).

There are examples in the governmental sector where the head of an organization decides to implement even more management systems into an integrated management system. An example for the integrated quality and information security management systems implementation is the Hungarian Intellectual Property Office. They were certified to ISO 9001:2008 and ISO/IEC 27001:2005 in January 2011 [3] and integrated information service managent system (ISO 20000-1:2011), and updated ISO 27001 to the 2013 version (in 2013).

2.3 NIST SP-800-53 rev. 4.

NIST is the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce which is responsible for publishing detailed information security guidance for decades.

Most relevant general information security guidance from NIST includes:

- SP 800-12 (An Introduction to Computer Security: The NIST Handbook, 1995) which gives an overview of computer security, originally to employees of federal government bodies who are responsible for handling sensitive systems.
- SP 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems, 1996) describes common security principles; high level description of what should be included in a computer security policy.
- SP 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 2000) describes the federal security risk management approach.
- SP-800-53 rev. 4. (Security and Privacy Controls for Federal Information Systems and Organizations, 2013) is the fourth version of the collection of almost 200 hundred (194 in total) relevant information security controls and also a security management guidance.

The NIST SP-800-53 rev. 4. guide [1] represents a well balanced portfolio of controls which is tested by US governmental organizations. In Appendix F, the controls are grouped into 18 sections covering logical, physical and human security.

The following list shows the structure of the control catalogue:

ACCESS CONTROL
AWARENESS AND TRAINING
AUDIT AND ACCOUNTABILITY
SECURITY ASSESSMENT AND AUTHORIZATION
CONFIGURATION MANAGEMENT
CONTINGENCY PLANNING
IDENTIFICATION AND AUTHENTICATION
INCIDENT RESPONSE
MAINTENANCE
MEDIA PROTECTION
PHYSICAL AND ENVIRONMENTAL PROTECTION
PLANNING
PERSONNEL SECURITY
PROGRAM MANAGEMENT
RISK ASSESSMENT
SYSTEM AND SERVICES ACQUISITION
SYSTEM AND COMMUNICATIONS PROTECTION
SYSTEM AND INFORMATION INTEGRITY

NIST reissued its mapping guide, Appendix H in 2014 to include the mapping of the updated ISO information security standards.

2.4 Cobit 5 for Information Security

ISACA is a global professional association which develops globally accepted best practices for information systems. It covers a broad range of fields within IT governance, IT management, IT risk management, and IT audit and information security management.

Its flagship knowledge product is Cobit, created originally to guide information systems auditors later extended to IT management and governance.

Cobit has been covering the information security process and related control objectives already (f.e. DS5 process in Cobit 4.1, 2007), however it is only a short list of control objectives. ISACA realized the need for a more detailed and business oriented

information security guidance. In 2008, they published a business oriented information security guide, called Business Model for Information Security (BMIS). In BMIS ISACA set out to publish an information security guide to include holistic factors to consider, while setting up and maintaining an effective information security control framework in 2009.

In addition to Cobit 4.1, additional “flagship” best practice guides were published since 2007. The ValIT Guide (ISACA, 2008) which is a guide based on proven IT an IS related investment management [5] to help enterprises realize the value from such investments, and the RiskIT Guide (ISACA, 2009) which is an information risk management guide.

ISACA harmonized its professional frameworks in 2013-2014 under the umbrella brand of Cobit 5. The main volume is the process framework and additional volumes are issued to integrate the previous guidance, including information assurance, IT risk and information security.

Cobit 5
COBIT 5 Implementation
COBIT 5: Enabling Processes
COBIT 5: Enabling Information
COBIT 5 for Information Security
COBIT 5 for Assurance
COBIT 5 for Risk
COBIT 5 Assessment Programme

In Cobit 5 the viewpoint of the same IT related processes is changed to the relevant topic of the guide. Consequently, Cobit 5 for Information Security is the information security viewpoint of the Cobit 5 IT processes and enablers. Cobit 5 for information security has a detailed mapping to ISO 27001 and a simple mapping to the assessment guide of NIST SP-800-53 in Appendix H of the Cobit 5 for Information Security guide.

2.5 Decree 41/2015. of the Ministry of the Interior (of Hungary)

The Hungarian law on electronic information security for governmental and municipal organizations was issued in 2013 as L. Act of 2013 of the Hungarian Parliament is abbreviated as Ibtv. in Hungarian (L. Act of 2013).

Similar regulations used to be in effect before this regulation, however they were limited in technical scope or its effect was limited only to central governmental bodies.

A detailed implementation regulation of Ibtv was issues also in 2013 as Decree No. 77/2013 of the Ministry of National Development. The decree is basically a summarized subset of the NIST SP 800-53 rev4 standard of the US NIST institute.

In 2015, L. Act of 2013 and the relevant implementing regulations were reviewed, among other changes, the control framework for the law was reviewed as well. Changes were minor in content, for example the requirement for Information Security Policy, and Information Security Strategy was deleted, and there are some added controls: dedicated incident handlers, and incident handling training.

However changes were major in terms of the timing of requirements, and the level of requirement most organizations have to reach. Previously, organizations were obliged to improve their security by one level in every two years. After the changes, organizations – which develop new information systems – have to meet security level requirements by the time their system go live. In the modified requirements, the organization operating their own information systems have to reach level 4.

3 Adapting Information Security Control Frameworks

3.1 Why use information security control frameworks

For an information security officer it advisable to follow a well established information security standard or guide, while establishing its information security framework, and policy. However, no guide or standard can cover all potential requirements, and organizations rarely need to implement all possible requirements. The advantages of using standards are manifold: common language with auditors / vendors, easier to adapt other best practices, etc.

3.2 Mapping of Standards and Best Practices

International Standards Institutes and Professional organizations have realized the value of interoperability, as presented in the previous section.

All major information security standards / guides discussed in this article have an official requirement mapping to one or more major information security standards / guides.

3.3 Mapping of Hungarian Information Security Regulations to relevant standards and best practices

Regulatory and contractual requirements for information security are not the only source of requirements. While structuring an Information Security Framework as set out in the L. Act of 2013, would make it easy to prove compliance to the National Electronic Information Security Authority of Hungary, it may not help reach other goals of the organization like the adoption of international practices or even ISO 27001 certification. [6]

The author as a part of his PhD research project analyzed the requirements of Decree 77/2013 NFM of Law L. of 2013 and prepared the requirements mapping to NIST SP-800-53 rev 4. And used the NIST-ISO 27001 mapping table to complement the original mapping with the requirements of ISO/IEC 27001:2013 Annex A. As Hungarian regulations have changed in mid 2015, so the mapping had to be modified accordingly.

The following table shows an example of the mapping:

Req ID (41/2015)	Req ID (77/2013)	Control name	NIST SP 800-53 rev4	ISO/IEC 27001:2013
3.1.4.1	3.3.2.1.	BCM policy	CP-01	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
3.1.4.2	3.3.2.2.	BCP for loss of IT resources	CP-02	A.6.1.1, A.17.1.1, A.17.2.1

Majority of the requirements set out in Decree 77/2013 NFM followed the order of the NIST requirements, leaving out some of the NIST requirements based on the decision of the Authority. During the revision of Law L. of 2013, the relevant Decree was modified as well. Few requirements were deleted and many were rearranged. Thus, the new Decree can still be mapped to NIST requirements.

Conclusions

Relative importance of information and automated information systems is increasing.

