Leszek Wiszniewski

The role and significance of intelligence analysis in ensuring national security

In the 21st century people are forced to receive ever greater amounts of more or less useful information. One of the main factors influencing this phenomenon is technology developing at a staggering rate. People using the internet, including social media (e.g. Facebook, Twitter, YouTube), are the addressee of 34 gigabytes of data, which according to the scientists from the University of California in San Diego translates into 100,000 words daily (twice as much as at the beginning of 1980's)[1]. This results in the necessity to process information quickly and to rank it according to its significance. The politicians in our country holding managerial positions face similar problems. Information overload often impedes making the decision on which human health and life may depend. Therefore, due to the dynamically changing environment of national security as well as multitude of challenges and threats arising from this process, the significance of data analysis will be increasing. Of particular importance are materials drawn up on the basis of data coming from covert sources, which enable the geopolitical situation assessment (e.g. in case of hybrid activities carried out by an opponent, including disinformation) and taking pre-emptive action (e.g. preventing terrorist attacks by arresting people involved in their preparation or preventive use of security measures in case of vague signals of potential threats). The role of secret services (foreign intelligence and counterintelligence) and uniformed services will also be enhanced. The legislator gave them the competence to gather information by intelligence operational activity as well as to draw up on its basis adequately prepared analytical products for decision-makers.

In the first part of the work the problem of data analysis will be discussed from a theoretical standpoint, including definition issues and analytical cycle with particular emphasis on the ways of collecting information and different kinds of analysis. In the second part, legal conditions regarding selected Polish institutions responsible for ensuring security and preparing analyses within their scope of competence will be presented.

---

[1] *The American Diet: 34 Gigabytes a Day*, https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [access: 3 IX 2019].

Definition issues

At the beginning of the deliberations on data analysis we should refer to scientific literature in order to properly understand the terms used in this study. According to the definitions found in the *Polish Scientific Publisher Dictionary of the Polish Language* (Polish name: *Słownik Języka Polskiego PWN*) analysis is 'mental retrieving of characteristics or components of the examined phenomenon or subject'[2], whereas information is 'notifying of something, communicating something; message, instruction'[3]. In academic materials a phrase appears that 'information' is (…) *a collection of facts, events, features etc. of defined objects (things, processes, systems) contained in the message (communication), and expressed in such a way (form) that the recipient can respond to the situation that has arisen and undertake mental or physical action*[4]. In the specialist military and security literature one can read that (…) *data analysis in the area of national security consists in giving sense to this information, so (1) it includes correct inference about the consequences of the content of information and (2) it maximizes the usefulness of the information in making decisions by the recipient by formulating recommendations of specific action*[5]. Understanding the concept of information security remains an essential question. In the publications on the subject it is used in two contexts. The first of them refers more to information processing threat which is confirmed by Piotr Potejko (*information security is a set of activities, methods, procedures, undertaken by authorized authorities in order to ensure the integrity of the gathered, stored and processed information resources by securing them against adverse, unauthorized disclosure, modification or destruction[6])* and Krzysztof Liedel *(information security is very often understood as protection of information against adverse – accidental or aware – disclosure, modification, destruction or preventing its processing*[7]). Slightly different understanding of the term is suggested by Leszek Kwiatkowski, who claims that (…) *what is meant by information security of the subject (man or organization) is the possibility of obtaining information of high quality as well protecting the possessed information against loss*[8]. This view is shared by Krzysztof Liderman *(information security signifies justified trust in the quality and availability of the obtained and*

[2] L. Drabik, E. Sobol, *Słownik języka polskiego*, Warszawa 2005, p. 14.

[3] Ibidem, p. 277

[4] P. Sienkiewicz, *10 wykładów*, Warszawa 2005, p. 62.

[5] J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, p. 256.

[6] P. Potejko, *Bezpieczeństwo informacyjne*, w: K.A. Wojtaszczyk, A. Materska-Sosnowska (ed.), B*ezpieczeństwo państwa*, Warszawa 2009, p. 194.

[7] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, p. 19.

