Evaluation, Analysis and Reporting at the Beginning of the 21st Century

Kund Miklós Regényi*

Abstract

The basis task of every intelligence service, the evaluation, analysis and reporting has always been of utmost importance, yet this impotance is still growing in the first half of the 21st century.The war in the Ukraine higlihgts the value of correct and reliable analysis and reporting as well.However, this branch undergoes changes and challenges due to intelligence sharing policies and the rapid evolution of artificial intelligence. This study outlines how abovementioned phenomena can shape the intelligence & reporting work in a modern intelligence community.

Keywords: *evaluation, analysis, reporting, artificial intelligence (AI), intelligence sharing, information security, information cloud, fusion centre*

Introduction

It cannot be emphasized enough that of the two great predictions of the end of the short 20th century, the end of the Cold War – that is, the end of history[1] or the clash of civilizations[2] – the latter seems to be coming true. The obvious and true conclusion is that our world, if it is capable of providing a comfortable and livable home for billions of people, has become extremely complex. Prosperity and freedom may just be a short transition before the deep contradictions that Huntington described as the clash of civilizations surface.

There is no doubt that for the national security services dedicated to identifying hidden and man-made challenges, this means continuous testing and adaptation. It is also clear that summarizing the acquired knowledge, orienting the collecting of information and, above all, providing the decision-makers with adequate and credible, well-founded information are more important than ever (although they have always been important). In the present research article, I will show that this is the area where the biggest changes have occurred. By way of analogy, a meeting with a secret human source in 1917 was very similar to the one in 2017. If anyone could get into a time machine and witness such a conversation, the expert would immediately recognize what it was about. All of this cannot be said about evaluation, analysis and reporting system.

* Ph.D. isan assistant lecturer at the National Security Institute, University of Public Service, Budapest, Hungary; ORCID 0000-0003-1833-9523.

[1] See Fukuyama.

[2] See Huntington.

Basic concepts

In order to present the changes, it is worth familiarizing ourselves with the basic concepts. The process of evaluation, analysis and reporting is often referred to collectively[3], which is correct, as it is a process that builds on each other. However, for a better understanding, let us now isolate and separate the individual elements. The evaluation is nothing more than a thought process during which we determine what the generated information is good for, i.e. which element of the organization's task system it promotes, if at all; and how good it is, i.e. how authentic and how verified. In practice, we can place the generated information along four axes. The first is the intelligence tasking, i.e. whether the generated information can be matched to any element of the intelligence tasking. The second is the aspect of the specific professional work process – this is usually the advancement of case processing in the operational work – i.e. the extent to which the generated information justifies or refutes the basic assumption. There are two other axes. One is the expansion of the conditions of secret reconnaissance. A simple example: if a person posts on social media that he will be on vacation abroad for two weeks, at first glance it does not help our professional work, but in fact it does a lot, since during this period we can take operational measures that can put our investigation in a better position. The fourth axis is also important, since we list here the part of the information that is not relevant for our organization, but may be significant for cooperating law enforcement organizations, for example, they indicate or prove the existence of a crime or criminal organization. In this case, the information must of course be transferred to the cooperating organizations.

The next work process, the analysis, will be discussed in more detail in the next part of the paper. I note here that analysis is the process of uncovering hidden connections, identifying and eliminating parallels, and creating an overall information picture. This is the level that orients covert reconnaissance; furthermore, this is the level where the information picture is being modified and adapted to reality, taking into account the new knowledge of secret reconnaissance.

Speaking about the reporting, as the name clearly shows, it means the work process when decision-makers receive relevant, authentic and up-to-date information, on the basis of which they can make the strategic decisions that are of outstanding importance from the point of view of the country, or at least the sphere of national security. The information can be made upon tasking, this would correspond to the professional model known as the intelligence cycle, but of course it is expected that an organization draws the attention of decision-makers to those processes and phenomena that could have remained hidden and did not appear on the surface. It is clear that the information must also cover the proposed measures and their beneficial and adverse effects.