A regulation in itself provides limited help to Information Security Officers on how to comply with them. However, there are so many compliant organizations which had to bear the negative impact of information security incidents and will be in the future as well. [7]

International standards are not costly and they are proven useful. A summary of the description:

	ISO/IEC 27001	**NIST SP-800-53 rev4**	**Cobit 5 for Information Security**	**L. Act of 2013**
Focus	generic information security requirements	detailed information security requirements	generic information security requirements	electronic information security requirements
Scope	Any organization	US federal and state organizations	Any organization	Hungarian governmental and municipal organizations
Mapping available	NIST SP-800-53 rev4, Cobit 5 for Information Security	ISO/IEC 27001	ISO/IEC 27001, ISO/IEC 27002, ISF 2011, NIST SP-800-53A rev1	NIST SP-800-53 rev4
Certification	available	not certifiable	not certifiable	not certifiable
Cost of standard	CHF 118 (approx. HUF 34.000)	free	USD 75 (approx. HUF 22.000)	free

Hungarian regulations on electronic information security within state and municipal sector are based on NIST SP-800 53 rev. 4., ISO 27001 and CObit 5 are also useful when implementing a compliant information security framework.

Acknowledgement

This work was supported by the patience of my family and the professional contribution of both of my doctoral supervisors, Prof. Rajnai and Prof. Magyar. I appreciate their support very much.

References

[1] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2013

[2] ISO 27001 official homepage at ISO.ORG accessed in 15.11.2015

[3] MSZ ISO/IEC 27001:2014 standard, 2014, MSZT

[4] HIPO homepage accessed at 16.11.2015 at http://www.sztnh.gov.hu/hu/tajekoztato-a-szellemi-tulajdon-nemzeti-hivatalanak-minosegiranyitasi-es-informaciobiztonsagi

[5] John Thorp, CMC, ISP Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map, ISACA Journal vol 5 2008,

[6] Rajnai Z.-Puskas B.: REQUIREMENTS OF THE INSTALLATION OF THE CRITICAL INFORMATIONAL INFRASTRUCTURE AND ITS MANAGEMENT, In: INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS (ISSN: 1334-4684) (eISSN: 1334-4676) 13: (1) pp. 48-56. (2015)

[7] Rajnai Zoltán: Út a digitális kommunikációs rendszer felé (II.), NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK (ISSN: 1417-7323) 1. évf.: (2. szám) pp. 217-229. (1997)

ZOLTÁN NYIKES

INFORMATION SECURITY ISSUES OF RFID

Abstract

After presenting a brief history of RFID, the author discusses the general and security issues related to RFID and their possible solutions. Information security is examined as an integral part of overall security. Furthermore, various information security solutions and technologies are presented in this study to address specific security issues. From the wide range of application possibilities, the author has selected the document protection and the administrative security. Paper-based documentation cannot be completely ruled out from everyday life. Although great progress has been made in the field of authentic instruments and banknotes, many security elements have not yet appeared in the everyday life. The various application possibilities of "smart" paper and digital watermark can be considered here. When examining the question of future development, the author presents some of the likely alternatives predicted by experts for the forthcoming years.

Keywords: radio frequency identification, quality assurance, cost reduction, RFID applications, RFID and security, questions and concerns regarding RFID, protection of data

General introduction to RFID

RFID (radio frequency identification) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal or person. RFID is coming into increasing use in industry as an alternative to the bar code. The advantage of RFID is that it does not require direct contact or line-of-sight scanning. An RFID system consists of three components: an antenna and transceiver (often combined into one reader) and a transponder (the tag). The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. [1]

A brief history of RFID

The first radio-frequency identification technology was developed during World War II. Sir Robert Alexander Watson discovered and perfected the radar, which was used only for reconnaissance and detection. It was not yet capable of providing identification. In 1939, British scientists accidentally discovered that when a pilot was making a swinging movement

of the plane, the shape of the reflected radio waves was changing, which allowed to distinguish between friendly and hostile aircraft in the radar screen. This can be regarded as the first passive RFID system; which eventually led to the development of the first active aircraft detection system, the IFF. The boom of the RFID technology in the 1970s was preceded by its introduction in the 1960s. R. F. Harrington's studies on electromagnetic fields provided bases for the subsequent spread of RFID. Its first commercial applications started in the early 1960s. Sensormatic was a leading company in the development of RFID solutions. The EAS anti-theft system is still a widely used technology today. Major developments took place both in America and in Europe in the 1970s to introduce RFID in the monitoring of animals, vehicles and production processes. It became widely popular among farmers to track their livestock. The Los Alamos Research Institute also developed a system to track nuclear devices during these years. In the 1980s, the research and development phase was followed by the implementation of new solutions and their application in various products. In the United States, it was primarily used to keep track of delivery processes, to ensure personal access and to identify animals. In the 1990s the range of RFID applications further expanded: it was introduced in motorway tolling, as well as in immobilizers or (skiing) season tickets. The first microwave Schottky diodes integrated on CMOS circuits allowed the creation of microwave RFID tags with a single IC, which made possible a greater read range, as well as faster data transfer rates. The UHF RFID gained momentum in 1999, when the Auto-ID Center was founded. The company developed a low cost RFID tag containing a microchip. The tag is only used to store a serial number, which requires smaller memory, therefore it is cheaper. The serial number is searchable in an Internet-based database to receive further information about the product. Before that the RFID TAG had been a mobile database. Today, large multinational trading companies are planning the full implementation of RFID. Besides the US Department of Defense, various pharmaceutical and tyre manufacturing companies are interested in the technology. The really widespread use of RFID can be expected nowadays, after the second generation standards have been approved by EPCglobal. [2]

Possible applications of RFID

• Logistics, commercial warehouses;

• Library and archival applications;

• To trace assets, asset inventory;

• Production optimization;

• Supply chain management;

• Retail trade;

• Toll systems;

• Security and access control systems;

• Livestock. [3]

RFID tags classified

Class 0	UHF read-only, pre-programmed passive tag
Class 1	UHF or HF; write once, read many (WORM)
Class 2	Passive read-write tags that can be written to at any point in the supply chain
Class 3	Read-write with onboard sensors capable of recording parameters like temperature, pressure, and motion; can be semi-passive or active
Class 4	Read-write active tags with integrated transmitters; can communicate with other tags and readers
Class 5	Similar to Class 4 tags but with additional functionality; can provide power to other tags and communicate with devices other than readers

TABLE I.: RFID TAGS ARE CLASSIFIED AS CLASS 0 THROUGH CLASS 5, DEPENDING ON THEIR FUNCTIONALITY [4]

Questions and concerns regarding RFID

The use of RFID for personally identifiable information has been the subject of debate for years. It raises concerns mainly about the protection of personal data. People see a threat in the way that RFID tags can be read without having to face the owner, as the unique identifier of the stamps can be connected to the owner's personal data. In addition, RFID tags can be placed on any goods without the knowledge of the customer. Moreover, the tags can be read remotely by any readers that are hidden in the environment, so an individual may not even be aware of being "read". For example, a customer cannot deactivate the detectors in a department store. When payment is settled by bank card, the purchased product can be related to the customer. Consequently, the customer can be identified by name. Therefore, it may be possible to track not only the product, but also the customer from a larger distance. Various deactivator gates have already been in use, but their efficiency is still questionable. Of course, radio signals can also be encrypted by different cryptographic methods, but this may be limited by the memory capacity of passive tags. Besides the protection of privacy, another important issue is whether RFID is detrimental to health or to the environment. The RFID-related electromagnetic fields (EMF) are generally weak, and the population is exposed to radiation at a rate that is lower than the current standard limits. Nevertheless, the number of wireless devices has greatly increased by now. [5]

RFID and security

More recently, the implementation of RFID systems in high security applications has come into focus. It is enough to consider the increasingly popular PayPass credit card-paying system or patient identification. These solutions require the integration of certain security supplements into the existing systems, which are able to prevent unauthorized access or login. These advanced authentication systems reveal the fact of possessing a secret. The purpose of applying an appropriate algorithm is to prevent the compromise of the private key. Today's high security RFID systems have the capability of preventing the following attacks:

• Unauthorized access to the media with the purpose of duplicating or changing the stored data.

