

Ing. Martin Havlík, Ph.D., MBA, MSc.¹
Ministry of Defense of the Czech Republic

Dissemination of misleading Information and elimination of risks resulting from them

Introduction

The constant and everyday contact of human beings with the ubiquitous mass media, and especially with the widely used social networks and the Internet in general, generates many opportunities for stakeholders to disseminate their own information without any validation of their validity. While it may not always be about deliberately spreading false information, their occurrence is currently very intense and often more or less affecting the public's opinion. Each of us has certainly encountered cases where a lot of false information has been published on the Internet (whether within a widespread electronic encyclopedia of Wikipedia or other portals), which were then expanded and often taken as credible facts. Not only in professional scientific publications and other specialized articles. The emphasis is placed on the validity of primary and secondary sources of information and often also on critical work with sources and literature. If we want to avoid the impact of absorption and spreading of false messages, and in particular to resist purposeful or accidental misinformation, it is always necessary to verify all the important information before it can be used.

In particular, today's young generation is largely affected by the lack of critical thinking in verifying the information they encounter on a daily basis. The aim of this article is not to criticize the access to information, but to provide some guidance on how to correctly approach methodologically possible information about defective character or targeted propaganda.

The article deals with the issue of eliminating potential risks arising from the dissemination of misleading information, often also referred to by the English term Hoax [:houks:]. The article is primarily addressing the entire broad scientific community and the general public dealing with disinformation and security environment analysis. The intention is not to make a comprehensive summary of existing expertise or to thoroughly analyze the issue of a selected portion of misleading information, but to point out the main related pitfalls and to provide an initial overview of how to proceed in eliminating the associated risks. Although there is a wide range of experts dealing with the dissemination of misleading information abroad, there is as yet no relevant and comprehensive overview of the work that contains the main procedures and instructions for dealing effectively with misleading information (disinformation). Some state actors address the issue of spreading misinformation and defending against this information in recent years with great efforts and financial resources.

¹ The author has been working since 2005 for the Ministry of Defense of the Czech Republic.

Definition of basic concepts and typology of misleading information

For the concept of misleading information, the English word “Hoax” is now widely used. However, in some professional and articles, many equivalents can be encountered, such as false information, misinformation, fraudulent information, mystification, or, for example, alarm messages in the Czech language.¹ For the purposes of this article, the term misleading information, or the English equivalent of Hoax, will be used primarily. English linguist Robert Nares (1753-1829) deduced the likely origin of the word Hoax from the older word Hocus, which simply means “trick”.² The English word Hoax in translation means: false message, mystification, journalistic duck, scam, alarm message, fiction, prank, swindle, Canadian joke. In the computer world, the word Hoax is most often referred to as the alarm message that warns against the absence of a dangerous virus.³

„Hoax is deliberately or if you want to deliberately create a fraudulent (fake misleading message), trying to be right, and if possible spreading among the most end users. From the security point of view, Hoax is the most dangerous one created for the primary purpose of propaganda aimed at influencing the interests of state or non-state actors.“⁴

If we want to make a certain categorization of misleading information, it can be divided into:

- text information;
- sound recordings;
- pictures;
- video;
- virus files;
- a combination of the above.

The basic groups of fake misleading message (Hoaxes) according to the Hoax.cz portal⁵ include:

- warning of fake viruses and various computer attacks;
- a description of other unrealistic hazards;
- false requests for help;
- rumors about mobile phones;
- petitions and challenges;
- pyramid games and various offers for easy earnings;
- Chain letters of luck;
- joking news;

¹ For more, see <http://manipulatori.cz/lexikon/hoax/>

² Manipulátoři.cz. *Co je to Hoax?* [online]. 2015 [Accessed on: 2017-04-24]. Available from: <http://manipulatori.cz/lexikon/hoax/>

³ Hoax.cz. *HOAX* [online]. 2017 [Accessed on: 2017-04-24]. Available from: <http://www.hoax.cz/cze/>

⁴ Author's own definition.