The new face of analysis

As already mentioned, analysis is the most exciting part of data processing. This is where most of the values added to the information by the national security organizational system are formed. This is the work phase that shows the most changes at the beginning of the 21st century compared to previous years. As a point, it should be mentioned

[3] See related chapters in Lowenthal and Graves.

that information should be stored in a way that can be identified, sorted and rearranged. This requires data about the data, i.e. metadata. We can create metadata ourselves, but in such an obvious way for the location and source of the information, the persons, devices, vehicles etc. included in it.

The data has been stored in electronic form for a long time, which of course raises the question of the authenticity of the data. Basic data must be available to analysts in a non-modifiable form. An even more exciting question is that the structured data repositories typical of previous decades – which implemented the placement of data and then querying the stored data based on a predetermined (and constantly expanded) system of criteria – seem to be fading away, since artificial intelligence-based search engines are the preliminary criteria perhaps making its definition redundant. I will return to this later.

It is also a challenge that so far the information has been available to analysts mainly on a textual basis. It is quite clear that this situation is changing rapidly. The vast majority of information is now available in image and sound formats. Their quick storage and retrieval becomes particularly important, taking into account the increasing popularity of the new generation of analysts, who can be defined as 'digital natives'.

Another practical dilemma is the issue of internal information flow. Currently, the process is taking place, where the laborious, time-consuming and, not least, soul-killing process of preparing an extract from the report and another extract from the extract, i.e. the manual processing of the basic information, is increasingly being replaced by the automatic provision of assignments of various degrees and levels to the recorded information, obviously predetermined criteria and search terms. If this is necessary from the point of view of data security, sending instead of assigning, i.e. physically placing or moving to another storage location is also conceivable.

Perhaps the most important dilemma of analytical work is the dilemma of information security and information exchange. Information security basically corresponds to the classic practice of information collecting, according to which everyone can only know – but must know – only as much of the information as is necessary to carry out their work. This basic principle served well in the past centuries of the development of secret services, and it still serves well today in the phases of secret reconnaissance and information collecting. In contrast to this is the aspect of information exchange, which suggests that in order to uncover hidden connections and create the details of the operational situation, it is advisable for the individual analyst or the analysis group to get to know the widest possible range of information, preferably the entire range, since in our complex world, quick and effective situational awareness it is the only way.

It is clear that the two aspects are quite opposite. In the work of a national security service, the aspects of security and information security can never be neglected. How should this contradiction be resolved? Obviously, it is extremely important to be able to demonstrate who accessed each piece of data, when and why. Of course, it is also necessary to be able to show what basic information was used to prepare a summary, similar to the footnotes of a scientific work, even if these footnotes are not necessarily displayed. It is also clear that, with the complex application of operational forces and tools, a kind of protection must be implemented around the analyst's work area, electronic devices and person, which extends from simple regime rules through elements of cybersecurity to human security. All these rules can only fulfill their purpose if the staff is prepared for them, their organizing principles are clearly presented, and thus they create a kind of internal identification between the analysts and the regime rules that make their work more complicated on the surface – but actually make it possible at all.

The explosive increase in the amount of available data resulted in a qualitative change in the analytical processes. Today, the number of elementary data is not measured in hundreds of thousands, but in millions. This change induces further very important changes, which is both an opportunity and a challenge for national security analytical work. Platform fusion should be presented as an opportunity. Here, we mean that data from different systems are available to the specialist involved in the information acquisition at the same time, in the case of analytical or simpler data, on the same platform. Here follows a simple example: if, during the collecting process, social media information about the person subject to the measure is also displayed, it can orientate the measure and significantly advance the taking of adequate response steps.

The next considerable problem and challenge are how to find and retrieve large amounts of data and to identify, represent, and possibly interpret the relationships between them. It is obvious that this requires computers, it is obvious that this requires self-learning, i.e. computer programs capable of improving themselves, which we commonly call artificial intelligence[4]. This significantly reshapes the evaluation and analysis work, since in many cases, indeed, most often, you do not have to work with information itself, but you have to control the computer. Intuition, personal identification with the task, even under these circumstances, I believe, are values to be preserved.