• Placement of media of unknown origin within the zone by circumventing authentication algorithms.

• Interception of radio traffic, or falsely creating the impression of an authentic media playback ("replay and fraud"). [2]

Mutual symmetric authentication

Mutual symmetric authentication is based on a three-step procedure between the reader and transponder in accordance with the ISO 9798-2 standard, which checks both parties' knowledge of the secret cryptographic key at the same time. [2]

Derived key authentication

Each transponder is equipped with a private key in order to improve safety. To achieve this, first the serial number of the transponder must be extracted. The secret key is created with the help of a master key and a cryptographic algorithm. As a result, each transponder receives its own ID, and a serial number that is linked to the master key on the downlink channel. As the first step of the common authentication, the reader retrieves the ID of the transponder. With the help of the master key, the special encryption module of the reader generates the private key of the reader. [2]

Encrypted connection

The solution described in the previous chapters is now completed with a potential attacker. In this case, there are two types of attackers. The first type attempts to stay in the background and retrieve valuable information in a passive way by interception. The second type, however, actively participates in the data exchange, and modifies its content for its own benefit. Cryptographic solutions can be used against both types of attackers. The value of data will be encrypted, and, as a result, the attacker cannot draw any conclusions on its original content. Data link encryption works on the same principle. In case of sequential encoding, each character is encrypted individually, while in block coding encryption is done by character blocks. The biggest difficulty of the RFID systems with encrypted data traffic is the distribution of the symmetric key before its use. [2]

The **stream encoders** are a set of cryptographic algorithms which encrypt the characters of the open text in succession, but by different functions. First, a random key will be generated, which will be the shared key between the parties in the information exchange. The key will then have an XOR connection with the characters of the open text. The random key must have at least the same length as the open text, otherwise statistical attacks of the repeated patterns can be expected. In addition, each key is used only once, which requires a

high level of safety in the key distribution. In this form, stream encoding is completely unsuitable for RFID systems. In order to overcome the complications caused by key distribution and generation, true random number generators were replaced by "pseudorandom" generators, along with "pseudorandom" keys. [2]

Other security recommendations

In case of **Hash-based** access control, by taking into account the resource management of cheap smart tags, a simple security procedure based on one-way hash functions will be presented in the followings. Typically, the scheme is implemented by using hardware. The tags working in locked or unlocked mode separate a small section of their memory to store the metaID earmarks. In order to lock a tag, its owner stores the hashed version of a random key as the metaID of the tag in the transponder. This can be done by RF or in a direct physical way. In order to unlock the key, the host retrieves the metaID of the tag, finds the key in the database, and then returns it to the transponder. The tag hashes the key, and compares it with its own metaID. As soon as these two hashes correspond with each other, the key unlocks itself, and provides full functionality for the surrounding readers. In order to prevent any abuse of unlocked tags, tags should be kept unlocked only for the duration of information flow. The method provides great protection against unauthorized access by taking advantage of the difficulty of inverting a one-way hash. However, it does not prevent spoofing attempts, only detect them. Furthermore, the reading device can also check the content of the tags with the help of the back-end. [2]

In the case of **random access control**, the solution uses one-way hash functions, which is efficient for a small number of tags, and prevents unauthorised requests, while the tags remain able to respond to the request of certified readers. In addition to the above-mentioned transponders which are able to calculate one-way hash functions, this solution can also generate random numbers. At the request of the reading device, the transponder first generates a random number, and then it retrieves the concatenate of the ID and the random number from the hash. [2]

In the case of **asymmetric key** negotiation, the readers can gain much information from the asymmetry between the uplink and downlink channels during the transmission of data which are sensitive to interception. [2]

The method of **Chaffing and Winnowing disturbs** the interception equipment by filling the communication with useless messages, or chaffs, which are continuously filtered by

the transponders with the help of a simple MAC (winnowing) when useful data is being sent. [2]

Detection units may also be added to the RFID system to detect unauthorized reading.

In the case of screaming tags, the above-mentioned units can also be used successfully against DoS attacks, as they can detect off-mode transponders. [2]

Application of RFID with respect to document security

The concepts of security and safety refer to Digital and/or Photocopied/Printed Data Security/Information Security, as well as brand and packaged product security against unauthorized access or modification, partial or complete deletion, damaging or destruction. It also means the full protection of the confidentiality availability and integrity of the data or product.

Data security and protection system

Depending on the method and the degree of detectability, security solutions have the following groups:

- Overt Security Solutions
- Covert Security Solutions
- Characters and symbols which can be reconstructed by machine tools, characters, line, colour or other code sequences, which can be made visible by using radiation (lasers, ultraviolet, infrared, radio, x-ray and electron beam) or chemical reagents. [6]

RFID solutions for document management

Document identification with RFID stickers

- RFID is used on the document in the form of an identification sticker.
- The collision-free technology allows the identification of hundreds of documents per second; therefore it is ideal for archive application.
- The management of high safety level documents: the sticker can record who, when and how long had access to the document [7]

E-Inks, such as materials containing liquid-dispersed, positively charged white particles and negatively charged black microcapsules, which become white or black

depending on the polarity of the magnetic or electric field, and their planar distribution carries two-dimensional visual information. [6]

Liquid RFID Ink Solutions were developed by Cross ID Communication Materials, and they are able to identify the materials or products to which they are added, by emitting radio signals. By adding this liquid to printer and photocopier ink, a tamper-proof, high security printing product can be produced. [6]

The Smart Paper, the media type of the future, which can be programmed by using the semiconductor polymers, microchips, radio frequency devices, or printed integrated electronic elements placed on the surface of the paper. [6]

The Digital watermark first appeared in the market of printed and photocopied products in 1992. It can consist of, for example, a number and code combination which may be reconstructed by a machine only and a digital signature. The visible or invisible watermark can be placed on the surface of the media, or embedded into the material of the media, depending on the purpose of protection. [6]

RFID Forecasts, Players and Opportunities 2016-2026

IDTechEx find that in 2015, the total RFID market is worth $10.1 billion, up from $9.5 billion in 2014 and $8.8 billion in 2013. This includes tags, readers and software/services for RFID cards, labels, fobs and all other form factors, for both passive and active RFID. IDTechEx forecast that to rise to $13.2 billion in 2020. [8]

Using new, unique information researched globally by IDTechEx technical experts, the RFID market is analyzed in many different ways. Full analysis by each market is given in great detail including in-depth historic data by application type from 2005 year by year to 2021 and with a 2026 outlook. For passive RFID, forecasts are provided separately for the following application areas. Number of tags are provided for each, average sales price and total value of tags. [8]

In addition, ten year forecasts are provided for battery assisted passive and active RFID and RTLS in the following applications:

- Pharma/Healthcare
- Cold retail supply chain
- Consumer goods
- Postal
- Manufacturing parts, tools
- Archiving (samples)
- Military
- Retail CPG Pallet/case
- Shelf edge labels
- Conveyances/Rollcages/ULD/Totes
- Vehicles People (excluding other sectors)
- Car clickers other tag applications [8]

