IT-INDUCED COGNITIVE BIASES IN INTELLIGENCE ANALYSIS: BIG DATA ANALYTICS AND SERIOUS GAMES

A. ZANASI & F. RUINI
Zanasi & Partners, Italy.

ABSTRACT
Cognitive biases are unconscious deviations in judgement - rooted in the very nature of the human mind – that represent a common source of failure in intelligence analysis. This article investigates the relationship between cognitive biases and big data analytics in the intelligence domain. Big data analytics tools can assist analysts with the discovery of hidden patterns within large datasets, thus eliminating some of the factors responsible for the rise of cognitive biases. Such technologies, however, do not make analysts immune to cognitive biases and, if in the hands of inexperienced users, may even facilitate their occurrence. To illustrate this dynamics, the article provides a series of examples showing how different types of IT technologies commonly used by intelligence analysts may cause or facilitate the emergence of specific cognitive biases. Building on the work carried out during the RECOBIA and LEILA projects, the article proposes serious games as a solution for mitigating the effects of both IT- and non-IT- induced cognitive biases.
Keywords: intelligence analysis, IT-induced cognitive biases, RECOBIA, LEILA, serious games.

1 THE INTELLIGENCE CYCLE

The 'intelligence cycle' is a concept traditionally used to describe the intelligence process. It refers to a series of recurring and interrelated phases driving the work of intelligence practitioners, from the identification of the needs of intelligence consumers to the delivery of the final intelligence product [1, 2]. The intelligence cycle articulates in five stages: planning and direction, collection, processing, analysis and production, dissemination [3].

During the planning and direction phase, the intelligence requirements are defined, the tasks are scheduled and the needed resources are allocated. Planning and direction is followed by the collection phase, during which raw data from all available sources is gathered and aggregated. Collection may involve different types of intelligence [4]: human intelligence (HUMINT), signals intelligence (SIGINT), imagery (IMINT) and geospatial (GEOINT) intelligence, open source intelligence (OSINT), etc. Once the data has been gathered, the following step consists in converting it into a suitable format for analysis, which is the aim of the processing stage. This phase involves activities such as language translation and decryption and may rely on analysis techniques such as data and text mining. The next stage is analysis and production, whose aim is to transform the available information into usable intelligence. Throughout this phase, information's reliability, validity and relevance are assessed and weighted. Data/text mining techniques can be very effective to help analysts 'connecting the dots', for example by allowing to uncover relations between data of heterogeneous nature. Once the analysis and production phase is completed, the work culminates in the preparation of different forms of intelligence reports directed at contextualising the findings and drawing conclusions. This last step is defined as 'dissemination' and it is directed to the consumers whose needs had informed the definition of the initial requirements. While dissemination is intended to provide consumers the knowledge needed to support their decision-making, it may also generate feedback and further information requests, triggering a new intelligence cycle.

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N3-438-450

2 MAKING SENSE OF BIG DATA: BIG DATA ANALYTICS AS A TOOL FOR INTELLIGENCE ANALYSIS

'Big data' has become the buzzword of the moment in the intelligence community as in many other areas of society [5, 6]. The term big data is typically used to refer to datasets that, due to both their size (volume) and complexity (velocity at which new data is generated and variety of its sources), can only be effectively exploited by using technologies whose capabilities exceed those of traditional data processing applications [7].

The process of deriving insights from big data is known as 'big data analytics'. Big data analytics relies on the analysis and mining of big data in order to generate knowledge at a scale and specificity impossible before. Due to its ability to uncover relationships and patterns hidden within the data, big data analytics has been applied across a wide range of fields, from security and law enforcement to business and finance to healthcare and sports.

One of the most popular and effective big data analytics techniques is known as 'data mining' [8]. Also referred to as 'knowledge discovery in databases', data mining can be defined as the process of extracting valuable, usable and previously unknown knowledge from large information repositories and its use for supporting decision-making. Data mining exploits methods derived from the fields of statistics and artificial intelligence (e.g. machine learning) in order to process both structured and unstructured, quantitative and qualitative, data. Intelligence and law enforcement agencies rely on data mining to perform several activities. Deviation detection, for example, a data mining technique aimed at identifying anomalies within a dataset by singling out objects that are different from the others, is often used for spotting signs of possible criminal behaviour. Other techniques that have been exploited for purposes such as the analysis of criminal careers and profile offenders include clustering (a machine learning technique which aims to automatically create 'clusters' of items sharing similar characteristics) and classification (which allows to automatically assigns items to a pre-defined category) [9, 10].