The expansion of computers and computer programs requires new skills from the analyst. You need to be aware not only of a specific topic, and not only of secret intelligence and the work processes and task system of the organization, but you also need to understand computer data processing. It is a huge challenge to find such broadly qualified people, or to train them. It is clear that both paths must be taken, i.e. specialists with appropriate basic qualifications must be attracted to the services, and in parallel the existing staff must be trained in order to use the technical systems at the highest possible level. It is an interesting phenomenon that the ever-expanding internal world of information technology creates more and more people who are so specialized that they can solve almost everything in the world of computer technology, but they do not move so confidently outside the world of computer technology. It is expected that a new type of professional will appear: a professional who acts as a connection point between the world of computing and the world of national security challenges; is able to understand and formulate problems in such a way that it is understandable and manageable for the other side.

The next phenomenon is that a new kind of quality is created through the analysis of a large amount of data, which does not necessarily bear the characteristics of evaluation and analysis work in the classical sense, but can rather be described as a kind of information acquisition - i.e. the generation of basic information that becomes the subject of later analysis processes. From the organization's point of view, this means that the phases of analysis and covert reconnaissance and operational data collection are blurred. An example: by analyzing the data of public area video recording cameras, the movement pattern and relationship system of a target person can be created, i.e. with data analysis, we can obtain the kind of knowledge that, according to the classical working method, is created as a result of the work of surveillance[5]. (Another such field could be the analysis of open source information.)

---

[4] For an easy-to-use definition from the legal perspective see Eszteri.

[5] The phenomenon become the general principle in the well-known intelligence handbook of Rolington.

The peculiarity of the operation of machine learning is that it can make use of its self-learning ability only by using it as widely as possible, and by applying the principle of trial and error as widely as possible, in the same way as its creator, humans learn. The obvious conclusion from this is that artificial intelligence-based programs should not only be used as widely as possible, but so-called learning data, i.e. data that is not connected to a specific task but professionally relevant, should also be processed by the system in order to use it as efficiently as possible in the future. It is not only necessary to create the technical conditions for this, but also the legal conditions, since the stockpiling type of data collection and the storage of data over a longer period of time are often subject to legal restrictions.

I have already pointed out that the development of artificial intelligence may render the maintenance and further development of structured data repositories unnecessary. In other words, the systematization and recording of data in a database – whether done by manual or machine work – can become unnecessary, the manpower, working time and financial resources spent on this can be better utilized elsewhere. This option is undoubtedly very tempting. However, in addition to the advantages, the elimination of structured data repositories also has disadvantages. The result of data extraction from an unordered data set with artificial intelligence always results in a larger hit field, just think of the dilemma of evaluating and using a query made by the Google search engine. In relation to work organization, this means that the work that we apparently saved during the organization of the data does not disappear, it is only transformed; we have to do it during data extraction and interpretation of the extracted information set. That is, the savings do not occur at the system level, but only in relation to certain subsystems.

The new face of reporting

After the problems of the analysis have been reviewed, it is worth spending a few thoughts on the possible dilemmas of the reporting. The terrorist attacks of 2001 led to very extensive systemic investigations within the US Intelligence Community. One of the big lessons was that the system contained a lot of information that, when summed up, could have led to the adoption of overt measures suitable for thwarting terrorist attacks. However, this information was not found, and this can be traced back to, among other things, the fact that law enforcement and national security services are hierarchically functioning, highly structured systems, where information is provided in a well-established way, in compliance with the rules of competence and authority[6]. This in itself is a kind of hindrance for data collectors and analysts, in the sense that it delays the formulation of primary conclusions and their official dissemination. This is humanly understandable, since who would want to attract the attention of the management with his insights, conjectures, which at first seem foolish, and his ideas that cannot or hardly fit into the previous way of thinking. As a result, however, the information did not reach the decision-makers and they could not meet to be the subject of a thorough analysis. It is, therefore, necessary to create the conditions for the information to be provided in a kind of "information cloud" (i. e. in a low-hierarchical manner, for a wider group of people that may not even be fully defined in advance).

[6] See the 9/11 comission report. https://govinfo.library.unt.edu/911/report/911Report.pdf.

The concept of information fusion centers is logically similar, but organizationally very different. This refers to organizations that are in possession of the information of not one, but many, preferably all, law enforcement and national security agencies, and thus, by following all information and filtering out possible contradictions, they are able to provide decision-makers with efficient, time- and energy-saving, so-called single-channel information. Obviously, such an organization must find its place and role among the long-standing members of the national security community. The history of development of the American OSS and the CIA clearly shows how it is not a simple process[7].