[8] L.F Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, p. 147.

used information[9]) and Józef Janczak together with Andrzej Nowak who claim that (…) *when there is talk of information security it always refers to the subject which is threatened by lack of information or the possibility of losing information resources*[10]. The National Security Bureau experts made an attempt to clarify the term information security of the state. They presented the information security of the state in *The doctrines of information security in the Republic of Poland* (Polish name: *Doktryny bezpieczeństwa informacyjnego RP*) of 2015 as:

> (…) cross-sectoral area of security whose content refers to informational environment (including cyberspace) of the state; a process which aims to ensure secure functioning of the state in the informational space by controlling its own, internal infosphere as well as effective safeguarding national interests in the external (foreign) infosphere. It is achieved by conducting the following tasks: providing adequate protection of the possessed information resources and protection against hostile disinformation and propaganda activities (in the defensive sense), while simultaneously maintaining the capacity to conduct offensive activities in this area against potential opponents (countries or other entities). These tasks are specified in the (operational or preparatory) strategy (doctrine) of information security, while an adequate information security system is maintained and developed in order to execute them[11].

For the needs of this work it is worth adopting a broader definition – suggested by L. Korzeniowski or K. Linderman – of the term 'information security', which refers to the capacity of obtaining information allowing decision-makers to ensure national security.

The subchapter devoted to the definition issues is where it is worth explaining what propaganda (disinformation) and informational noise are, which have recently become a debate subject in the Polish public space. Disinformation is a message incompatible with the reality which may become (...) *an element of information fight between competing entities*[12] (e.g. states or companies). Propaganda and disinformation were more broadly defined in the project The doctrines of information security in the Republic of Poland: (…) *spreading manipulated or fabricated information (or a combination of both) in order to make the recipient behave in a specific way beneficial to the one who disinforms or in order to distract the attention from the actually*

---

[9] K. Liderman, *Bezpieczeństwo informacyjne*, Warsaw 2012, p. 22.

[10] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, p. 18.

[11] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [access: 3 IX 2017].

[12] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, p. 36.

existing events[13]. Whereas linguists define the term informational noise as 'an excess of information hampering the extraction of true and essential information'[14].

Intelligence cycle

Data analysis is only one of a few stages of a broader process which aims to support the authorities of a given state in decision-making, allowing them to ensure broadly understood security of the citizens. In the publications on the subject this process is traditionally referred to as intelligence cycle, which usually consists of – depending on the taxonomy adopted by particular scientists – four to six stages. For the purpose of this publication four phases of this cycle have been adopted which include:

1) **defining the information demand** by state organs which are authorized to do so under applicable law and commissioning tasks to the subordinated institutions (e.g. security and public order services, intelligence and counter-intelligence agencies). This stage is closely correlated to the current global events and occurrences (e.g. armed conflicts, terrorism) which may have negative influence on the national security. It is on their basis that the government lays down the guidelines for the activities of the services. In this context it is necessary for the decision-makers to be able to prioritize threats;
2) **collecting information by services according to the authorities' needs**;
3) **analysing the gathered data**[15];
4) **passing the final analytical products (in accordance with competences) to the recipients**. Tomasz Aleksandrowicz notices that this stage – in case when there is no reaction of the authorities to the received document – concludes the intelligence cycle, and if another commission appears then we deal with so-called open intelligence cycle[16].

[13] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP…*

[14] http://sjp.pwn.pl/sjp/;3067966 [acces: 13 V 2017].

[15] The problem of collecting data and its processing will be presented in the further part of the publication.

[16] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie,* Warszawa 1999, pp. 55–56.

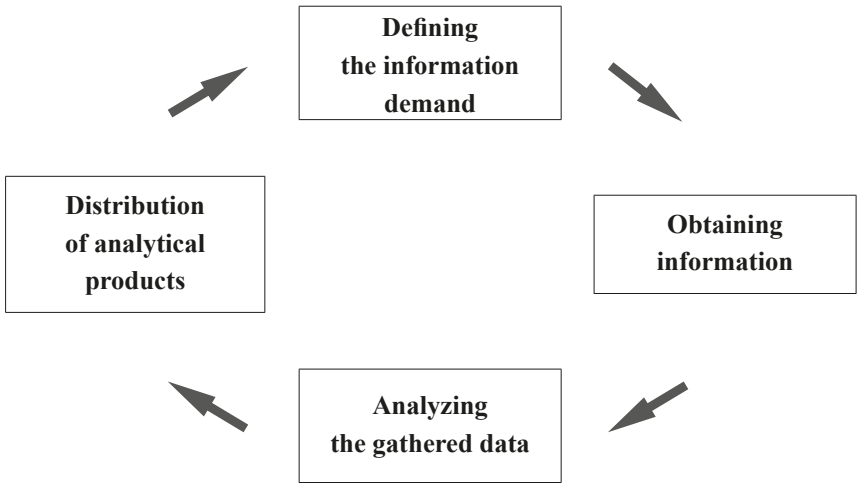

Figure. Intelligence cycle.