⁵ Hoax.cz. *HOAX* [online]. 2017 [Accessed on: 2017-04-24]. Available from: <http://www.hoax.cz/cze/>

- Nigerian fraudulent emails;¹
- fraudulent lotteries;
- PHISHING.²

Goals of misleading information and tools used

In connection with the topic of this article, it is also necessary to currently reflect the continuous development of new communication and information technologies, especially in the context of their use for influencing public opinion.³ Not only the growth of social networks and other mobile communications applications at present, but also the comprehensive general orientation of the company to the daily use of modern communication technologies, provide the spread of any misleading news (including targeted propaganda). From all communication platforms, it is necessary to emphasize the importance of today's highly frequented and globally extended social networks and the availability of a global Internet network as the main source of information. It is also necessary to keep in mind that the increasing literacy of all users in the use of software tools also increases the ability to create and target misleading information in a sophisticated way. The very dissemination of misleading information and various propaganda is not often defended by somewhat relevant and objective mass media (this can be observed in public, especially television, media in recent years).

We can categorize the goals of spreading misleading information into several of the following basic groups. In this context, it is necessary to take into account that the breakdown is not dogmatic and, in deeper reflection, readers can find other own categories or specific subcategories of a more thorough division. The main goals of spreading false messages are:

- Getting sensitive information - especially collecting email addresses, phone numbers, access data and passwords, which are then a very valuable business article, not only in the context of information marketing.
- Getting profit - it's about getting access data and passwords to bank accounts or other private accounts with the primary goal of getting funds from the target

¹ Fraudsters send emails with tempting offers for a large sum of money. Alleged dispatchers are, for example, widowed wealthy entrepreneurs who ask for help transferring money from the country. More than a million dollars are promised as a reward for help. The main trick of the scam is that the captured victim is forced to gradually pay several thousand dollars for alleged money-related expenses, which are still postponed by various pretexts.

² Large numbers of addresses are sent out by fraudulent letters, which at first glance look like information from a particular bank. These letters make full use of so-called social engineering. The beneficiary is informed of the alleged need to fill in the data in the prepared form, otherwise the account may be blocked or otherwise restricted the use of its financial intermediaries. The e-mail is a link to the ready pages with a form that as if they were referring to the bank's server. In fact, the user is redirected to a foreign server but created in the same style as the site of the relevant institution. A cognizable user does not know the difference and can fill in the preset boxes where confidential information is required - account numbers, Internet banking codes, pins for payment, etc. The information thus obtained can easily be misused by the fraudsters.

³ HAVLÍK, Martin. Sdílení zpravodajských informací v rámci principu „potřeba sdílet“, *Vojenské rozhledy*. 2015, roč. 24 (56), č. 2, s. 83–91. ISSN 1210-3292.

person. Additionally, it may be the spread of misleading advertising aimed at reaching the widest possible range of potential customers who will be convinced to buy unnecessary or fraudulent products and services.

- Spread of viral infections - This type of misleading information is primarily targeted at major private and state institutions to destroy their critical infrastructure, or to obtain financial gain from the attacked subject.
- Propaganda aimed at influencing public opinion - it has recently been the most resonant issue associated not only with the alleged misinformation of world powers, for example in supporting political pre-election campaigns but also with the activities of state and non-state actors to propagate their own propaganda to influence the widest possible spectrum public opinion in their favor.
- The straining of data streams - this is not the case for ordinary non-users, but for corporate networks and portals it can be a major existence problem.

In recent years, the tools used to disseminate false information has reversed very significantly from the originally used television or radio stations and the classical printed media (especially newspapers and magazines) into the global Internet environment where the primary tool is, in particular, social networks. Although there is an overwhelming focus on the dissemination of information over the Internet, other forms of dissemination of information cannot be ignored. The diagram below shows the main communication channels and tools used to disseminate information from the source to the potential addressee.



Fig. 1 The main communication tools used to disseminate information
Source: Author's own processing

The meaning and scope of the above-mentioned main means of communication must always be understood in direct connection with the dislocation of major state or non-state actors to disseminate misleading information in individual regions of the world, specific states, or on a global scale. Current dictatorships and authoritarian regimes (for example, DPRK, China, Cuba, etc.) can rely on state media represented by television stations, especially in the propaganda of state, while the access of the population to the Internet is very limited and under very thorough censorship. On the other hand, in developed countries, the primary Internet (especially social networks) and private TV channels are used by source entities (spreading the misleading messages). It is therefore unclear in a general sense to prioritize which of the means of communication are more or less involved in spreading false information. This is always to be reflected in the comparison with the surrounding factors of the environs (territories). For the sake of clarity, it is also appropriate to mention, for example, the very active propaganda of the so-called Islamic State, which is distributed territorially through the authorities of the state (especially Iraq, Syria and numerous Muslim diasporas around the world), distribution of warning leaflets (especially Afghanistan) (Southeast Asia Region and the Middle East) or the dissemination of information through its own portals on the Internet and partly also social networks.

