The Mind Is Like a Parachute, It Only Functions When Open. National Security: the Importance of the Human Being that Works Behind The Machine[1]

Sabrina Magris[1], Claudio Masci[2], and Luciano Piacentini[3]

[1] NATO Subject Matter Expert, President of École Universitaire Internationale Rome, Italy
president@ecoleuniversitaireinternationale.net
[2] General of Arma dei Carabinieri, former Italian Intelligence Officer, lecturer
claudio.masci@libero.it
3 General of Italian Army, former special forces and Brigade "Col Moschin" Chief of Unit, former Chief of General Staff "Folgore" paratroopers Brigade, former Italian Intelligence Officer, lecturer
endurancerace@hotmail.com

Abstract. This paper describes how the human being is, and always will be, the heart of the machine.

It will addresses the role of the human being that works behind technological devices, the importance of the practitioner's human mind-set when employed to think, conceive, devise, create and put in action informatics tools (hardware and software), all fundamental actions for the optimal success of the final product. During the last years, together with the growing importance of cyber security and with the necessity of protecting national and international critical infrastructures, it has been given almost total trust to the machine and less to the human being. To better perform the tasks and to really protect National Security, the human being -and especially who recruit intelligence technicians and practitioners- have to be aware of cognitive errors and biases that can affect at the beginning the developing process of data mining systems, creation and elaboration of algorithms, Artificial Intelligence.

The international intelligence community is becoming more and more aware of the importance of the human being, particularly after answering to the question about why in some cases the machine has failed.

It is necessary dedicate specific development to the human being cognitive abilities thanks to dedicated training in order to mitigate or overcome biases.

Keywords: National Security, Cyber Security, Human Being, bias, I-BIAS, training.

[1] Copyright © 2020 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-2597/paper-15.pdf

1 Introduction

The aphorism [9] attributed to Albert Einstein timely than ever and pertinent in the era of information warfare, considered as "the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own [7], era in which both into the cyber-space and into the real battlefield a “hybrid warfare” is being fought, intended as a military strategy characterized by a great flexibility, that unites conventional warfare, irregular war and the war made by attack actions and cyber sabotage [4]. The hybrid warfare was defined as “unrestricted warfare” by the Chinese Colonels Qiao Liang and Wang Xiangsui in 1999 [15].

The two Officers – while describing the methods of the asymmetric warfare [12] claimed that it was no longer necessary continuing to spend billions of dollars for new weaponry and defensive space shield, when the danger of an attack – moreover – can originate also from groups that resort to the use of amount of money characterized by only a few thousand dollars.

The aforementioned Officers, by means of concepts focused on the worldwide globalization process and on issues related to the financial context, stated that the war has changed – with no regard to tools, technology, modalities and forms – but in its own essence and function. It was a concept aimed at making understand to their decision-makers and generals that “war is not even anymore war but a clash in very different fields” [15]: starting with the world of communication, through the use of Internet, and both by culturally facing each other through the new social networks and mass media, and by attacking with the use of financial transactions. Numerous real activities so far never considered as “war, but a hybrid way of facing each other” [15], learning as much as possible from others successes and failures with the purpose of obtaining a multiplier effect on the results. These results are obtained by combining from time to time the most suitable factors for success. In other terms and more specifically, with the combination - for example - of aircraft that cannot be intercepted, cruise missiles, nuclear deterrence, financial warfare and terrorist attacks.

Turning to the Chinese Institutional environment, the two Colonels have written: “managers ignore that it is not their capacity of understanding the combinations that represents the solution to the problem. What really matters is understand which elements must be associated in order to increase the combinations together with the combination modes” [15].

The importance of the mind and its indispensable function, that is understanding, appears clearly already at the beginning of the 2000. It is an importance, moreover, also previously supported – in February 1994 – in the “Martre Dossier” [18], relevant with the French plan for the realization of Economic Intelligence and Business Strategy.