The past decade has witnessed the flourishing of a new branch of the data mining discipline known as 'text mining' [11]. Text mining is the process of mining information from textual contents available in either structured (e.g. patents, meta-data, library catalogues, etc.) or unstructured (e.g. e-mails, blog posts, social media posts, etc.) form. It can count on multiple applications in the domains of intelligence and law-enforcement. For example, it is employed to analyse the content and style of terrorist communications in order to detect common patterns across different documents: by studying the characteristics of a particular text (e.g. the frequency with which specific words appear) - a technique known as 'stylometry'- it becomes possible to verify authorship, text's authenticity as well as to link the author to other anonymous writings [12].

Advancements in semantic computing, the essence of text mining, have brought important progress to the discipline of cognitive computing too. In 2015, TEMIS S.A. – a French company leader in text analytics solutions – was acquired by Expert System – an Italian software company specialised in semantic intelligence - with the declared goal of producing ground-breaking semantic technology for cognitive computing. In addition to those developed by TEMIS and Expert System, there are currently many other tools that provide text analytics functionalities and which could be successfully applied to the domain of cognitive computing. Worth mentioning software include RapidMiner, KNIME and Weka, which the authors of this article used for the analysis of data derived from social media within the framework of two EC-funded research projects: iSAR+ and SOTERIA.

3 COGNITIVE BIASES IN INTELLIGENCE ANALYSIS

The growing pervasiveness of big data into society, thus the increasingly larger array of information available to intelligence professionals, has made the task of data interpretation even more important than before. As an observer put it, '*the intelligence community can collect all the data in the world, but that data only will be as useful as the people charged with analysing and disseminating it can make it*' [13]. More responsibility has been put on the shoulders of individual analysts, whose knowledge and skills now more than ever provide the key to good intelligence. At the same time, the advent of big data has also emphasised some of the risks rooted in the inherent limitations of the human mind.

One of the main sources of error among intelligence analysts is known as 'cognitive biases' (CBs) [14, 15]. Cognitive biases are involuntary mental errors caused by the innate and unconscious propensity of humans to simplify decision-making by reducing the amount of information and uncertainty the have to process. CBs can be seen as cognitive shortcuts (or deviations in judgment) and are typically based upon factors such as memory, experience, education, cultural background, political or ideological bias, use of reasoning heuristics or simple rules of thumb. As notably demonstrated by Heuer [16], cognitive biases may occur at multiple stages of the intelligence process. A common CB that may arise throughout the intelligence cycle, for example, is the so-called 'confirmation bias', which is the tendency to search for or interpret information in a way that confirms analyst's own initial perceptions or judgements. The rise of this bias may jeopardise the quality of intelligence analysis by inducing analysts to ignore conflicting information or make judgements based only on part of the available evidence.

Cognitive biases may affect the strategy used for gathering data as well as the way in which results are interpreted once the data has been processed [17]. Bulk collection of data concerning citizens' communication activities – identified by former NSA contractor and whistle-blower Edward Snowden as a ubiquitous practice within the US intelligence community - offers a good example of how such a dynamic may unfold. Having at disposal, for a given individual, a full history of meta-data related to his/her phone calls, positioning information extracted from GPS sensors, logs of Internet activities and other types of records has made it possible for intelligence analysts to retroactively investigate on an individual's past behaviour for signs of suspicious conduct. The risk is that, confronted with huge volumes of data on a specific target, analysts may end up focusing only on information supporting their pre-conceived theories while neglecting or attributing minor importance to the rest. Worryingly enough, the more data on a given individual is available, the more likely is that a biased analyst will find the 'evidence' he/she is looking for.

Big data analytics too is not immune to cognitive biases [17]. While data in itself may be seen as an objective representation of reality, its interpretation is inherently subjective and, as such, highly vulnerable to heuristics and cognitive factors. Even if in possession of all the information needed to make a correct judgement, analysts may still be subject to errors, such as seeking out or favouring information that supports their initial beliefs. The availability of large datasets (big data) could even foster such errors, by making it easier for analysts to find the (biased) evidence they are looking for. The use of big data analytics techniques is considered to be an effective way to ensure that all the available data, not just the portion confirming the analyst's pre-existing hypotheses, is taken into due account. The problem is that even the most advanced big data analytics tools can be of limited value if not matched by an adequate level of knowledge and experience on the part of the users. While technology alone may be