An important attribute in the use of means of communication (media) is their own scope. The Internet network generally has a global overlap with a partial limitation on areas where its distribution network is not fully built (developing countries, authoritarian regimes, etc.). Television channels can have both global (in the case of satellite channels) and especially regional and national coverage, while radio and print media are narrowly regional or national.

In the case of the propagation of misleading information, it is also necessary to always take into account the effect of interference on the transmission path from the source to the addressee of the information (noise effects, interference, intentional editing of the content of the information, etc.). These effects (see the following figure) can cause partial distortion of information (whether intentional or accidental) or a substantial change in the content of the original information. The communication channel is therefore the most vulnerable part of the communication system to create misinformation (misleading messages). In particular, a communication channel represented by a global Internet network, current hardware and, above all, software tools provide disinformation broadcasters with great room for application (very often effective) of their interests.

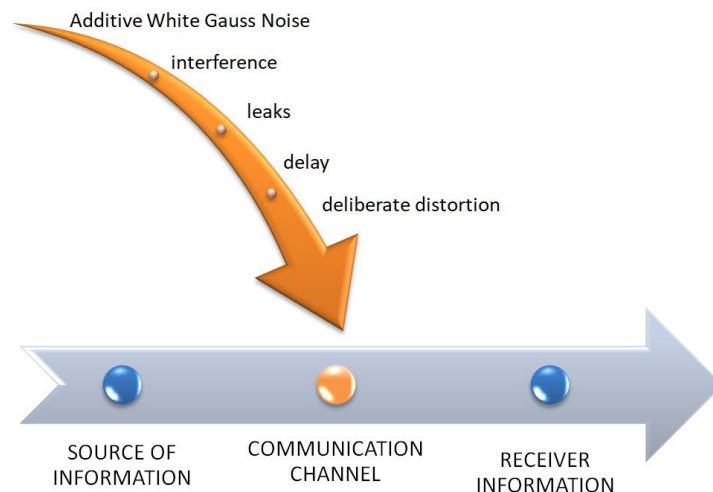


Fig. 2 General diagram of the communication system
Source: Author's own processing

The communication channel is generally understood to mean a physical environment serving to transmit a signal between the transmitter and the receiver. In general, the communication channel is specified by certain parameters that may be both random and non-random. Significant noise (AWGN¹) is often added to the transmitted signal. Various random interferences, whether of natural origin (atmospheric malfunctions, etc.), or from “industrial sources”, come into the communication channel. However, there may still be other random phenomena such as different types of leakage. In addition to these random parameters, the signal can be influenced by other effects that may be of a non-random nature. Such non-random phenomena may be the propagation time of the signal by the channel, its phase shift, etc.²

Elimination of potential risks generated by the dissemination of misleading information

Based on STEM³ research results on propaganda and disinformation of a political nature, more than five percent of the population of the Czech Republic generally misinforms, and almost one quarter of the population⁴ believes in disinformation media more than traditional media. The Czech Republic is considered to be the most vulnerable, according to research findings, when up to 40 % of young

¹ AWGN (Additive White Gauss Noise), which adds a useful signal linearly without any intermodulation; the term white refers to noise whose power spectral density is constant (frequency-independent), and the term Gaussian expresses the fact that the distribution of instantaneous amplitudes of this noise is governed by the Gaussian distribution.

² ŽALUD, Václav. *Moderní radioelektronika*. Praha: BEN - technická literatura, 2000. ISBN 80-86056-47-3.

³ STEM / MARK is a full-service agency that has been focusing on marketing research since 1994. [online] [Accessed on: 2017-09-11]. Available from: <http://www.stemmark.cz/>

⁴ Nebud' loutka propagandy. *PROČ BY SIS MĚL ZVOLIT INFO?* [online]. 2016 [Accessed on: 2017-04-24]. Available from: <http://zvolsi.info/>

people do not have the information to distinguish misinformation media content.¹ As the above-mentioned research focuses only on one segment (propagandistic expression and disinformation of a political character), it is necessary to realize that it cannot be directly related to phishing information like PHISHING, etc.