In this context, the Economic Intelligence was defined as “collection and processing of information with sophisticated, difficult and delicate accessibility” [19]. The activity consists in the identification of the future intentions and abilities of a competitor, considering that the intention is the real reason of the actions.

In order to face these challenges – intentions of a competitor, factors that will influence its decisions, the area in which its interests converge, psychological attitudes –

brain must be put to work in order to understand the reality of: markets, techniques, ways of thinking of the competitors, their culture, their intentions and their ability to put them in act.

In light of these elaborations of thought, today we find ourselves immersed into a reality rich technical and technological connotations. It is a very distant reality from the cultural language of every Country or ethnic group, which seems to be moving forward towards a dimension of higher tranquility but it is not true at all.

In fact, the current society is characterized by the immediacy of the information that is mostly focused on new technological processes which have produced profound changes into the economic, social and cultural fields.

The majority of people attribute these drifts to the spread of the new technologies that stimulates inattention, in order to prevent "thinking". In fact, some believe that the widespread technological offer is a strategic one, it means that it is desired and programmed non only for the return – of considerable size and relevance – profits, but also to devastate and liquidate the western-Mediterranean humanistic culture, which allowed us to overcome over time irrational, horrendous and bloody conflicts that it has generated.

2 Who Works Behind the Machine: Limits, Cognition, Skills

It is essential to keep in mind that who operates behind the machine is a human being, it is to say that is someone called upon to think, conceive, devise, create and put in action informatics tools (hardware and software), all fundamental actions for the optimal success of the final product.

During the last years, together with the growing importance of cyber security and with the necessity of protecting national and international critical infrastructures, it has been given almost total trust to the machine and less to the human being.

The international intelligence community is becoming more and more aware of the importance of the human being, particularly after answering to the question about the way how in some occasions (i.e. the terroristic attack of Islamic matrix at the *Bataclan* theater, Paris, France, 13 November 2015) the machine has failed. After this terroristic attack terrorists warning problem and suspects report have arisen in the intelligence community.

The research made by the machine to detect terrorist suspects was wrong due to wrong selected criteria. This situations was caused by limits and errors of the human being that was not well trained regarding terrorist's behavior, and by erroneous categorizations related to radicalized terrorist and radicalized terrorist's behavior [17].

The weakness of the machine is the human being. Human being is the first input since it always exists a human initiating point, even when creating necessary tools for cyber security, and there will be a human final evaluation point or a human final decision (which, in the case of National Security, is the decision-maker).

Weather it is about analyzing raw data (primary data), creating or managing database, collecting analyzed data, pre-elaborate same data, creating learning models useful

for AI (Artificial Intelligence), the human being imports in these actions his own cognitive asset, with its abilities but also with his limits.

Biases are cognitive limits and errors of perception [20] that impact with thinking, analyzing and reasoning of every human being. No human being is exempt from biases since they are inherent into the brain and into the brain stem, into the culture, and into the behavior and they can interfere with every working activity, avoiding subjects from perceiving reality as it really is.

Biases, which are widely studied in the neuropsychology field, can be caused by society, education, social influence, culture, previous experiences; they can be implicit or explicit [5], and they involuntarily interfere by instilling also the belief of taking the wright decision or of making the wright action.

Particularly in the Intelligence and National Security field there have been found several troubles in the intelligence analysis and in the operational level and it has been theorized a specific type of bias connected to the intelligence field, the so-called I-BIAS [17]. The term I-BIAS indicates all of those errors of perception, errors of vision and culture that impede correct analysis or induce practitioners and technicians to make mistakes creating system and research models based on basic errors.

Among the most studied biases within the intelligence field there is the confirmation bias [10] which means seeking only that information that is consistent with the lead hypothesis, judgment/opinion, or the conclusion that is being considered primary, and the attentional bias [1] that manifests itself through a facilitation of attention orientation or as a difficulty in diverting attention from pertinent stimulus.