Source: Self-study based on K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa, pp. 82–87.

It is worth presenting a few examples of disturbing the information cycle. Experts distinguish mistakes made both by decision-makers and analysts. The recipients of the final products may:

- formulate their needs in an unclear way which may result from the lack of ability to use the possessed forces and resources, including secret services;
- not use the knowledge and conclusions presented in the documents[17]. In this context it is worth pointing to the problem described in the social psychology by prof. Irving Janis i.e. groupthink syndrome (GTS). It is defined as (…) *an irrational pattern of thinking and behaving in a group, which imposes an artificial consensus and suppresses any dissenting voices*[18]. It means that decision-makers (politicians or military commanders) as members of a bigger group may yield to it and – being afraid of exclusion – they may willingly limit their intellectual scope for adequate situation assessment. Some of the GTS examples – mentioned by I. Jenkins in the article *Groupthink*, published in 1971 – are wrong decisions made by the Americans, including lack of proper preparation for the Japanese attack on Pearl Harbor, the failed Bay of Pigs invasion and the decision to increase American involvement in the Vietnam War[19].

[17] J. Konieczny, *Analiza informacji w dziedzinie*…, p. 248.

[18] K. Albrecht, *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, p. 217.

[19] I. Janis, *Groupthink*, "Psychology Today" 1971, no. 6, pp. 43–46, 74–76.

Mistakes may also appear at the stage of preparing analytical material for the final recipient. Among the most frequent of them are[20]:

- the conviction that the amount of material necessary to create the analytical product for the external receiver is sufficient and lack of interest to use the incoming information which affects the assessment of the threat (this behavior may result from an analyst's laziness, who already has his draft document prepared and accepted and new data radically changes the adopted assumptions, which entails further work on the same document);
- lack of proper verification of the information supplied by the source. False news may distort the picture of reality which may lead to politicians making wrong decisions;
- writing according to the expectations of the addressees or supervisors (e.g. people responsible for processing data fearing for their career may present in the analyses the assessments and theses compatible with the way the management of their institution see the world);
- delay in material transfer (lack of information at the appropriate time hinders making the right decision).

Methods of collecting information

A data analysis is preceded by the process of obtaining this information. In the publications on the subject a great number of methods of gathering information on national security are mentioned. Currently, one can point to at least a few of them. Among the most popular ones one should point to:

- **OSINT** (Open Source Intelligence) called also *white intelligence* in Polish – collecting information from overt sources i.e. traditional and electronic media, social media (e.g. Facebook), official state registers, public administration documents made available to the public, lectures, science conferences and materials which can be accessed without special permits or skills. In the recent years OSINT has become an invaluable source of knowledge as a result of the progressive phenomenon of digitalisation, ever greater internet access and human willingness to share a broad spectrum of private information using social media.
- **HUMINT** (Human Intelligence) is obtaining knowledge from so-called personal sources of information. HUMINT should be understood as classic intelligence activities. Mostly, state institutions (e.g. secret services) authorized to conduct intelligence operational activity attempt to come into possession of materials from people having information of essential importance for internal or external security of the state, its constitutional order, the position of the state

[20] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, pp. 112–115.

on the international stage as well as its military and economic potential. Secret service officers use a broad spectrum of tools to initiate a contact and later to recruit. In the publications on the subject it is pointed to different kinds of motivation of the people who agree to cooperate with security institutions. The most popular theory makes reference to the acronym **MICE** (i.e. Money, Ideology, Coercion, Ego). According to its assumptions people pass information to the services due to, e.g. money received in return, opinions held by this person, fear of being discredited;