unable to prevent the occurrence of some cognitive biases, its misuse may even trigger their occurrence or contribute to amplifying their effects. Historically, the intelligence community has devoted far greater attention to exploring the benefits of IT, than to understanding its flaws. An attempt to deviate from this trend has been recently made with the research project RECOBIA (REduction of COgnitive Biases in Intelligence Analysis), funded under the European Commission's Seventh Framework Programme (FP7) [18]. Aimed specifically at improving the quality of intelligence analysis by mitigating the negative effects of CBs affecting analysts, the project saw the participation of researchers from 9 European organisations (including the authors), alongside a wide network of stakeholders from the intelligence domain. One of the aspects investigated during RECOBIA was precisely the two-fold nature of IT as both a solution and a potential source of cognitive biases. The project proposed a set of strategies for the mitigation of CBs and identified a number of them whose root may be the incorrect use of technology.

4 IT-INDUCED COGNITIVE BIASES

Information technology has become part of every stage of the intelligence cycle. Analysts use technology to better collect, organise, process and evaluate information. According to a classification proposed by Pirolli and Card [19], IT tools may serve five different functions in intelligence analysis: search and filtering (e.g. databases and search engines), read and extraction (e.g. data and text mining applications), schematisation (e.g. visualisation software), build case (e.g. project management software and statistical tools) and relation discovery (e.g. link analysis software). Reliance on such technologies may provide considerable benefits to the analysts, one of the most important being the possibility to automate operations that could otherwise take a very long time if performed manually. If used incorrectly, however, each of the above categories of tools may expose intelligence analysts to a multitude of cognitive biases.

This is the case, for example, with search engines. Analysts rely on search engines both for exploring their own databases (using tools such as HP Autonomy's IDOL) as well as to delve into the Web (e.g. Google, Yahoo!, Bing). Most search engines allow users to formulate search queries using natural language, either in the form of full sentences or as lists of keywords. While such methodology may appear neutral at first glance, the specific words used for formulating the query may actually reflect preconceptions and beliefs existing in the user's mind. This may inadvertently alter the results towards the user's expectations, thus facilitating the rise of the confirmation bias. Other biases may result from the proclivity of users to only look at the very first results being returned by search engines. Such tendency may cause analysts to draw hasty generalisations or formulate conclusions based on weak or insufficient evidence, a fallacy known as the 'law of small numbers'. Worth noting is that search engines rankings may be deliberately manipulated, not only by their owners, but also by the users ('Google bombs' are the most extreme example of how this might happen [20]), in order to make certain results looking more important than they actually are, thus inducing a flawed perception of the information being available online.

Schematisation technology may also increase the analyst's vulnerability to cognitive biases. Tools such as visualisation software are designed to develop graphical models that fit the available data, thus providing analysts with an instrument for rapidly understanding it. While improving the ability of analysts to make sense of large volumes of information, visually representing the data may induce the observer to assign disproportionate weight to

specific pieces of evidence based on how these are displayed. Users may end up paying undue attention to items that appeared on the screen more recently than others, come first in a series or feature either at the top or at the bottom of a list, dynamics respectively known as the recency, the primacy and the serial position effects. Other schematisation technologies (e.g. statistical software and automated classification tools) may trigger cognitive biases when used for measurement purposes. For example, switching from one automatic classification tool relying on a specific scale to another relying on a different one may induce a biased perception about variability within the data.

IT tools also help analysts searching for relations within the available data. Link analysis software (e.g. IBM i2 Analyst's Notebook) is designed to facilitate the identification of connections between items within a dataset through operations such as association discovery, sequential pattern discovery and similar time sequence discovery. One of the risks associated with link analysis software is that an incorrect interpretation of the results may lead users to misread the relationship between items and events. A similar error may expose analysts to biases such as the 'illusory correlation' bias, that is the tendency to perceive a relationship between two variables when no relationship actually exists.

Data and text mining software represents another potential source of CBs. Data mining clustering techniques, for example, allow to automatically group objects within a dataset into 'clusters' reflecting their degree of similarity. Despite being an effective technique for classifying information, clustering may generate misleading results when performed incorrectly. A common mistake amongst inexperienced users consists in relying on the default settings recommended by the software in use, rather than tailoring the parameters according to the specific needs dictated by both the dataset available and the objective of the analysis. Errors of this sort are likely to return clusters excessively 'big' (i.e. containing a large number of objects), thus blurring the differences between objects. This may in turn trigger the occurrence of the 'out-group homogeneity' bias, i.e. the tendency to perceive members of one's own group as being relatively more varied than members of other groups (which conversely tend to be seen as highly homogeneous). Analysts falling prey of the out-group homogeneity bias are likely to overestimate the similarities between objects (e.g. people) in the same cluster, an error that may have detrimental consequences in the context of intelligence activities such as terrorist profiling [21]. One of the cognitive bias resulting instead from the use of text mining software is known as the 'ambiguity effect'. As an information extraction technology, text mining allows to infer the meaning expressed in texts as well as to classify text documents based on specific ontologies. The presence of ambiguous words within documents may nonetheless cause a semantic misinterpretation of the data, resulting in an incorrect classification of text entities and, in turn, of entire documents. A document classification error is likely to have cascade effects along all the steps of the analysis process, as analysts searching for documents within their databases will obtain a non-correct number of results. Important documents risk to be ignored in favour of other pieces of information that might prove irrelevant.