Unfortunately things that surround human being are not the only ones capable of limiting his cognitive abilities since there is also another type of bias, defined as physiological bias [2]. The physiological bias it is the elaboration of internal and external information aimed to cover up what is missed of the real information. The brain creates an ostensible version of what happens – based on the information it has already stored, without codifying new information – because it does not have the reality of what happens. At the neural level it indicates the deficiency of substances that enable the connections between the parts of the brain involved causing the non-codification of the information received [2].

Regarding the practical side, for the technicians this means thinking and projecting in a wrong manner at the beginning of developing process of data mining systems (even if there is supervision from a third part), or pre-canalize data elaboration in a wrong manner (i.e. algorithms).

Correcting these errors since their beginning leads to decrease the errors number, to increase the chance of creating models and tools aimed at the successful completion of the task (i.e. identifying threats, identifying suspects) and to widely decrease economic costs.

If we want to win the war or to excel on the strategic level, right instruments and right minds are needed, because, in the end, informatics instruments are being trained with data that are already biased through the human decision.

Human brain, as scientifically proven, can be modified in a more complex way than the machine, also because, as already mentioned, behind the machine there is the human being that creates and manages it. And if between people there is a difference in the

intellect, not all of us are Leonardo da Vinci (artist and scientist, 1452-1519) or Caravaggio (painter, 1571-1610), there will be and there is indeed an insurmountable gap between human being and human being.

Machine progress, systems progress but they are always subjected to the variables commended by the human being; just examine in deep the problems created some years ago (October 2016) to the giants of Web that, when attacked in their systems with obsolete programs, especially through a *system Dyn* attack that impaired DNS system (Domain Name System) worldwide. During this attack the giants Web systems went haywire around the world for an entire day.

The lack of an economical investment chosen by the human being has thus created a global insecurity that machine could not face up to or resolve. But the human being was aware of it. In this case too the mad variable determines what the machine will be able to do or to not do within its limits imposed by technology, science, and biases of the human brain.

Unfortunately, we are not aware of it or we do not notice it, but it is necessary to realize that we are living into the era of information warfare[7], it is to say the "war of information". Yes, we are at war, an asymmetrical [12] and unconventional warfare [6] that develops itself with unequal weapons and an incredible discrepancy of tools, time and sources. The attacked ones often do not have the knowledge of having to fight, while the attackers, instead, know it very well. And it is in their silent soul – warm and comfortable – that they acquire important and sensitive information as well unconscious behaviors to be used in order to neutralize the attacked.

In this regard it is consider that the technique is a tool at our disposal and we do not realize that it became the environment that surrounds us, a "full immersion into the battlefield". It is a technique that is built according to rules that are only measured with the criteria of functionality, efficiency and convenience, which do not hesitate to subordinate human needs and requirements to the need of the technical apparatus.

Technique it is only functionality and it does not concede us – into the context of a social harmony that we have lived so far – to reprocess and associate, into a society that is more compatible with the time that the evolution imposes, the concepts of: knowledge, culture, individual, dignity, solidarity, identity, freedom, salvation, truth, ethics, politics, religion and history.

Making a logical equation – but not a mathematical one – it is possible to affirm that:

- logos = rationality = word = transcendence = Mediterranean-western civility = harmony, proportion, limits and measure.

A civility founded on knowledge, on writing and on transcendence, fundaments on which the Greek thought, the Roman legal organization and Christianity had built the civility we are living in.

- number = technology = binary system = cultural homologation = numerical power = economic power.

A civility founded on the number that debases the sense of democracy where the numerical quantity is power, enhances the amount of money to acquire and is leading us towards "New Middle Ages" ruled by new lords and global vassalage.

We are realizing a technological society that tends to "regulate", that is to uniforms the behavior to a rule or to a technological process, but not to regulate it.

Regulation presupposes the emanation of norms anchored to legitimacy, especially in terms of a moral justification of behavior.

All technological innovations (tablet, smartphone, etc.) – individual tools for the dissemination and spreading of knowledge – apparently make free those who use them. But – as how really things are – subjugate them to the faceless power of whom decides how the machine works and of their new deity, the AI (Artificial Intelligence): which levels out, conforms, and deletes the individual personality and cancels the identity of each of us.