The medium that carries information is also changing. Nowadays, informational work is predominantly carried out in the form of paper-based, textual reports and information supplemented with images and maps. In addition, the value of direct oral information, in other words the genre of briefing, during which the manager or the expert verbally informs the customer about the available knowledge, usually supplemented with projected images, is of course increased. This genre strengthens and deepens the mutual trust between those who order the information, that is, the decision makers, and the national security organizations that extract the information. The parties get to know each other's way of thinking and world view. It is also a serious advantage that possible contradictions and unclear details can be clarified immediately. It is also possible to immediately formulate and issue tasks and measures related to the information. Obviously, all of this must be recorded in writing.

Changes are also being prepared at the other end of the spectrum. It should be taken into account that the generation that basically acquires its knowledge from social media, internet channels, and mobile devices is already in a decision-making position, and it is obvious that it also adheres to this medium as a decision-maker. I will not go into the technical and security aspects of the problem now, as they would fill a separate research article. From the point of view of informative work, this means that information should not be recorded in the form of text, but in the form of images and/or infographics. This again raises questions such as those I have already mentioned in connection with the general rise of computer technology. It is clear that the practitioners of the assessment and analysis profession need to be enriched with new skills.

Of course, customers raised on social media have a different attitude to the dilemma of information exchange, since sharing information is a value in the world of Facebook and its clones. I believe that a serious educational process is needed here, the center of which should be the responsibility of the user, i.e. the conscious commitment that the possession of the information provided to him or her/them – and otherwise extremely exciting, thus almost provoking sharing – obliges him or her/them to refrain from sharing for the sake of the greater good, the security of the country, the homeland, or perhaps the military and / or economical alliance, and to preserve your competitive advantage. The fact that the problem is real has been highlighted by recent scandals (for example, the forwarding of official correspondence to private mailboxes)[8].

As a final thought, a question must be formulated: if centers carrying wide-ranging – comprehensive at the level of needs – knowledge in a concentrated manner, freely connecting knowledge with each other and thus creating new value, appear and spread, what effect will this phenomenon have on the role of the so-called case officers? In

[7] Office of Strategic Services and Central Intelligence Agency, see https://www.cia.gov.

[8] To underline the importance of this, consider the fact that Donald Trump's – for that time the President of the United States of America – had 77,7 million followers on 20. April, 2020.

other words, where will the place be for those professionals who plan, organize and carry out the next steps of operational intelligence in the processing of a case with all partial knowledge. Isn't there a danger that those directly involved in the data collection will learn less and less about the real purpose of the data collection and will increasingly strive for the technical realization of the implementation in a broader sense. Should we be afraid of this at all, or should we rather welcome and speed up the process?

I cannot provide answers to these questions at this time. However, a hypothesis can be formulated that people who are able and ready to act autonomously have a place in the system of secret reconnaissance of the present and the future. I believe that, if not elsewhere, the role of business managers in today's sense will remain in the process of obtaining information from human resources. Obviously, their analytical support can represent another step forward in terms of working more efficiently in an increasingly complicated world, and this step forward is also needed.

References

1. Huntington, Samuel P.: The clash of Civilizations and the Remaking of World Order. New York, 2011, Simon & Schuster. ISBN 978 1451 628975.

2. Fukuyama, Francis: The End of History and the Last Man. New York, 2006, Simon & Schuster, ISBN 978 0743 284554.

3. Jensen, Carl J. – McElreath, David – Graves, Melissa: Introduction to Intelligence Studies. Milton Park / Philadelphia, Taylor & Francis Group – Rutledge, 2022 3. ISBN 978 0367 711566.

4. Lowenthal, Mark M.: Intelligence. From Secrets to Policy. Newberry Park, Sage Publishing – CQ Press, 2022 9. ISBN 978 1071 806371.

Rolington, Alfred: Strategic Intelligence for the 21st Century: The Mosaic Method. Oxford, Oxford University Press, 2013. ISBN 978 0199 654321.

5. Eszteri, Dávid: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései [Certain responsibility aspects of the development and use of Artificial Intelligence], in: Infokommunikáció és jog [Law and info-communication], 12, (2015), Vol. 62-63, pp. 45-57. ISSN 1786-0776.