5 COGNITIVE BIASES IN INTELLIGENCE ANALYSIS: A CASE STUDY

Cognitive biases may arise at different stages of the intelligence cycle and have variegated impacts on the actual results of the process [22, 23]. The case study presented in this section provides a practical example of how cognitive biases, including IT-induced ones, may undermine the performance of intelligence analysts.

5.1 Scenario

A countryman claims to have witnessed a spaceship landing on a field he owns. The man reports that something looking like a Martian exited from the spaceship, being rapidly shot at by the man with a shotgun he had with him. The man missed the target, allowing the visitor to quickly run to his spacecraft and fly away. The countryman provides law enforcement officers with a detailed account of the events. In particular, he reports the alien to be about 1.20 meters tall and describes the spaceship as made by a single block of material, with two circles of respectively about 30 and 60 cm of diameter underneath. The officers depict the countryman as an unschooled and very modest (living off the electrical grid), yet credible person. Taking into account also the traces left by the object, the officers confirm that a large UFO, with a hexagonal basis, had landed and subsequently taken off from the field.

5.2 Investigations

Asked to further investigate the case, a LEA intelligence analyst (one of the authors), starts evaluating different hypotheses. He begins by rejecting the possibility that a traditional airplane could be involved in the landing because of inconsistencies between the size of the reported landing area and the space actually required by an airplane for landing and take-off. A helicopter and a VTOL aircraft are also excluded, as the traces these kind of vehicles typically produce are incompatible with those found on the ground. To validate these conclusions, the analyst checks on civil and the military aviation databases if any landing had been declared on that particular day and location as well as if other types of flying objects could have left traces comparable with those found on the ground. No such information is found in either of the databases, thus the conclusion is that, if the report is true, the object involved is indeed a UFO.

5.3 Follow-up

Before concluding his investigation, the intelligence analyst interviews a military aviation expert. The expert claims that no flying object could have landed in that particular area, except for a particular model of helicopter, which the analyst later found to be used by agencies linked to the Ministry of Agriculture for pesticide spraying. The helicopter sprays pesticides by means of a hexagon-shaped device attached to its landing skids. The presence of such a feature explains the peculiar nature of the traces found on the countryman's field. The expert adds that flights, even when involving war jets, are not always declared by pilots; hence the possibility that a flight/landing had taken place despite the absence of such information within the official databases of the aviation authorities. The fact that the countryman reported a spaceship instead of a helicopter has to do with his lifestyle: he had no TV and never had the chance to see a helicopter before. The pilot, described as an alien, was looking like such to the countryman because of his height (he was short indeed, although surely taller than 1.20 meters) and the fact that he was wearing a protective coverall suit, loosely resembling a silver skin, inclusive of a helmet.

5.4 Discussion

The intelligence analyst's initial failure in providing an accurate assessment stems from a variety of cognitive biases he was affected by. To begin with, the analyst overestimated the reliability of the aviation databases' content, which reported no landings on the day and

Figure 1: (left) A Martian. Or maybe just a man wearing a coverall protective suit? (right) A helicopter used for spraying pesticides (see the characteristic landing skid)

location of the event. His failure to consider that databases do not always provide a 100% accurate representation of reality may be attributed to the so-called 'anchoring bias' (defined as the tendency to rely too heavily, or 'anchor', on one specific trait or piece of information when making decisions), which resulted in the analyst prematurely dismissing the possibility of a helicopter being involved in the landing. Such conclusion was strengthened also by the specific methodology the analyst relied upon during his investigation. Rather than testing and comparing multiple hypotheses simultaneously, he proceeded by evaluating each hypothesis through direct testing only. Commonly referred to as the 'congruence bias', this fallacy induced him to give excessive weight to direct sources (the report from the law enforcement officers as well as the civil and military aviation databases) without focusing on indirect and alternative hypotheses - such as the possibility that the databases may not have reported all the landings – if not at a later stage of the investigation, when a military aviation expert was consulted.