Additionally, the report provides units, asp and total value for RFID readers as follows:

- UHF Fixed portal
- UHF Embedded and handheld
- HF and LF Hand held, fixed, embedded
- LF Vehicle
- NFC Cellphone [8]

Passive UHF market data segments - 10 year forecast	Passive HF RFID market data segments - 10 year forecast	Passive LF market data segments - 10 year forecast
Retail apparel and footwear	Contactless cards/fobs	Livestock and
Retail-other	Smart tickets	Access control
Logistics, conveyances, roll cages	Books	Vehicle immobilizers
Asset management /inventory	Medical	Medical
Medical/heal th care	Assets/tools	People
Air baggage and cargo	Passports	Other
Access control/ticket ing	People	
Embedded	NFC applications	
People	Other	
Other		

TABLE II.
PASSIVE UHF MARKET DATA SEGMENTS - 10 YEAR FORECAST [8]

Conclusions

The current analysis of the topic can contribute to the development of the present and the future radio frequency identification and registration systems [9, 10]. Quality assurance and cost reduction in information technology are not only supported by the government, but are also gaining a growing role both in private and corporate spheres, as well as in public

sector. As a consequence, radio frequency identification and the related information security considerations will be increasingly in the forefront of development in the coming years. The aim is to develop such identification procedures that protect the interest of users, and comply with the laws and the agreements on the protection of personal data. As the above example of document security has shown, these solutions offer a wide range of applicability, and they could meet today's security requirements with minimal innovative effort. [11, 12] High-frequency radio communication chips, which can be stuck or printed on anything or planted anywhere, have already been introduced into various fields: including logistics, trade, health, border security, education or law enforcement, and they will be used even more extensively in the future.

References

[12] Margaret Rouse - RFID (radio frequency identification) definition, http://searchmanufacturingerp.techtarget.com/definition/RFID, 20 Sept 2015

[13] Studies on RFID systems in view of application and technology – Inter-University Centre of Telecommunications and Informatics (ETIK), Budapest, September 2006

[14] IT café – European agreement on the ethical use of RFID tags http://itcafe.hu/hir/eu_eb_rfid_intelligens_cimke_kroes.html , 20 Sept 2015

[15] EPC-RFID INFO – RFID Tags, http://www.epc-rfid.info/rfid_tags , 5 October 2015

[16] Éva Juhász – RFID – A Current Issue (20 July 2011) http://krono.inaplo.hu/index.php/inter/8-networkstudies/916-rfid-egy-aktualis-kerdes , download: 10 October 2013

[17] Emil Eiler – Security printing for the protection of digital data, brands and documents, packaged products and consumers, MAGYAR GRAFIKA 2007/7.

[18] László Rácz – RFID-Radio Frequency Identification-[Online] http://www.allaminyomda.hu/file/1000185 , download: 10 October 2013

[19] Raghu Das, Dr. Peter Harrop – RFID Forecasts, Players and Opportunities 2016-2026, (October 2015) http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2016-2026-000451.asp , download: 5 October 2015

[20] Fregan Beatrix: Un personnage éminent de l'historie de la Défense Hongroise HÍRVILLÁM = SIGNAL BADGE (ISSN: 2061-9499) I: (1) pp. 302-304. (2010)

[21] Rajnai Zoltán Bleier Attila: Structural problems in the fixed communication systems of the Hungarian Army In: Fekete Károly: Kommunikáció 2009. 346 p ISBN:978 963 7060 70 0

[22] Rajnai Zoltán: Les radios de l'avenir pour les armées In: Fekete Károly: Kommunikáció 2004, pp. 269-273

[23] Fregan Beatrix - Fábián Éva: The special relationship for European integration, In: Fekete Károly: Kommunikáció 2010. 397 p. (ISBN:978-963-7060-21-2)

ISTVÁN SEBŐK

A RISK ANALYSIS METHOD PRESENTED THROUGH THE SAFE USE OF THE 9 MM GLOCK-17 PISTOL

Abstract

The process of risk management is used in all aspects of life and military operations. The method is applied in the financial, the military and many other sectors as well. In military sector, it is a basic element in the planning of military operations. A possible risk analysis method will be presented in this study, by showing risk estimation during the use of a pistol. Anyway, it is a legal requirement for any military organization or unit to carry out such an analysis.

Keywords: pistol, risk management, maintenance, identity hazard

Introduction

The Hungarian Defense Forces (hereafter: HDF) introduced the risk management process into the training activities, the operational environments, and the materiel acquisitions in the late 1990s. Risk management was originally perceived solely as a labor safety. However, by the early 2000s, the HDF established a goal to integrate risk management into the all HDF processes and activities, and into every individual's behavior, both on and off duty. Since the process was introduced, the personal involvement of commanders in preventing accidents has become a basic factor in the steadily diminishing number of accidents in the HDF.

Leaders must understand the importance of the process in conserving combat power and resources. Risk management, like reconnaissance and security, is an ongoing, permanent process. Within the problem, the leaders must know when the process begins and who has responsibility. It must be an integral part of the military decision. The process is an important means to enhance situational awareness.

The GLOCK pistols are the product of advanced technology and incorporate numerous innovative design features, which results in an easy operation, an extreme reliability, a simple function, a minimal maintenance, a good durability and a light weight. GLOCK was the first company to successfully produce a polymer handgun receiver and

marry it to a strong steel slide and barrel. The GLOCK pistol incorporates the “Safe Action” system, which features three safeties and is similar to a constant double action only system. Special processes arise from this construction and function, this procedure is presented in this study.

Risk management process:

Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance the risk costs with the mission’s benefits. Leaders and soldiers at all levels use risk management. It applies to all missions and environments across the wide range of HDF operations. Risk management is fundamental in developing confident and competent personnel and units. Proficiency in applying risk management is critical in conserving combat power and resources. Leaders must train the personnel to provide them with the critical skills to be used in the five-step risk management process.

Risk is characterized by both the probability and the severity of a potential loss that may result from hazards due to the presence of an enemy, an adversary, or some other hazardous condition. Perception of risk varies from person to person. What is risky or dangerous to one person may not be to another. Perception influences the leaders’ decisions. A publicized event such as a training accident or a relatively minor incident may increase the public’s perception of risk for that particular event and time, sometimes to the point of making such risks unacceptable. Failure to effectively manage the risk may make an operation too costly, politically, economically and in terms of combat power (soldiers’ lives and equipment). This chapter presents the background, the principles, the applicability and the constraints relating to the risk management process.

Five-step risk management process:

Risk management is the process of identifying and controlling hazards to conserve combat power and resources. The five steps of risk management are the following:

- Step 1. Identify hazards.
- Step 2. Assess hazards to determine risks.
- Step 3. Develop controls and make risk decisions.
- Step 4. Implement controls.
- Step 5. Supervise and evaluate.

Step 1. identify hazards:

A hazard is an actual or potential condition where the following can occur, due to the exposure to some damage or loss of personnel, equipment and property. Specialties of terrain and weather should be considered in this step. In addition to those due to the enemy or adversaries, the most obvious hazards to military operations are due to terrain and weather. Terrain and weather affect the type of hazard encountered. When the enemy uses terrain to his advantage, the risk is clearly tactical. The features of terrain and weather may create situations where accident risks predominate. When looking at this from a purely mission perspective, familiarity of the unit with the terrain and its associated environment must be paramount. The basic issues are how long the unit has operated in the given environment and climate. Weather works hand-in-hand with terrain to create hazards. To identify weather hazards, leaders and soldiers must assess the impact on operating systems. Mistakes include not considering the effects of climate and weather on maintenance of weapon and equipment before beginning an operation.