When verifying the information, a certain amount of critical thinking is needed. It is always necessary to think about the content of the claim, who shared this claim, who is the source of it, where and when the content was created, and for what purpose it is disseminated among addressees.² The validity of the information is most easily judged by its comparison with the reality. However, this is often not a simple process, and in some cases this is almost impossible. For validation, the information can therefore be used to divide the verification process (verification) into phases, which can always serve the target user. The following paragraphs briefly describe partial verification phases, the implementation of which leads to an objective assessment of the validity of the information as a whole. This process is also illustrated schematically for clarity (see Figure 3).

- Verifying the content of the information - the primary basis for verifying the contents of the information itself should be to verify all key contexts by keywords. For this purpose, it can simply serve the respected internet search engine. In this context, it is necessary to reflect multi-criteria search, alternative search of various language mutations and also original sources in other languages (very often in English). Emphasis should also be placed on the timeliness of related facts and the verification of numerical data.
- Verification of place and date of origin of information - very often publicly available events (weather forecasts, important objects in the case of image information, inscriptions, monuments, transport, background sound effects, etc.) can be used to verify the location and time of origin of the information. Frequently, misleading information about the image is easily detected, either by the common eye or by using available software tools (publicly available on the Internet).
- Verification of the source of the original information - according to the set and respected rules of creation of any information products, it is always necessary to indicate the original source of the information. Thus, at first glance, the user identifies the fact that the source is missing, this information is already somewhat unreliable or at least suspicious. In particular, in a global Internet environment, all available information cannot be considered as true. Before using the information, we always provide the source itself with a thorough partial analysis. Let's realize that the person who disseminates the information is usually not the author of the information.

¹ Novinky.cz. *Studenti Masarykovy univerzity bojují s mýty v médiích, spustili kampaň pro středoškoláky*, 2016. [online] [Accessed on: 2017-04-16]. Available from: <https://www.novinky.cz/veda-skoly/419499-studenti-masarykovy-univerzity-bojuji-s-myty-v-mediich-spustili-kampan-pro-stredoskolaky.html>

² KREJČÍ, M. *Fact checking manuál*, Think-tank Evropské hodnoty, 2016. [online] [Accessed on: 2017-04-11]. Available from: <http://www.evropskehodnoty.cz/wp-content/uploads/2016/10/Fact-checking-manuál.pdf>

- Identifying the Purpose and Purposes of Dissemination of Information - A very common phenomenon in the case of spreading misleading information (misinformation) is the use of the same underlying frame (template) for repeated misinformation. These facts can serve us to validate misleading information in the future, by conducting a comparative analysis of the new Hoax with the existing ones. For this purpose, some current online databases can be used to collect some misleading information. The most useful one can be considered:

- <http://hoaxes.org/>
- <http://www.snopes.com/>
- <http://www.hoaxbuster.com/>
- <http://www.hoax.cz>
- <http://manipulatori.cz/>
- <http://libraryguides.library.clark.edu/evaluating-information/hoax-sites>
- <http://usm.maine.edu/library/checklist-evaluating-web-resources?ID=0>
- http://www.info-skills.lib.vt.edu/evaluating_info/
- <https://theconversation.com/uk/topics/hoaxes-14337>