- **SIGINT** (Signals Intelligence)[21] which includes: **COMINT** (*Communication Intelligence* – communication information which comes from phone calls, conversations held on radio and other means of communication), **ELINT** (*Electronic Intelligence* – data coming from analysing electromagnetic signals, not used in telecommunication) and **TELLINT** (*Telemetry Intelligence* – technical and intelligence information coming from the gathered and processed light signals or foreign telemetry). In conclusion, SIGINT involves obtaining information by means of radars, phone tapping, directional microphones, and – possibly first of all – the control of the information flow on the internet. Currently, when one takes into account many users' low awareness of ensuring security of their action in the cyberspace, the materials originated in such a way become incredibly precious not only for hackers or criminal groups but also for state services which in a covert way and under the applicable law should obtain any knowledge of interest to them. At the same time, because of a large amount of information sent via telecommunication networks, gathering and analysing it requires specialist skills or computer software which support the processing of the gathered materials.
- **IMINT** (Imagery Intelligence) which is designated in the literature as **PHOTINT** (Photo Intelligence)[22] – obtaining knowledge, e.g. from photographs taken by satellites equipped with high-quality cameras or by officers during surveillance of people or installations. Information obtained in this way allows… to indicate or confirm undesired environmental changes (e.g. movement of enemy troops, new constructions developed for military use);
- **MASINT** (Measurement and Signatures Intelligence) – scientific and technical intelligence received by quality and quantity data analysis (metric, angular, spatial, wavelength, time relationships, modulation, hydromagnetic) coming from specialized technical sensors[23].

[21] Own translation based on: *Global National Security and Intelligence Agencies Handbook*, Washington 2015, p. 279.

[22] Ibidem.

[23] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji…*, p. 59.

Types of analysis and analytical techniques

Another stage of the intelligence cycle is the analysis of the knowledge gathered according to the request of the politicians holding managerial positions in the state. One can point to at least two main **types of analysis** constituting support in the decision-making process. These are:

- **strategic analysis** – understood as comprehensive diagnosis of the past and present events, which enables us to prepare a forecast of security threats in the wide sense of the term as well as conclusions and recommendations. They enable the recipients of such material to make a decision bringing long-term effects;
- **signal analysis** – prepared on the basis of the services' current work. Usually it takes the form of one or two paragraph long so-called information cube. In the material consisting of one paragraph only (its form resembles press release) one can find answers to the most basic questions (who? what? where? when?). In case of analyses of two paragraphs short conclusions and possible recommendations are included additionally.

Analytical techniques used in the course of preparing documents essential to the national security are a separate issue. The more interesting of them are:

- **high impact and low probability analyses.** Their authors describe events which may imply serious consequences for the national security but the probability of their occurrence is not large. Important elements of such a study are: diagnosis how an undesired situation may occur and indicators (so-called red flags) warning against approaching danger;
- **future occurrence scenario analyses.** On the basis of the gathered information, own experience and knowledge of typical cases analysts prepare the event forecast in the short, medium and long term. Usually, this kind of analysis consists of three possible versions (scenarios); an optimistic one (the most beneficial for the state), a pessimistic one (negative) and the most probable one;
- **"red hat" analyses.** Their aim is to recreate opponent's pattern of thinking (people, terrorist organizations) and to predict – including all variables – their possible decisions in the future (including potential decisions, e. g. undermining the national security).

Collecting and processing information by selected state institutions

In the Polish security system numerous state institutions function which prepare analytical products for decision makers. The scope of the information which is necessary to prepare analyses passed to and processed by particular entities is varied

and results from their statutory competence. Civilian secret services gather different kinds of information than military ones and law enforcement organs gather still others.

Polish counterintelligence and intelligence – acting under, and within the limits of the law – are responsible respectively for (…) *acquiring, analysing, processing and forwarding to appropriate authorities information which may be vital to the protection of internal security of the state and its constitutional order*[24] (Internal Security Agency, Polish acronym: ABW) and for (…) *acquiring, analysing, processing and forwarding to appropriate organs the information that may be vital to the security and international position of the Republic of Poland and its economic and defensive potential*[25] (Intelligence Agency, Polish acronym: AW). At the same time, the Heads of the ABW and AW are obliged to pass, without delay, to the President of the Republic of Poland and to the Prime Minister the information which may be vital to the security and international position of the Republic of Poland. Furthermore, unless the Prime Minister decides otherwise the Heads of the ABW and AW pass the information to constitutional ministers in accordance with their competence[26].