Step 2. assess hazards to determine risks:

Development as well as engineer and technical properties of the device, in this case the pistol, should also be considered. GLOCK pistols combine the safety and simplicity of revolver-like operation with a manageable constant double action only trigger pull, high magazine capacity, rapid recovery and the reduced recoil of a modern, semiautomatic pistol. The major metal components of GLOCK handguns are treated with GLOCK's special hardening surface process called “tenifer” that leaves them nearly as hard as a diamond, seals out moisture and helps prevent corrosion. This surface hardening process penetrates the surface of the slide, barrel and GLOCK brand metal sights. The matte black finish is a final process applied to the surface making the pistol extremely resistant to abrasions and scratches. Should this black finish wear off after heavy and extensive use, the surface still retains its corrosion protection and durability.

Step 2 completes the risk assessment. Risk is the chance of hazard or bad consequences. This step examines each hazard in terms of probability and severity to determine the risk level of one or more hazardous incidents that can result from the exposure to the hazard.

Hazard Probability:

Leaders assess each hazard in relation to the probability of a hazardous incident. The probability levels estimated for each hazard may be based on the mission, the course of actions being developed and analyzed, or on the frequency of a similar event:

- **Frequent (a)** occurs very often in service life. Expected to occur several times over duration of a specific mission or operation.
- **Likely (b)** occurs several times in service life. Expected to occur during a specific mission or operation.
- **Occasional (c)** occurs some time in service life. May occur about as often as not during a specific mission or operation.
- **Seldom (d)** occurs in service life, but only remotely possible. Not expected to occur during a specific mission or operation.
- **Unlikely (e)** occurrence is not impossible, but it can be assumed that this will almost never occur in service life.

Hazard Severity:

This point addresses the severity of each hazard. It is expressed in terms of loss of or damage to equipment or property. The degree of severity estimated for each hazard may be based on the knowledge of the results of similar past events.

- **Catastrophic (i):** Loss of major or mission-critical system or equipment.
- **Critical (ii):** Extensive (major) damage to equipment or systems.
- **Marginal (iii):** Minor damage to equipment or systems, property, or the environment.
- **Negligible (iv):** Slight equipment or system damage, but fully functional and serviceable.

Risk Assessment Matrix:

In this point the leaders describes into estimates the levels of risk, and what they understand about the probable hazardous incidents for each identified hazard, and put in an estimate the overall risk for the operation. Estimating risk follows from examining the outcomes of the probability and severity of hazardous incidents.

This point is more art than science. Much depends on the use of historical lessons learned, intuitive analysis, experience, and judgment. Uncertainty can arise in the assessment of both the probability and the severity of a hazardous incident. Uncertainty results from

unknowns about a situation; from incomplete, inaccurate, undependable, or contradictory information; and from unforeseen circumstances. Therefore, assessment of risk requires good judgment.

The standardized matrix can assist in this process. The estimated degree of severity and probability for each hazard is put in the severity row and the probability column, respectively. The point where the severity row and probability column intersect defines the level of risk. For example, if the hazard is estimated to have a *critical* severity (II) and a *likely* probability (B), the level of risk is high (H).

Risk Assessment Matrix					
	Probability				
Severity	Frequent (A)	Likely (B)	Occasional (C)	Seldom (D)	Unlikely (E)
Catastrophic (I)	E	E	H	H	M
Critical (II)	E	H	H	M	L
Marginal (III)	H	M	M	L	L
Negligible (IV)	M	L	L	L	L
E – Extremely High Risk H – High Risk M – Moderate Risk L – Low Risk					

Figure 1.

Risk Assessment Matrix

E - Extremely High: Loss of ability to accomplish the mission if hazards occur during the mission.

Example GLOCK -17 pistol:

- Observed problem: The pistol slide fails to lock open on last round.
- Probable causes: Worn slide stop lever notch.
- Correction: Contact Warranty Department if replacement of the magazine and slide stop lever did not correct the issue.

H - High: Significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if hazards occur during the mission.

Example GLOCK -17 pistol:

- Observed problem: Trigger safety fails to return to engaged (forward) position.
- Probable causes: Improperly stored in original box with trigger in full forward position (trigger safety fully depressed).
- Correction: Replace trigger bar. When stored in original box, pistol must be unloaded, trigger in back position.

M - Moderate: Expected degraded mission capabilities in terms of the required mission standard will have a reduced mission capability if hazards occur during mission.

Example GLOCK -17 pistol:

- Observed problem: Inconsistent trigger pull or will not release.
- Probable causes: Connector loose in housing.
- Correction: Replace housing.

L - Low: Expected losses have little or no impact on accomplishing the mission.

Example GLOCK -17 pistol:

- Observed problem: Light off-center strike.
- Probable causes: Slide lock reversed or not beveled.
- Correction: Replace.

Step 3. develop controls and make risk decisions:

After assessing each hazard, the leaders develop one or more controls that either eliminate the hazard or reduce the risk (probability and/or severity) of a hazardous incident. When developing controls, they consider the reason for the hazard not just the hazard itself.

Types of Controls: Controls can take many forms, but fall into three basic categories-educational controls, physical controls, and avoidance.

- Physical controls. These controls may take the form of barriers and guards or signs to

warn individuals and units that a hazard exists. Additionally, special controller or oversight personnel responsible for locating specific hazards fall into this category.

- Avoidance. These controls are applied when leaders take positive action to prevent contact with an identified hazard.
- Educational controls. These controls are based on the knowledge and skills of the units and individuals. Effective control is implemented through individual and collective training that ensures performance to standard.

I. Fully Assembled Pistol control:

I./1. Slide Lock:

- With thumb and forefinger, try to pull down on both sides of the slide lock lever. It should not move downwards if the slide is forward and locked in battery. This lets you know the slide lock is present and “locked” properly.

- Using the disassembly grip, move the slide rearward approximately 3 mm and pull down on both sides of the slide lock and release. This verifies the slide lock will "unlock" and the spring is operational.

With the slide lock lever fully engaged, point the pistol in a safe direction and pull the trigger while pushing the slide forward. The slide should remain “locked” and not move forward off the receiver.

I./2. Trigger Safety:

- With the slide forward, action set and the trigger forward (ready to shoot), press on both sides of the trigger and try to move the trigger backwards. The trigger should only move slightly rearward (not releasing the firing pin). Be careful not to press on the center portion (trigger lever safety) of the trigger pad. This verifies the trigger lever safety is present, operational and would prevent any unwanted rearward movement of the trigger bar.

- After making sure the pistol is unloaded, point it in a safe direction and pull the trigger. When the finger depresses the trigger lever safety, it should allow the trigger lever safety and trigger to move rearwards and release the firing pin.

Recoil Spring/Guide Rod Assembly:

The recoil spring should be strong enough to move the slide forward reliably to chamber cartridges even if the pistol is somewhat dirty, dry or the ammunition is not perfect.

With an unloaded pistol, point it 45° upwards and pull the trigger. While holding the trigger back, pull the slide to the rear and release it very slowly. The recoil spring should be able to push the slide completely forward and fully into battery. This test verifies that the recoil spring is strong enough to chamber ammunition despite less than ideal circumstances.