The analyst's methodology was also flawed by a bias known as the 'Semmelweis reflex', which is defined as the tendency to reject new evidence that contradicts a certain paradigm. The Semmelweis reflex prompted the analyst to place greater trust than what would have been reasonable to do in the military aviation database, which indicated no other flying objects as being compatible with the traces found on the countryman's field and, ultimately, convinced him that no alternative hypothesis needed to be tested.

Regarding the reliability of the information provided by the countryman, the accuracy of the analyst's assessment was undermined by a combination of two cognitive biases respectively known as the 'fundamental attribution error' and the 'representativeness heuristic'. The fundamental attribution error bias caused the analyst to put more emphasis on the countryman's credibility as a person than on his lifestyle and cultural background. As a result, the analyst blindly trusted the man's 'technical' description of the observation, also non-questioned by the military police officers, without putting things into context (i.e. weighting the fact that the man was living out of electricity and, therefore, he did not have access to TV, radio, etc. at home). The perceived credibility of the countryman was also a product of the analyst incurring in the 'representativeness heuristic': because of the alleged similarity between the reported UFO and what according to the collective imagination an alien spaceship looks like, he considered the countryman's representation of the events to be the same as he would have given. This induced him to further downplay the impact of the countryman's culture and level of education on his way of perceiving events, further contributing to an evaluation of the man's report as sufficiently credible.

6 STRATEGIES FOR THE MITIGATION OF COGNITIVE BIASES: THE LEILA PROJECT AND THE SERIOUS GAMES

Mitigating cognitive biases may prove to be a very challenging task. As unconscious deviations in judgement, CBs cannot be entirely neutralised just by making analysts aware of their existence (although there has been extensive debate on this aspect, as reported for example in [24]). Successfully reducing their impact is likely to require deeper forms of intervention, targeting the very cognitive dynamics underlying people's reasoning.

The research carried out within the context of the RECOBIA project has identified a number of possible options to limit the impact of cognitive biases on intelligence analysts, ranging from the adoption of specific analytical techniques, to the implementation of psychological mitigation strategies, to the use of IT-tools supporting intelligence analysis.

Analytical solutions to cognitive biases pertain mainly to the domain of 'structured analytical techniques' (SATs), a systematic and transparent methodology allowing to address CBs by externalising the analyst's thinking process. 'Analysis of competing hypotheses' (ACH) is one of the most effective SAT techniques existing, as it prompts the analyst to generate and compare multiple explanations (hypotheses) by focusing on evidence that disconfirms rather than confirms each of them [25]. By ensuring that equal attention is paid to all the information and hypotheses, even those clashing with the analyst's original preferences, ACH has been assessed as a valuable technique for minimising the incidence of cognitive biases such as the confirmation bias.

For what concerns the field of psychology - another relevant source of mitigation strategies - the research conducted by the authors has identified amongst others the 'dissimilarity focus', a specific psychological exercise that requires participants to compare similar entities (e.g. two pictures) and spot differences between them. Studies have shown that engaging in some form of dissimilarity comparison is more likely to trigger critical thinking than confirmatory thinking [26]. Taking part in a dissimilarity focus exercise prior to starting an assessment of multiple sources or pieces of evidence is therefore recommended as potentially making analysts less prone to looking for confirming evidence.

As far as technology-based mitigation strategies are concerned, particularly promising solutions have been found in the use of 'serious games' for training intelligence analysts. Serious games are training tools – often digital in nature - exploiting techniques and processes typical of the gaming sector for purposes other than entertainment [27]. As a training instrument, serious games are becoming increasingly popular within the intelligence community due to their ability to simulate real-world situations and foster the acquisition of skills otherwise difficult to develop via traditional learning methodologies. Over the past few years, specific serious games have been designed for preventing analysts from incurring in cognitive biases. In 2011, an extensive research project focusing on the application of serious games to the intelligence sector was launched by IARPA, an agency under the responsibility of the US Directorate of National Intelligence. Known as the 'Sirius Program', the project aimed at developing a set of videogames directed at measuring and improving the ability of analysts to both recognise and avoid the most common cognitive biases threatening their everyday job [28]. One of the games, called MACBETH, simulates the role of an intelligence analyst whose mission is to prevent an imminent terrorist attack by figuring out the identity of the terrorist suspect. In order to help the player mitigating the CBs affecting his/her way of reasoning, the game relies on a system of feedback and awards that encourage the analyst to select disconfirming evidence and use it for formulating hypotheses [29]. A similar effort has been carried out by Symborski and colleagues with the development of the serious game 'Missing' [30].