3 Scientific Finding that Will Affect the Future

The above mentioned future perspective is not aimed at having a negative view about the future but is the elaboration of some scientific data that cannot go unnoticed to those who deal with National Security, whatever it is the role or the point of view.

Recent scientific studies [8, 14] have proven a decrease into the cerebral cortex of youth that led to the loss of numerous neuronal connections and neurotransmitters, that quantifies itself in a decrease of 20%; reduction due to the excessive use of technology that have caused changes and distortions in the perception and in the cognitive perception, making these subjects unable of valuing emotions and reactions, and bringing them to reason almost as a machine, a robot and less like a person.

The majority of youth of today carry with them this involution, because human being has changed from the bottom, physiologically. The human being has a unique capacity for higher order cognition -such as planning and multitasking- but in the last few years youth are losing this set of capabilities.

Executive functions are a set of cognitive processes essential in organizing and monitoring behaviors.

Concluding, the development of more complex executive functions, including cognitive flexibility is what allows adults to complete challenging tasks.

These mental capabilities make the human being the best machine in the world, able to make a lot of mental and cerebral connections and actions each second throughout the day.

Unfortunately, with the excessive use of technology, Internet, electronic devices and videogames all these capabilities have failed. The excessive use of technology, as proven, causes physiological and biological modification both in the brain and in the behavior since it interferes in the abilities of attention and concentration with profound effects on the short-term attention, short term memory [26] and increasing biases. Youth could perform a significant deterioration in the neuropsychological measures of attention and concentration if compared to other youth grown up with less exposure to these inputs, proving that they are thinking according to binary models.

In the current context and having a look to the future, it is fundamental keep in mind these scientific results since minds homologation, thus the ones of the future practitioners and, consequently, of the technologies created for supporting the National Security, renders Institutions and private entities less competitive, less powerful in terms of brain and, if homologated, more easily to forecast in actions and developing, which in operational terms mean being more easily exposed to counter-intelligence operations.

It becomes fundamental being aware of the fact that development into the field of technologies must necessarily be accompanied by the human brain development, which creates and conceives these instruments, since they are chained processes and non-separated processes as they erroneous appear.

As stated above to make it clear that "there is no regulation without regulator" and that the relationship between the computer (tablet, smartphone, etc. …) and those who use it is never one of a binary type. It is a relationship that develops under the aegis of a third part, that is of who conceived the machine and its programs of functioning "based on his own interests".

4 How to Better Protect National Security

In order to guarantee National Security and to be at the forefront in the cyber security field it is necessary to maintain an active development of specific cerebral capabilities, because who works in the intelligence field can not be the same as others as but have to be above the attackers and have to forecast the opposing actions, evaluating all the variables, even mad ones. Action that the machine is still unable to perform.

It is necessary to put in action all the possible strategies, whether they are physical, cognitive, strategic. In particularly, reasoning with a long-term perspective taking in to account practitioners, in order to counter act -in a separate level- the rapid and constantly develop of technology by a competitor or non-state actors.

As before evidenced, we are living a new form of war, the "cognitive warfare"[27] whose objective is taking possession of information, production sources, circulation of information and knowledge.

Undoubtedly there is a war in progress where we are all unconscious actors in a war theater – enlarged, unconventional and asymmetrical – of which we are not able to understand rules and dynamics, nor the subject of the dispute, nor to recognize our companions of events, nor to discern the criteria of identifying our opponents.

In essence we are suspended above a social-subjective dimension, where our cognitive limits favor the "invisible ones" by delivering to their countless threat agents – that populate the improperly defined virtual world (but that is not so) – a large, simple and favorable operative field.

But what is the object of this transfer? Information, all kind of: personal, behavioral, working, interpretative, as well as opinions, preferences, logistic and housing activity, habitudes and personal tastes in various formats (text, images, videos).