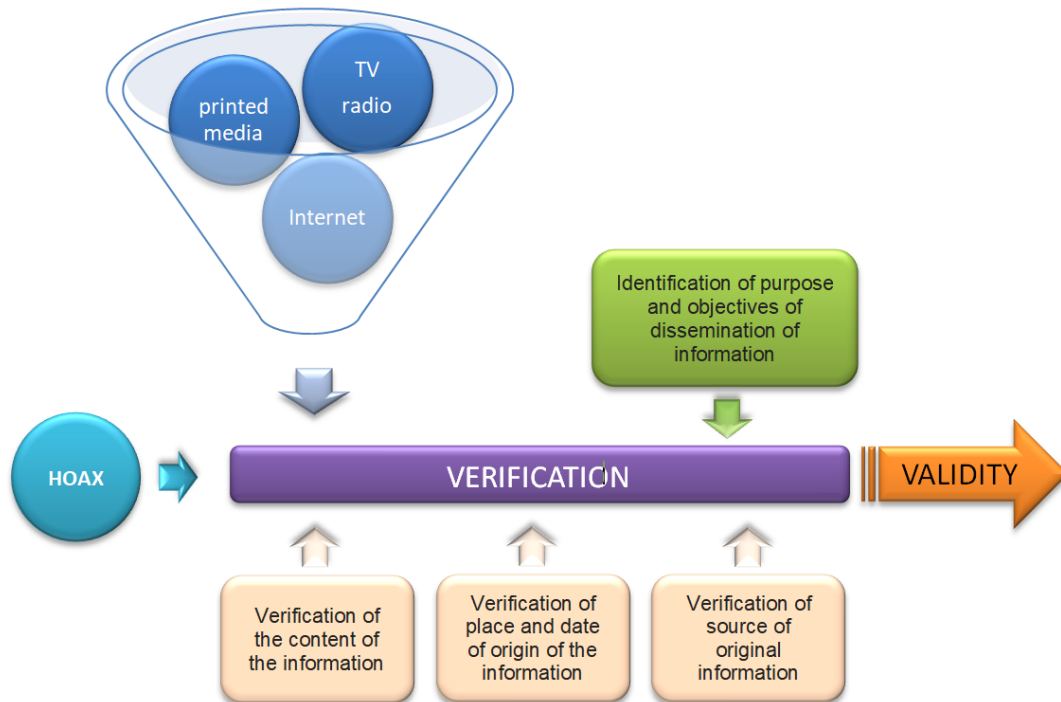


Fig. 3 Possible process of verifying fraudulent information
Source: Author's own processing

The success or failure of eliminating or at least detecting misleading information and possibly impacting the development of the security environment itself is currently very dependent on many important factors and on the partial verification procedures. Several standard processes can be used to perform the verification.

- Direct verification - verification of the same fact (information) by another method.
- Indirect verification - Comparison of two information of the same object based on different sources (notably non-identical sources).

- Opponent Verification - Reversing the critical contexts contained in the information under review, especially through the use of critical thinking and critical access to source information.
- Expert Verification - Compares the content of the facts with the opinion of an expert who is an expert in the field and who is not influenced by the information under consideration.

An important factor is the uninterrupted increase in the volume of information distributed over the Internet, as well as the development and use of more sophisticated software tools that allow for prima facie a highly plausible adaptation and falsification of the original information. These factors and some critical illiteracy in assessing the credibility of information have the greatest impact on the further spread of disinformation among a broader range of addressees, which often influencing public opinion. This list of influencing factors can not in any way be regarded as conclusive and dogmatic, however, in order to illustrate the problems described, at this stage it is quite sufficient, inspirational and conclusive.

Conclusion

Although there are currently many warning information pointing to problematic resource work (and on-going information), many users are often misled by misinformation, and they are further spreading it. Many misleading information of a variety of characters is spreading avalanche, especially in an Internet environment (not only with the use of social networks). To combat the effect of misleading information, it will be necessary to focus your own efforts on critical resource work. We must not believe everything we hear in the media or what we see on social networks, but we must always verify the veracity (validity) of individual information. Especially in cases where we want to prevent negative consequences and impacts on society. An example may be disinformation that directly affects public opinion and the views of the population on key political and security issues with an impact on the potential security of the country. People generally do not realize that misleading information can be harmful enough, not just for individuals (for example, in cases of computer virus spread or access password monitoring), but also for society in case of threats to national interests. A rather striking finding is the fact that almost a quarter of the population of the Czech Republic believes in disinformation and, in particular, the young generation lacks critical thinking about access to verification of consumed information. In the case of spreading misinformation and targeted propaganda, the current trend is increasing, with the use of sophisticated tools and purposeful use of the misleading information.

In this context, it will be necessary to promote the dissemination of awareness-raising with critical approaches to work with information sources. At the very conclusion of this review article, it is also appropriate to emphasize that the text of the mentioned social networks and other related modern means of communication are not the originators of the very causes of deceptive information but are a very effective tool for the penetration of disinformation among the wider audience.