Important steps forward in the use of serious game technology for the training of intelligence analysts have recently been taken by the European Commission as well. The EC-funded research project LEILA (Law Enforcement Intelligence Learning Application) reflects the growing interest of EU policy-makers in exploring new ways to apply IT solutions to the field of intelligence [31]. The European consortium running the project, led by KEMEA (Center for Security Studies pertaining to the Greek Ministry of Public Order and Citizen Protection), comprises innovative SMEs (Zanasi & Partners, FVA), large industries (GLOBO Technologies), NGOs (ORT France), research and training institutions ('Carol I' National Defence University, Alpha Labs). The main objective of LEILA is to improve the performance of law enforcement intelligence analysts by providing them with an innovative learning methodology able to enhance their cognitive capabilities and reasoning skills as well as foster a creative approach both individually and at a group level. Such methodology rests on a set of serious game-based learning experiences designed to raise the trainees' awareness about CBs as well as teach them how to mitigate their effects. In particular, LEILA led to the development of four distinct learning experiences [32]:

- 'VUCA (Volatility, Uncertainty, Complexity and Ambiguity) Challenge', a learning experience designed to test the ability of participants to deal with crisis scenarios, within a context of limited time availability, by filtering through large amounts of information that keep flowing in during the game;
- 'WhatATeam! Challenge', focused on the development of the key competences needed for successfully operating in diverse and distributed teams. Articulated in several modules, it includes the 'EagleRacing' phase, a game-like team experience in which the trainees, over a period of 7 weeks, operate as members of a virtual team with common challenges to face;
- 'LabRint: The Brussua Challenge', a computer game in which the player is asked to investigate on a security event (armed attack scenario). By analysing the available pieces of evidence, the trainee has to validate various hypotheses about the exact nature of the event, by building so-called 'inference schemes';
- 'Cyberint', similarly to 'LabRint', poses the player in front of a security scenario, which is in this case about cyber-security. The learning experience requires the player to analyse several incoming pieces of information in order to determine which of three possible hypotheses is correct.

The four LEILA learning experiences have been extensively tested by relevant end-users - from both LEA and not-LEA organisations - throughout the project, via dedicated pilot sessions. A first round of pilots (A) was carried out in 2015, with events in Romania and Greece. A second round (B) followed in 2016, with pilot sessions in Greece, France, Italy and Romania. Throughout the whole project, the learning experiences have been tested by over 400 participants. The evaluation has been carried out by means of both qualitative and quantitative methods: metrics (collected within the serious games), questionnaires and debriefing chats. The results confirmed the assumptions according to which serious games (as implemented in the LEILA learning experiences) can be beneficial for training intelligence analysts in avoiding the pitfalls of cognitive biases.

7 IT TECHNOLOGIES: CAUSE AND REMEDY FOR COGNITIVE BIASES

As described in the previous section, it exists in the literature a wide array of techniques that have been developed over the years in the attempt to at least mitigate the main negative

effects due to cognitive biases. Most of those techniques are 'analogue' in nature, as they do not rely on technology of any sort. So far, they apparently have not been able to solve the cognitive biases problem. As also testified by the positive experience emerged from LEILA, IT technologies seem to carry with them a better potential. But at the same time they bring new issues to the light.

The range of IT technologies that could be employed as de-biasing solutions includes many of the same tools that were discussed previously as possible source of cognitive biases. This raises a key dilemma: how can intelligence analysts exploit technology's full potential without falling prey to its inherent risks? To answer this question, one should start by acknowledging that both IT-induced and non IT-induced biases may often be tackled by means of the same kind of mitigation strategies. Semantic technology, for instance, may support analysts in processing large amounts of textual data, thus reducing the effects of non IT-induced biases (e.g. the anchoring bias). At the same time, semantic technology may prevent analysts from obtaining biased results when performing queries on search engines (a typical example of IT-induced bias): a search carried out with a search engine supporting semantic technology, in fact, is likely to incorporate various combinations of the terms inputted by the users, making results less vulnerable to biases nestled in the analyst' own wording of the search query.