I./3. Magazine Spring:

The magazine spring must be strong enough to feed all ammunition reliably and be able to push the magazine follower up with sufficient strength to move the slide stop lever up to lock the slide to the rear when no ammunition remains. Insert an empty magazine and pull the slide completely rearwards force- fully. The slide should lock back every time without any assistance. This test ensures that the magazine spring is strong enough to lock the slide back when no ammunition remains in the magazine. It also checks for proper operation of the follower and slide stop lever.

I./4. Firing Pin Safety Release:

When the trigger is pulled, the firing pin safety moves upwards and clears the firing pin channel to allow the firing pin to move freely to strike the primer with sufficient force. With an unloaded pistol, point it in a safe direction and pull the trigger. Hold the trigger rearward and shake the entire pistol. You should hear the firing pin moving forwards and backwards. This ensures the firing pin channel is unobstructed and the firing pin safety has been moved enough to allow the firing pin to move freely.

II. Field inspections while field stripped control:

II./1. Slide:

Firing Pin/Firing Pin Safety Engagement:

With the slide off the receiver, use your finger to pull back on the firing pin lug. Ease the lug forward again and it will rest against the firing pin safety. The firing pin safety should block any forward movement of the firing pin. Press forward on the back of the firing pin lug and attempt to force the firing pin forward. There should be no forward movement of the firing pin unless the safety is depressed. If there was no forward movement with the safety engaged, then press in on the firing pin safety and the firing pin should now move freely

forwards. This inspection verifies that the firing pin safety does block the firing pin and prevents any forward movement unless the safety is depressed.

Firing Pin Free Movement:

With the firing pin safety depressed, shake the slide forwards and backwards. You should be able to hear the firing pin moving freely. This check verifies that the firing pin channel is unobstructed and the firing pin may move forwards freely when the safety is depressed.

II./2. Receiver:

Slide Stop Lever Tension:

When properly assembled, the slide stop lever should be under spring tension and slight backwards and forwards movements should be possible. The slide stop lever should be held down until the follower forces it up. With your fingers, pull the rear of the slide stop lever upwards and release. It should snap down with force. If the slide stop lever does not have sufficient downward force, it may engage the slide notch pre- maturely and lock the slide back even if ammunition remains in the magazine. This check ensures that the slide stop lever has sufficient downward spring pressure and should not lock the slide back prematurely.

II./3. Drop Safety:

Using your fingers, pull the trigger forward (or push forward on the vertical extension of the trigger bar). On the top of the back of the trigger bar, you will find the cruciform. The arms of the cruciform rest on the drop safety ledge when the trigger is in the forward position. The drop safety ensures the back of the trigger bar does not move downwards and release the trigger bar unless the trigger is pulled fully to the rear. With your pin punch centered on top of the cruciform, press down firmly and see if the back of the trigger bar will move downwards. It should not move down unless the trigger is pulled. After seeing that the drop safety is operational, press forward on the vertical extension of the trigger bar and pull the trigger. The back of the trigger bar should move backwards and then downwards. This shows that the drop safety would prevent any premature separation of the trigger bar and firing pin.

III. Maintenance/Cleaning Supplies:

Using the disassembly grip, retract the slide approximately 3 mm while pulling down on both sides of the slide lock. While holding the slide lock in the downward position, move the slide forward. Remove the recoil spring/guide rod assembly by grasping the end nearest the barrel lug and pulling it straight up. Lift up on the barrel lug and remove the barrel. You should have the following: slide, barrel, recoil spring assembly, receiver and magazine(s).

III./1. Cleaning Supplies:

Use only solvents and lubricants designed for use on firearms. Any product that is advertised and/ or marketed for use on guns may be used on GLOCK pistols. When using solvents, make sure all solvent is removed before lubrication, use or storage of the firearm. Under some circumstances, a dry cleaning may be appropriate. After cleaning, GLOCK pistols require a minimum of lubrication.

III./2. Barrel:

Inspect the barrel to ensure that the bore is clear. Using a proper size bore brush or cloth patch, push it all the way through from the chamber and out the muzzle end of the barrel. Heavy fouling may require multiple passes. With a small brush (toothbrush), clean the lug areas, feed ramp and outside surfaces of the barrel. When satisfied all residue and solvent has been removed and all surfaces are dry, move to the slide.

III./3. Slide:

Inspect the slide for any obvious fouling. Holding the slide with the firing pin channel up to prevent solvents from entering, clean the breech face and extractor area with the toothbrush. Take care to scrub under the extractor hook. Brush down the slide grooves, the ejection port area and all other surfaces. For cleaning the openings of the slide use GLOCK channel maintenance kit. When satisfied all residue and solvent has been removed, move on to the recoil spring assembly.

III./4. Recoil Spring:

Inspect the recoil spring/guide rod assembly for wear and obvious fouling. Using a cloth or brush, clean all surfaces. When satisfied all residue and solvent has been removed, move on to the receiver.

III./5. Receiver:

Use the brush to clean the rails and brush down all other surfaces as necessary. Be certain all solvent and residue has been removed before you attempt to reassemble the pistol.

III./6. Magazine:

Don't disassemble. Use a brush or cloth to clean down all surfaces as necessary.

III./7. Lubrication:

After a thorough cleaning, remove any remaining solvent from the pistol. Using a quality gun oil or grease product, lightly lubricate the barrel, barrel hood, barrel lug and the inside of the slide where the barrel hood contacts the slide. Apply a small amount of lubricant on either the frame rails or inside the slide grooves. Once the slide is replaced on the receiver and the action worked several times, the lubricant will be distributed equally along the slide grooves and frame rails.

Most important is one drop of oil placed just under the connector hook (located just above the right rear receiver rail). Any lubricant placed here will move down where the connector and trigger bar meet. If this area is not properly lubricated, the result may be a "hard" trigger pull that can lead to connector and/or trigger bar damage. GLOCK pistols are designed to operate properly with minimal lubrication. Large quantities of oil or grease may collect unburned powder, grit, dust or other residue that could interfere with proper functioning of any fire- arm. Extreme climate (cold or hot weather) could affect large amounts of lubricant.

Step 4.and step 5. implement controls and supervise and evaluate:

Leaders ensure that controls are integrated into control instructions, written and verbal orders, mission briefings, and staff estimates. The critical check for this step, with oversight,

is to ensure that controls are converted into clear, simple execution orders understood at all levels.

The leaders supervise the mission rehearsal and the execution to ensure that standards and controls are enforced. Techniques may include spot- checks, inspections, situation reports and brief-backs, buddy checks, and close supervision. During the mission, the leaders continuously monitor the controls to ensure they remain effective. They modify them as necessary. They and other individuals anticipate, identify, and assess the new hazards and elaborate suitable controls to avoid them. They continually assess variable hazards such as the fatigue, the equipment serviceability, and the environment, as well as modify controls – it necessary – to keep risks at an acceptable level.

Conclusions

Risk management must not be treated as an afterthought. It must be planned for up front. Leaders and managers during some materiel acquisition and before carrying out military or technical operations must budget for the risk control costs. In the course of planning these costs, they have to take into consideration the duration of the given operation and the life cycle of the given material or weapons system. When integrating risk management into sustained operations, the leaders must consider the possible obstacles and hardships, as well as the changes in the personnel, the eventual critical skill atrophy and the expected evolvement of the operations.