At the stage of gathering information officers use the powers defined in chapter 4 of the *Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002*. Among these powers, there are:

- intelligence control (including obtaining and recording the contents of telephone conversations by applying technical measures, also transmitted via telecommunication networks as well as the vision and sound of people from rooms, means of transport or space other than public)[27];
- covert cooperation with persons not being secret service officers[28];
- assistance of organs of government administration which are obliged to pass to ABW or AW information vital to the external security and international position of the Republic of Poland[29].

Processing the gathered information takes place in the specialized organizational units of particular services. There is no possibility to determine their detailed scope of competence on the basis of open sources of information, since these issues are regulated by regulations on classified information. A change to the organizational structure of the Internal Security Agency testifies to the growing significance of data analysis. In November 2018 *Ordinance no. 163 of the Prime Minister of 26 September 2018 on granting the Statute of the Internal Security Agency*[30] came into force. In ccordance

[24] *Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency* (i.e. Journal of Laws of 2016, item 1897, as amended), art 5.

[25] Ibidem, art. 6.

[26] Ibidem, art. 18.

[27] Ibidem, art. 27.

[28] Ibidem, art. 36.

[29] Ibidem, art. 41.

[30] M.P. of 2018, item 927.

with its provisions a new Department of Information, Analysis and Prognosis was separated from, as one can presume, Registry and Analysis Bureau (called also Bureau E). Currently, most probably its officers are responsible for preparing analytical products in the Internal Security Agency[31]. Moreover, one can conclude that – drawing on the interview with Gen. Adam Rapacki conducted by Krzysztof Liedel – terrorist threat analysis may be, to some extent, performed by the Counterterrorism Centre which was set up pursuant to the *Ordinance no. 102 of the Prime Minister of 17 September 2008 amending the Ordinance on granting the Statute of the Internal Security Agency* (act. repealed – note ed.). Gen. Rapacki indicated that (…) *apart from processing information of operational character the Centre prepares analyses on particular issues in order to render the knowledge distributed form the Centre uniform for all entities*[32]. In case of the Intelligence Agency even such deliberations were impossible until recently, since the statute of this institution did not reveal which organizational unit was responsible for data analysis (almost all of them bearing name: bureau)[33]. In this respect a change also took place in 2018. Pursuant to the *Ordinance no. 106 of the Prime Minister of 3 July 2018 amending the Ordinance on granting the Statute of the Intelligence Agency*[34] a new unit was created – the Department of Information, which – just like in the case of ABW – presumably prepares analytical work for the authorities of the RP[35].

Another scope of information is obtained and processed by military secret services. The Military Counterintelligence Service (Polish acronym: SKW) is obliged to (…) *acquire, gather, analyse, process and transfer information meaningful for the national defence, security or combat capacity of the Armed Forces of RP or other organizational units of the Ministry of National Defence*[36]. Whereas, the Military Intelligence Service (Polish acronym: SWW) acquires, gathers, analyses, processes and transfers to competent authorities information meaningful for the defence potential of the Republic of Poland, security and combat capacity of the Armed Forces of RP as well as the conditions of fulfilment of tasks outside the country by the Armed Forces of RP. This service also identifies and analyses threats which may affect the defence potential, appearing e.g. in conflict regions[37]. The Heads of SKW and SWW pass the gathered and processed information – after notifying the Minister of National

[31] Ibidem, § 3

[32] K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa,* Warszawa 2010, p. 132.

[33] *Announcement of the Prime Minister of 14 September 2016 on the publication of a uniform text of Ordinance of the Prime Minister on granting the Statute of the Foreign Intelligence Agency* (i.e. M.P. of 2016, item 936), § 3.

[34] M.P. of 2018, item 660.

[35] Ibidem, § 1.

[36] *Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service* (i.e. Journal of Laws of 2016, item 2138, as amended).

[37] Ibidem, art. 6.

Defence – without delay to the President of RP and the Chairman of the Council of Ministers. Moreover, if the information relates to the scope of activity of a competent minister they pass the information to this minister, unless the Chairman of the Council of Ministers decides otherwise[38].

At the stage of gathering information the SKW and SWW officers have the power to conduct activities defined in Chapter 3 of the *Military Counterintelligence Service and Military Intelligence Service Act of 9 June 2006*. In numerous cases they are in line with the ones prescribed for ABW and AW (e.g. intelligence control or covert cooperation with persons not being secret service officers). At the same time, it is difficult to determine which organizational units inside SKW and SWW are accountable for data analysis since their structure remains secret. (the legislator using terms like: department, board, bureau[39]).