Used literature and resources

- Databáze Hoaxů. 2017. [online] [Accessed on: 2017-03-20]. Available from: <http://manipulatori.cz/>
- ESET podcast #8 - Jak na internetu poznat hoax?, 2016. [online] [Accessed on: 2017-04-20]. Available from: <https://www.youtube.com/watch?v=IAuS7IILsng>
- KREJČÍ, M. *Fact checking manual*. Think-tank Evropské hodnoty, 2016. [online] [Accessed on: 2017-04-11]. Available from: <http://www.evropskehodnoty.cz/wp-content/uploads/2016/10/Fact-checking-manuál.pdf>
- HAVLÍK, M. Sdílení zpravodajských informací v rámci principu „potřeba sdílet“. *Vojenské rozhledy*. 2015, roč. 24 (56), č. 2, s. 83-91. ISSN 1210-3292.
- Hoax.cz. *HOAX* [online]. 2017 [Accessed on: 2017-04-24]. Available from: <http://www.hoax.cz/cze/>
- Manipulátoři.cz. *Co je to Hoax?* [online]. 2015 [Accessed on: 2017-04-24]. Available from: <http://manipulatori.cz/lexikon/hoax/>
- Nebud' loutka propagandy. *PROČ BY SIS MĚL ZVOLIT INFO?* [online]. 2016 [Accessed on: 2017-04-24]. Available from: <http://zvolsi.info/>
- Novinky.cz - *Češi jsou mistry v tom, jak pouštět do světa i úplné nesmysly*, 2016. [online] [Accessed on: 2017-04-10]. Available from: <https://www.novinky.cz/domaci/411068-cesi-jsou-mistry-v-tom-jak-poustet-do-sveta-i-uplne-nesmysly.html>
- Novinky.cz - *Fáma o migrantech na Facebooku zůstane bez trestu*, 2015. [online] [Accessed on: 2017-04-11]. Available from: <https://www.novinky.cz/krimi/384393-fama-o-migrantech-na-facebooku-zustane-bez-trestu.html>
- Novinky.cz - *Studenti Masarykovy univerzity bojují s mýty v médiích, spustili kampaň pro středoškoláky*, 2016. [online] [Accessed on: 2017-04-16]. Available from: <https://www.novinky.cz/veda-skoly/419499-studenti-masarykovy-univerzity-bojuji-s-myty-v-mediich-spustili-kampan-pro-stredoskolaky.html>
- Novinky.cz - *Zprávy o hrozících teroristických útocích nejsou pravdivé, upozorňuje policie*, 2016. [online] [Accessed on: 2017-04-13]. Available from: <https://www.novinky.cz/krimi/410947-zpravy-o-hrozicich-teroristickyh-utocich-nejdou-pravdive-upozornuje-policie.html>
- Novinky.cz - *Žáci věří fámám na sítích, školy jsou na to krátké*, 2016. [online] [Accessed on: 2017-04-13]. Available from: <https://www.novinky.cz/veda-skoly/415156-zaci-veri-famam-na-sitich-skoly-jsou-na-to-kratke.html>
- Surfařův průvodce po Internetu - *Zdroje*, 2017. [online] [Accessed on: 2017-04-19]. Available from: <http://zvolsi.info/manual/>
- ŽALUD, V. *Moderní radioelektronika*. Praha: BEN - technická literatura, 2000. ISBN 80-86056-47-3.

RESUMÉ

Hlavním cílem toho článku je pojednat o problematice šíření klamných informací a možnostech eliminace potencionálních rizik z nich vyplývajících. Úvodní část je věnována popisu základních pojmů se zaměřením na klamné informace a jejich typologii. Na tuto část navazuje popis hlavní problematiky cílů šíření klamných informací a využívané prostředky. V další části je pozornost věnována eliminaci potencionálních rizik generovaných šířením klamných informací, na kterou navazuje dílčí rozbor hlavních faktorů ovlivňujících verifikaci informací. Závěrečná část shrnuje některá doporučení, jak obecně přistupovat s kritickým myšlením ke zdrojům klamných informací.

Klíčová slova: Informace, klamná informace, riziko, Hoax, propaganda, bezpečnost, sociální sítě, komunikace, zpravodajství.

SUMMARY

The main goal of this article is to depict the issue of the dissemination of misleading information and elimination of potential risks resulting from them. The first chapter depicts the basic notions with a view to misleading information and typology. This chapter is followed by the description of the main dilemma of targets of the dissemination of misleading information. The following chapter describes elimination of potential risks generated by misleading information which leads to partial analysis of main factors influencing the verification. The final chapter evaluates some of the recommendations on how to approach sources of misleading information, by the means of critical thinking.

Keywords: Information, misleading information, Hoax, propaganda, risk, security, social networks, communication.