Other types of IT-induced fallacies may instead require specific tools and techniques in order to be mitigated. A relevant example concerns the errors sometimes committed by automated classification systems like those typically employed for profiling activities. In addition to having a potentially major impact on the outcome of intelligence analyst's assessment, this kind of errors may be pretty much impossible to spot for the analysts who blindly trust (because not instructed about their meaning) the results generated by the software they use. In order to better understand the true meaning of the results generated by a classification system, analysts may rely on a theoretical instrument known as 'confusion matrix' [28] which allows to evaluate the effectiveness of a classifier algorithm by comparing various indicators of its performance. Those indicators include the model's 'accuracy' (i.e. the proportion of correct vs. incorrect classification), its 'coverage' (i.e. the proportion of the data for which the model was able to make a classification) as well as its 'recall' (i.e. the proportion between the number of positive cases that were correctly classified and that of all possible outcomes). By being aware of the values for all those metrics in relation to the classifier in use, analysts may get to know the inner limitations of the instruments they have at disposal, thus reducing the possibility of drawing potentially biased conclusions on the basis of inherently flawed results.

8 CONCLUSION

The nature of the challenges that law enforcement agencies worldwide are facing nowadays makes the role played by intelligence analysts increasingly important. In fact, the most compelling security threats affecting Western societies (e.g. terrorist attacks carried out by lone wolves) can only be tackled by relying on accurate intelligence. For a law enforcement agency, to anticipate the move of the enemy is now a compulsory requirement.

Cognitive biases, despite having been investigated for decades, still constitute a cause of mistake for analysts. As a new generation of technologies emerged, so did new forms of cognitive biases, that we described in this article as "IT-induced cognitive biases". The research carried out by the authors within the context of two security research projects funded by the European Commission, RECOBIA and LEILA, has brought to the light the fact that tools

such as serious games, semantic technology and confusion matrices may play a positive role in reducing the impact of IT-induced biases on intelligence analysts.

Reliance on such techniques alone, however, does not make analysts completely immune to the effects of CBs. Cognitive biases are a complex phenomenon, which must be tackled at its roots. When it comes to IT-induced biases, the roots are often to be found in a lack of knowledge and experience on the part of users. The conclusion that follows is that any successful strategy to address cognitive biases in the use of IT needs to place a major focus on the training of the users. In the field of intelligence, this means teaching analysts how to properly use the available technology but also how to select the most appropriate tools for each specific tasks they have to deal with. Ensuring that intelligence analysts are fully aware of both the strengths and the limitations of the technology at their disposal is key in order to prevent them from falling victims to its inherent traps.

Zanasi & Partners, who already offers to its clients from the intelligence domain customised training courses that include modules on how to mitigate the effects of IT-induced cognitive biases, is also actively performing research on this domain. Today's security needs, matched with the rapid moving into a 'Big Data world', made compulsory to improve the instruments used by intelligence analysists on a daily basis, to improve their analytical skills by allowing them to mitigate the negative effects played by cognitive biases and, as result, to improve the quality of their work.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the EU Seventh Framework Programme (FP7/2007-2013) under grant agreements n° 285010 and 608303.

REFERENCES

[1] Frini, A., An intelligence process model based on a collaborative approach. *Proceeding. of the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011),* 2011.

[2] Penn State College of Earth and Mineral Sciences. The Intelligence Process, available at https://courseware.e-education.psu.edu/courses/bootcamp/lo07/09.html

[3] CIA. The Intelligence Cycle, available at https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html

[4] George, R.Z. & Bruce, J.B., *Analyzing Intelligence Origins, Obstacles, and Innovations*, George Town University Press: Washington DC, 2008.

[5] Couch, N. & Robins, B., Big Data for Defence and Security, available at http://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf

[6] Cukier, K. & Mayer-Schoenberger, V., The rise of big data: how it's changing the way we think about the world. *Foreign Affairs*, **92(May/June)**, pp. 28–40, 2013. http://doi.org/10.1515/9781400865307-003

[7] Laney, D., 3-D Data Management: Controlling Data Volume, Velocity and Variety, available at http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

[8] Cabena, P., Hadjinian, P., Stadler, R., Verhees, J. & Zanasi, A., *Discovering Data Mining. From Concept to Implementation*, Prentice Hall: Upper Saddle River, NJ, 1998.