The Central Anti-Corruption Bureau (Polish acronym: CBA), created in 2006 (…) *as a secret service to combat corruption in public and economic life, particularly in public and local government institutions as well as to fight against activities detrimental to the state's economic interests*[40], was obliged (…) *to conduct analytical activities concerning phenomena falling within the CBA's competence as well as presenting information within this scope to the Chairman of the Council of Ministers, the President of the Republic of Poland, the Sejm and the Senate*[41].

At the stage of gathering information CBA officers use the powers defined in chapter 3 of the *Act of 9 June 2006 on the Central Anti-Corruption Bureau*. In case of CBA they are also often in line with the ones prescribed for ABW, AW, SKW or SWW (e.g. intelligence control, covert cooperation with persons not being secret service officers). At the same time, presumably the Analysis Department is responsible for processing and analysing information acquired as a result of intelligence operational activities[42].

The Police and the Border Guard (Polish acronym: SG) which are supervised by the Minister of Interior and Administration, while conducting their statutory tasks also acquire intelligence information. Therefore, the Police processes data related to (…) *protection of public safety and order, including ensuring peace in public places and in public means of transport, road traffic and on waters allocated for common use*[43]. Whereas the Border Guard (…) *gathers and processes information concerning*

---

[38] Ibidem, art. 19.

[39] *Ordinance of the Minister of National Defence of 21 April 2017 on granting the Statute of the Military Counterintelligence Service (M.P. of 2017, item 431) and Ordinance of the Minister of National Defence of 13 June 2018 amending the Ordinance on granting the Statute of the Military Intelligence Service* (M.P. of 2018, item 694).

[40] *Act of 9 June 2006 on the Central Anti-Corruption Bureau* (Journal of Laws of 2016, item 1310, as amended), art. 1.

[41] Ibidem, art. 2.

[42] *Ordinance no. 72 of the Prime Minister of 6 October 2010 on granting the Statute of the Central Anti-Corruption Bureau* (M.P. of 2010 no. 76, item 953), § 3.

[43] Act of 6 April 1990 on the Police (Journal of Laws of 2016, item 1782, as amended), § 1.

the protection of the national border, border traffic control, preventing and counteracting illegal migration[44]. The process of data analysis and its transfer to decision makers occurs in the organizational units of particular services inside, respectively, the General Police Headquarters (Polish acronym: KGP) and the General Border Guard Headquarters (Polish acronym: KG SG). Inside KGP there exists, e.g.:

- The Cabinet of the Police Commander in Chief (Polish name: Gabinet Komendanta Głównego Policji), its tasks being (…) *coordinating the preparation of materials for the meetings of parliamentary committees and sub-committees and the participation of the Police Commander in Chief and his deputies in such meetings, preparing analyses on the operation of the Police in case of spontaneously arising needs of the KGP management*[45];
- The Chief Police Staff (Polish name: Główny Sztab Policji), its task being (…) *managing updated information on the state of security and order (...), including gathering and analysing data on current events and threats on the territory of the country as well as undertaking measures to prevent and eliminate them*[46].

Whereas, in the KG SG there exists:

- The Board for Foreigners (Polish name: Zarząd do spraw Cudzoziemców), its tasks being (…) *preparing cyclical and periodic analyses and materials, in particular on foreigners returning from the territory of RP*[47];
- The Analysis and Information Bureau (Polish name: Biuro Analityczno-Informacyjne) which is responsible for, inter alia, (…) *providing the Border Guard Commander in Chief and his deputies with assistance in the decision making process, in particular by preparing and supplying information and analyses of strategic importance for the operation of the Border Guard*[48].

It is enough to mention the scope of competence of only a few institutions to show haw many entities deal with data analysis. The materials obtained by these entities and their area of competence – despite varied tasks – often overlap. Therefore, the legislator in 2007 made an attempt to streamline the national security system with regard to data flow between its particular components. *The Act of 26 April 2007 on Crisis Management*[49] established the Government Centre for Security (Polish

[44] *Act of 12 October 1990 on the Border Guard* (Journal of Laws of 2016, item 1643, as amended), § 1.

[45] http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [access: 3 IX 2019].

[46] http://www.policja.pl/pol/kgp/glowny-sztab-policji [access: 3 IX 2019].