References

- ATP 5-19 Risk Management US ARMY
- FM 100-14, Risk Management, 23 APRIL 1998. US ARMY
- Glock Armorer's Manual 2009
- ISO 31000:2009 - Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- ISO Guide 73:2009 - Risk Management – Vocabulary
- ORM 1-0 Operational Risk Management USMC Marine Corps Institute

BOOK REVIEW

RET. COL. SÁNDOR KOLOSZVÁRI

IDEAS ON THE BASIS OF A BOOK CURIOSITY

"Individual Muslims may show splendid qualities, but the influence of the religion paralyses the social development of those who follow it. No stronger retrograde force exists in the world."
(W.Churchill on Islam. The River War, 1899)

In my retired private life, a book got into my hands, which has quite an actual content. (The Islamic State. Terrorism 2.0: Kossuth Publishing, Budapest, 2016.) Ákos Bíró wrote a review about the book in Honvédségi Szemle 2016/2. Nowadays, there is hardly any topic more seasonable than the Islamic State (IS). The authors – all of them are Hungarian researchers – handled the topic with good sense of cadence and took advantage of the interested Hungarian readers' demand. They put together a volume which introduces plastically this relatively new and quickly developing „phenomenon", its driving force, its ideological basis and its everyday practice, as well as its members' range of thought, summing up: the atmosphere of this whole „phenomenon".

The motivation of my personal interest is that throughout years I could work in a bilateral (Hungarian-Soviet) unit as a commander in Aleppo, in a Syria where at that time (1979-83) everything has started – at least it was the now existing events' first act. The excuse then was the march of the Soviet Union into Afghanistan, and the center of actions (I expressed myself very gentle) was Aleppo. This is how and when we, Hungarian employees got into the middle of actions. The authority created order in the city by hard tools (and by the deployment of a reinforced division), and that is why the Muslim Brotherhood's scene of actions had been relocated to the other parts of the country – mainly to Hama. After a long lasting series of action – that resulted in approximately 25,000 victims – the violence had

stopped, and the order was restored all over the country, which was highly appreciated by the residents.

At that time, many experts had already a certain opinion that the Arab world looked entirely different from the inside, and it was not possible to understand it from books, and we needed years to recognize, accept and experience the mystery of the Arab soul. Taking into consideration all of this, we are contemplating the current series of actions – which is even shocking for us – and we are facing the twisted formation and the incredibly dark technique of the Islamic State through a new kind of lens.

By the volume's superficial flick-through, it becomes evident that the authors prepared their work using an easy to follow logical order: from the abstract of the historical beginning through the very expressive representation of the ideology until the introduction of the operative toolbar. It might be unbelievable for the reader, but the Islamic State has already a story (with some overstatement: history). It does not have any community defined by frontiers, any territory accepted by international organization; yet, it is still working. Let us admit it, it is a real curiosity. Here, at the beginning of the book, we can see the expression of *terrorist organization*, the designation of *combatant*, the definition of *caliphate* as a form of government, the explanation of *strategy*, *allies and enemies*, as well as the identification of *war crimes and genocide*. Besides, the authors have clarified for the reader already in the first chapter that they are speaking about terrorist organizations as for real. Explicit speech that leads to the question of what this particular „artificial state" is nourished by, what it considers as its ideological basis. Is its ideology in tight coherency with the principles and practices of Islam?

Clearly the volume's most important part, rather its chapter, is the „Ideology of the Islamic State". I cannot ignore my personal experiences (throughout the years), so I will try to give a synthesis of the view expressed by the authors and the experience acquired on the spot as a former chief adviser.

I hope I am reading and understanding the expressed thoughts correctly that on one hand the authors refer back to the Koran as the ideological basis of the Islamic State and on the other hand, they refer back to the spread of Islam, to be more correct, to the tools of its (mostly violent) dissemination in its first century. If the unsuspecting reader who is really interested in the matter wants to understand this correctly (at least the defined thoughts of the authors) he/she should take the Koran in his/her hands and carefully study it (I use the expression „study" on purpose, because reading here is not enough). When 35 years ago I managed to do this – I admit, it was not an easy reading – I immediately had the impression

that this is a writing *which summarizes violent opinions*. Its vocabulary, conceptual system and terminology have already proved that. This can be seen in the analysis of the thoughts called „the roots of radical Islamism", „the world view of ISIL" or „the principles of its ideology"

As for the „tactics of the expansion of the religion", the experience, or rather the routine used after the death of Mohamed throughout quasi 200 years, have almost literally occurred again, which have not despised violence at all, in the cases of „faithless" or „apostate" people. This chapter introduces and illustrates convincingly the violent existence and uninhibited belligerence of the IS, with big emphasis (and with timely examples). The authors leave no doubt about what the world should expect, more closely those countries that have received or still are receiving the future (and present) activist of the Islamic State in big numbers. Their thoughts must be taken seriously especially because they are not alone with their views. The cruel „solutions", the inhuman and (it is a must to write down) uninhibited attitude, which are common daily practices for the IS are not just scaring, they represent the harsh reality.

Certainly, all of this emerged and got dominant by „state" impulse in the area controlled by the IS. We, who were part of a not more than 9 year-long foreign service in Syria, have already known a more peaceful world (compared to the nowadays conditions). The state itself resisted the pointless radicals and religion-based ferocity and if we want to impersonate: Háfez Asszad (the current president's father) esteemed order in the country, which was not hard for him as most of the people living in Syria preferred peace and quiet. This has not changed until today.

In the third part of the book, the authors introduce the tools, methods and solutions which are used by the activists of the IS in order to attempt „convincing" smaller mediums and even (with the help of the internet) the world that this is the only true path, this is the future, and that they are undefeatable. I must add: this is a unique way of propaganda. We can see it clearly – and the authors of the book refer to this several times – that everything what is happening there can be – unfortunately – accepted many people. We would show big narrow-mindedness if we were to not recognize it. Hopefully this volume is going to open people's eyes.

If we studied the chapters carefully it is impossible not to catch sight of the ever more extending „attack on the entire field", which can be called (with military terminology) as an invasion. The authors demonstrate this very convincingly to the interested readers.

The notes increase the volume's intelligibility, readability and credibility. And as I mentioned credibility: for me, who has lived years in Aleppo, which was called one of the world's hottest points even then, if a volume with a topic like this one lands in my hands, the first question I ask myself is whether the creators, authors lived in an Arab environment and if the answer is yes, on what kind of intellectual level did they move, or rather work? Did they have entrance into Arab families? The Arab soul's mysteries, the Arab world's atmosphere can only be known truly and authentically from the inside. Naturally, if they did not have the chance to do so, the things that are on the papers can still be credible. The prologue of the secretary shows that there is harmony on government level (as well), even governmental assistance can be addressed to the topic or the authors. Among the advisers of a volume with a topic like this, there is a place for an Arabist, an academic expert who certifies the content of the book with his professional authenticity, international reputation, accepted scientific rank in the Arab world and his Arab language knowledge. I know that all of that together is very rare to come by, but it seems to me that in this case this happened; at least the standard of the volume demonstrates it.

It is a big value of the book that after reading it, the reader feels an urge to try to answer some questions that are posed by many readers, such as: Was it necessary, was it allowed to intervene in the internal life of several Arab countries (Arab Spring), in the ranking of their „democracies"? Should we assist and how the huge crowd of migrants? Are we Hungarians well prepared in „Arabology"? Do we really know the „inner world" of todays' Middle East? Did we finally understand that it is only possible to cooperate with the Arabs by being mindful of their norms and traditions in the fields of politics, economy, trade and agriculture as well? And as regards the military questions, we must assume a special sensibility.