[9] de Bruin, J.S., Cocx, T.K., Kosters, W.A., Laros, J.F.J. & Kok, J.N., Data mining approaches to criminal career analysis. *Proceedings of ICDM 2006, the IEEE International Conference on Data Mining*, pp. 171–177, 2006.
[10] Mena, J., *Investigative Data Mining for Security and Criminal Detection*, Elsevier: Amsterdam, 2003.
[11] Zanasi, A., (ed). *Text Mining and its Applications to Intelligence, CRM and Knowledge Management*, WIT Press: Southampton, UK, 2007.
[12] Herz, J. & Bellaachia, A., The Authorship of Audacity: Data Mining and Stylometric Analysis of Barack Obama Speeches. *Proceedings of the International Conference on Data Mining (DMIN),* 2014.
[13] Zinner, C., Intelligence Must Plan to Develop Tomorrow's Analyst, available at http://www.afcea.org/content/?q=intelligence-must-plan-develop-tomorrows-analyst
[14] Smith, S.W., Security and cognitive bias: exploring the role of the mind. *IEEE Security & Privacy*, **10**, pp. 75–78, 2012. http://doi.org/10.1109/msp.2012.126
[15] Haselton, M.G., Nettle, D. & Andrews, P.W., The evolution of cognitive bias. In Buss, D.M. (Ed.), *The Handbook of Evolutionary Psychology*, John Wiley & Sons Inc: Hoboken, NJ, US, pp. 724–746, 2005.
[16] Heuer, R.J., *Psychology of Intelligence Analysis*, Books Express Publishing: Saffron Walden, UK, 2010.
[17] Wheaton, K.J. & Richey, M.K., You Can't Beat Biases with Big Numbers, available at http://www.growthconsulting.frost.com/web/images.nsf/0/3D6C419B4830EF0286257C55005D54CD/$File/SCIP14V6I1_IndustryInsight_Kristan.htm
[18] RECOBIA project, available at http://www.recobia.eu
[19] Pirolli, P. & Card, S., The Sensemaking Process and Leverage Points for Analyst Technology as Identified through Cognitive Task Analysis. *Proceeding of the International Conference on Intelligence Analysis*, 2005.
[20] Bar-Ilan, J., Google bombing from a time perspective. *Journal of Computer-Mediated Communication*, **12(3)**, pp. 910–938, 2007. https://doi.org/10.1111/j.1083-6101.2007-00356.x
[21] Zanasi, A., Cyber Defense, Cyber Intelligence e relative armi. Casi di collaborazione tra pubblica amministrazione, industria e ricerca finanziata dalla Commissione Europea. *Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business*, eds. S. Gori & S. Lisi, Franco Angeli: Milano, 2015.
[22] Winter, L.-C., Bedek, M. & Albert, D., Mitigating cognitive biases in intelligence analysis. *Journal for Intelligence, Propaganda and Security Studies*, **7(2)**, pp. 140–151, 2013.
[23] Hillemann, E.-C., Nussbaumer, A. & Albert, D., The Role of Cognitive Biases in Criminal Intelligence Analysis and Approaches for their Mitigation. *Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, pp. 125–128, 2015.
[24] Reese, E.J., Techniques for mitigating cognitive biases in fingerprint identification. *UCLA Law Review,* **59**, pp. 1252–1290, 2012.
[25] US Government. A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

[26] Dreisbach, G. & Fischer, R., Conflicts as aversive signals. *Brain and Cognition*, **72**, pp. 94–98, 2012.
https://doi.org/10.1016/j.bandc.2011.12.003
[27] Libes, D. & O'Connell, T., *Applying Serious Games to Intelligence Analysis*. Proceedings of SEA '07, the 11th IASTED International Conference on Software Engineering and Applications, ACTA Press: Anaheim, CA, pp. 311–317, 2007.
[28] IARPA's Sirius program, available at https://www.iarpa.gov/index.php/research-programs/Sirius
[29] Dunbar, N.E., *et al.*, MACBETH: development of a training game for the mitigation of cognitive bias. *International Journal of Game-Based Learning*, **3(4)**, pp. 7–26, 2013.
https://doi.org/10.4018/ijgbl.2013100102
[30] Symborski, C., Barton, M., Quinn, M., Morewedge, C.K., Kassam, K.S., & Korris, J.H., Missing: A Serious Game for the Mitigation of Cognitive Biases. *Proceedings of the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC),* 2014.
[31] LEILA project, available at http://www.leila-project.eu
[32] Zanasi, A., Ruini, F. & Bonzio, A., Intelligence analysts' training through serious dames: the LEILA project. *International Journal of Safety and Security Engineering*, **7**(3), pp. 380–389, 2017.
https://doi.org/10.2495/safe-v7-n3-380-389
[33] Kohavi, R. & Provost, F., On applied research in machine learning. *Machine Learning*, **30**, pp. 271–274, 1998.
https://doi.org/10.1023/a:1017181826899