[47] http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [access: 3 IX 2019].

[48] https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [access: 9 XII 2019].

[49] I. e. Journal of Laws o 2019, item 1398, as amended.

acronym: RCB) – a structure which coordinates the information flow and serves as a National Centre for Crisis Management. The primary tasks of RCB are: (...) *analysis and assessment of possible occurrence and development of threats, collection of information on threats and conduction of analysis of collected materials, development of conclusions and recommendations on preventing and counteracting the threats*[50]. The emergence of a separate organizational unit in the structure of RCB testifies to the role and significance of information in this institution, i.e. the Analysis and Response Bureau, which in turn includes e.g. the Operational-Analytical Centre. The tasks of this centre are: *monitoring and analysing the situation and level of the national security as well as the occurrence of threats in this respect; compiling accounts, reports, assessments: – of the activities conducted by the Centre in crisis situations – of the tasks entrusted by the Council of Ministers or the Chairman of the Council of Ministers, of the activities in crisis situations conducted by public administration organs competent in the matters of crisis management*[51].

Conclusions

The author of this work is aware that the subject has not been exhausted. His intention was merely to signal some interesting aspects of analytical work and current system solutions in the field of creating analytical products for the authorities of RP, supporting the decision making process in the area of national security. One can reach certain conclusions based on the consideration so far and bearing in mind that a full presentation of the problem would require a multi-page elaboration:

1. With regard to a large amount of information appearing daily (potentially vital to the life, health and property of Polish citizens, constitutional order or international position of RP) the role and significance of data analysis will increase. Therefore, the labour market will seek specialists who are able to prioritize threats and describe synthetically undesired phenomena.
2. Another challenge, resulting from increasing amounts of data, is creating new tools and ongoing improving the existing ones, including computer software assisting analysts in efficient processing and organizing the collected knowledge.
3. In Poland numerous entities are responsible for preparing analyses on potential threats to the national security. Frequently, these entities have similar competence and therefore unnecessary duplication of efforts in the area of identifying, gathering and processing information may take place. For this reason, constant and enhanced cooperation between them seems essential, including exchange of information to achieve synergy effect.

[50] *Act of 26 April 2007 on Crisis Management* (i.e. Journal of Laws of 2017, item 209), art. 11.

[51] http:// https://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [access: 3 IX 2019].

4. It is worth starting a discussion on reforming the security system, including creating one, central body or transforming the existing one (e.g. the Government Centre for Security), which would deal with analysing information passed from secret services and offices. Subsequently, its task would be preparing one comprehensive material on a daily basis, whose recipients would be the most important persons in the state. This conclusion seems justified if one takes into account the postulates expressed by the former Head of The Military Counterintelligence Service Andrzej Kowalski (in 2013 he indicated the necessity of establishing the Centre of Strategic Analyses at the Minister Coordinator of Secret Services[52]), the authors of *White Book on National Security of the Republic of Poland*[53] (Polish name: *Biała Księga Bezieczeństwa Narodowego*) or other experts dealing with the question of security (e.g. Casimir Pulaski Foundation[54]).

Abstract

The article presents the issue of data analysis and its role in the process of ensuring national security. In the first part, the theoretical aspects of processing messages essential from the point of view of decision makers were highlighted, including definition issues, means of collecting information as well as types of data analysis. Moreover, in the further part of the publication the emphasis was put on the multiplicity of bodies responsible for providing analyses to politicians holding managerial positions in the country. In the conclusions, it was postulated to enhance cooperation as far as data flow between particular components of the national security system is concerned and establishing a new institution responsible for coordination and preparing joint analytical products, e.g. for the President of RP and the Chairman of the Council of Ministers.

Keywords: analysis, data, national security, intelligence services, decision making process.

[52] *Plan zmian w służbach opracowywany od kilku lat*, http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 13 V 2017].

[53] The authors of the document signalled the necessity to build '(…) a unit (bureau, centre, department etc.) responsible for conducting strategic syntheses of information supplied by secret services and developing integrated assessments according to the needs of managing national security. Its task would be collecting information from all services responsible for particular areas of security and subsequently analysing and assessing the information for the needs of the supreme state management institutions'. CF *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, p. 210.

[54] G. Małecki, *Reforma służb specjalnych z perspektywy 15 lat*, https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 13 V 2017].