Those thoughts that are searching for answers are inevitably important parts of the volume: Which direction should the world move in order to have an organized prevention of the dangers that appear more and more specific? I believe, moreover it is my conviction that the authors take the reader in a good direction when they draw up how to stop the cruel aggression and how a worldwide unity is needed. The current events happening these days in Europe as a coincidence – millions are on the move – are against the nature and represent an absurd phenomenon. After the supposed and much needed order making– which is not going to be easy and will take further financial and human sacrifices – everyone should go back to his own former home and actively take part in restarting the life there.

Naturally, this time as well, some opened and even controversial questions remained, but the authors gave a good base to the way of further thinking (not rarely only between the lines) .

What should the world do with the Kurdish problem which is directly connected to the combat against the IS (and as for the Hungarian role: we are training the Kurdish Peshmergas for military operations undertaken by themselves while our NATO allied Turkey is beating up and chasing the Kurds)?

How should more religious leaders' declarations (including the Hungarian Muslim community) be "translated" to say that the Muslim religion is peaceful, while the world is facing the opposite? How is today's IS reacting to these kinds of declarations, these kinds of religious communities?

What are the small but rich Arab countries' roles and daily practices in this entire Islam cavalcade? Can the spectacular passivity, distancing and disengagement be accepted by the world?

What kind of a result will there be after analyzing the relation between different religious trends and the IS (especially concerning the extreme – for instance Wahhabist – movements)?

There is space to overthink the scope of problems, as there is not yet light at the end of the tunnel.

The Kossuth Publishing took a praiseworthy part in assisting a 250-page volume.

The Scientific Research Centre of the General Staff of the Hungarian Defence Forces recognized the issue's relevance and appropriately reacted to the readers' demands and drew up an accurate military diagnosis when indicated for the readers what is useful or indispensable to attentively read.

This book has its place in the library of the readers, who are fastidious and opened to the world's matters.

Before we put the book on the shelf, let us remember the motto at the beginning of this writing on the vision of Churchill published 120 years ago: „Far from being moribund, Mohammedanism is a militant and proselytizing faith."

Was he right? The answer is obvious.

CONDITIONS FOR PUBLISHING IN THE NATIONAL SECURITY REVIEW

Requirements to be met by the writings

Ethical requirements:

– the writing has not been published yet elsewhere in its present form;
– it represents the author(s)' exclusive literary property, which is verified by the author(s), through his signing an author's declaration;
– it must be annotated with correct references that can be easily checked up;
– as well as with appropriate bibliographical information (including the literatures referred to, the list of Internet material, together with the date of downloading);
– it can reflect the author(s)' own opinion, which does not need to necessarily coincide with the Service's standpoint.

Content requisites:

– we publish in our reviews – in conformity with their nature – those scholarly writings (studies, essays and articles) that relate to home defense, first of all to military science, national security, intelligence, reconnaissance, military security and security policy;
– the writing must be logically worded, easy to survey, coherent, relevant and well-arranged;
– the formulation of the author(s) own concept needs to be clear, his (their) conclusions have to be well-founded, supported by clear arguments and data.

Formal requisites:

– the size of the manuscripts cannot possibly exceed the space of one author's sheet (40,000 characters or 20-21 pages); written by Times New Roman 12 letters, 1.5 spacing; the pictures and graphics prepared in an easy to be processed format (.jpg or .tif), on electronic data carrier (CD), accompanied by a printed hardcopy. All this has to be taken into account when the author(s) sends his (their) writing to our address;
– however, the manuscript can be sent also by Internet to the following E-mail addresses: natsecreview@gmail.com (National Security Review) and felderito.szemle@knbsz.gov.hu (Intelligence Review). It is necessary to attach to the manuscript the author(s)' name, rank, position, sphere of activity, permanent address, phone number and Internet address;

– we pay royalty for the accepted and published writings, based on the contract of agency, in harmony with the relevant HDF regulations and according to our available financial resources;
– the Editorial Board has the manuscript revised in every case by the Service's competent, officers (with academic degree) or other experts;
– the Editorial Board preserves the right – taking into consideration the advisers' recommendations – to deny (without justification) the publication of those works that have proved to be ill-qualified to appear. However, it does not send back such writings and does not hold them either;
– everyone is entitled to publish in our periodicals, if the Editorial Board assesses his writing – on the basis of ethical, content and formal requirements – to be suitable for being published in our reviews and on the Internet. The Board holds until the end of the given year those writings that have been accepted, but not published. If the author wishes, we are ready to return his writing to him;
– the author has to enclose in his work an "Abstract/Résumé" maximum in 10-12 lines, in Hungarian and also in English;
– he also has to provide at least 3-5 keywords in Hungarian and English;
– we kindly ask the author to send us also the correct English title of his writing.

Concrete formal requirements of academic communications

Our periodical publishes exclusively such studies that are provided with appropriate references and are prepared on the basis of the MSZ ISO 960 design standard.

The author has to attach to his communication:

– NAME OF THE AUTHOR, (his rank);
– TITLE OF HIS WRITING (in Hungarian and English);
– ABSTRACT/RESUME (in Hungarian and English);
– KEYWORDS (in Hungarian and English);
– AUTHOR'S DECLARATION.

Bibliographical reference

We kindly request the author to apply the usual numbered references, with the method to be found in "the Bibliographical references, (Bibliográfiai hivatkozások) MSZ ISO 690. p. 19-20".

If the author fails to use this method, we send back his writing for re-elaboration.

Citations:

If the author has citations within the text, he has to mark them with raised numbers (superscripts) in the order of their appearance, immediately following a passage of research information. At the foot of that same page, a note beginning with the corresponding number identifies the source of information.

First citations:

If we have a list of citations (bibliography), the first citation has to comprise at least: the author's name, his full address, the page-numbers of the citation, in such a way to be easily identified in the list of biographical references.

Examples:

1. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. p. 6.
2. Tibor ÁCS: Military culture in the reform era. p. 34.
3. Lajos BEREK: Basic elements of research work in Military Science. p. 33.
4. www.globalsecurity.org/army/iraq (downloading time: 19 04 2012)

List of biographical references (biography):

We have to fill the list by arranging the authors' name in alphabetical order.

Examples:

1. Tibor ÁCS: Military culture in the reform era. Budapest, 2005, Zrinyi Publishing House. ISBN 963 9276 45 6
2. Lajos BEREK: Basic elements of research work in Military Science. In: Tivadar SZILÁGYI (editor): Excerptions. Budapest, 1944 Zrínyi Miklós Military Academy. p. 31-50.
3. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. In: New Defense Review, 2993. 47. vol. no. 6. p. 1-7, ISSN 1216-7436
4. www.Globalsecurity.org/army/iraq (downloading time: 19 04 2012)

Requirements for pictures, sketches, illustrations, diagrams and other appendixes:

– title of the picture or illustration;
– source of the picture or illustration (or its drafter);
– serial number of the picture or illustration, (e.g. 1. picture);
– if it is possible, a Hungarian legend should be provided when the caption of the picture or illustration is given in a foreign language.

Requirements for abbreviations and foreign terms:

– foreignisms and abbreviations should be explained – at their first appearance – in the footnote, in Hungarian and in the original foreign language;
– e. g. WFP – World Food Program – ENSZ Világélelmezési Programja.

Points of Contact of the MNSS Scientific Board:

Postal address:
Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1502 Budapest, Pf. 117

E-mail: natsecreview@gmail.com

Dr. Vida Csaba alezredes
a Tudományos Tanács titkára
E-mail: vida.csaba@knbsz.gov.hu

Háry Szabolcs alezredes
felelős szerkesztő
E-mail: hary.szabolcs@knbsz.gov.hu