We are not able to understand that every individual, man or woman, is a creator and provider of valuable and sensitive information as well as a potential target of interest. We are also unaware of the fact that on the other side of the "barricade" leaks a vast

world of as many human subjects, whom: operate into the cyberspace, have sophisticated tools at their disposal and are equipped with non-friendly intentions. They are animated by a "will to power" and moved by strategies and inscrutable goals, focused exclusively on the knowledge of other people's intentions and on their respective power and vulnerability factors, to be optimized in implications far from virtual.

Who are they? Difficult to say, research on the attribution of these new threats do not allow us yet to solve the enigma, however their analysis enables us to affirm that the actors are primarily state-actors or their proxies[2], that are appointees, military or civilians, private agencies, industrial companies, without any geographical or flag distinction or mercenaries, all of them skilled in moving into the deep world and dark web[3].

Furthermore, the extended and widespread network of social networks on digital platforms has favored the rapid and unreasonable adoption of informative behavior of all kind of information on a large scale, which is difficult to contrast with a containment solution.

The usual dilemma comes to the light again, when a finger moves up and indicates the sky looking to the moon. And the risk is when too many people look at the finger.

Everybody reason with machine with one thousand functions but these machines do not work without being connected to web networks. The reasoning is also without taking into account that in this scenario only 4/5 big companies play in the web space. As explained before when in the year 2016 half of the world (providers) was stopped. It is possible to have the best machine in the world but if these few providers turn on filters that impede the machine to work or to work in a wrong manner, what is it possible to obtain?

The practitioners, the human being have to look at the moon and not at the finger; growing generations have to learn to look at the moon and at the finger at the same time, due to complexity of the world and the current and future threats. When someone speaks about I-BIAS, this is the meaning.

5 Conclusion

Therefore we find ourselves living into a highly unbalanced reality on the technical dimension and on technological solutions, but completely undocked on the cultural and behavioral level.

It is necessary to dedicate specific development to the human being cognitive abilities through dedicated training in order to mitigate or overcome biases, regardless origins or previous experiences because this is even more a multidisciplinary and multi-

---

[2] Literally, type of server that acts an intermediary from clients seeking resources from other servers; in this case, considering the term from computer science and telecommunication, it means an appointee that acts for a third part.

[3] Deep web as part of Internet whose contents are not indexed by standard web search-engines; dark web as web contents inside the dark net –literally shadowy networks- that can ben reach only trough dedicated software.

level dimension that required a bottom change, change that can later create a domino effect by modifying and improving performances in favor of single person, entity, State.

The answer to this scenario can be exclusively provided on a cultural level, by opening our mind to critical stimuli, so to understand that we are not in front of a technological threat or a technical mechanism. This happens because the exploitation of the information that we unconsciously spread and the attacks - both cyber and computer ones - have a man-made origin, which constantly and in a free of charge way feeds itself with the information provided by us and by our unsuspecting and unaware behaviors. The most deleterious aspect: we are not just potential victims of blackmails for the payment of ransoms or theft of credit cards credentials, etc.… but also potential and probable targets, as we are unconscious vectors of these threats in the direction of the organization where we work.

We are all led to believe that as so far exposed is a "science fiction novel" just because we do not perceive the intangible with human eye e we do not touch it by hand.

But denial, deception, propaganda, information theft have always been intangible dimensions – before relegated elsewhere – now widespread in the digital world, exported to the network and in the social networks that we like so much. We activate these technological demons with every click we make and we do not notice it: as, for example, the fake news that infest the network not only for goliardic purposes.

The human factor and the so-called Human Intelligence (Humint)[4] are the only defense elements of the system to counteract the aggressors that are not machines, but human beings behind them.

The human being and the Institutions have always been able to count with numbers enemy or competitor's logistic sources, likewise cerebral and cognitive resources of technicians and practitioners in the field should be counted as their own quality. They have to be able to physically and mentally adapt themselves to the environmental changes and then to new forms of threat.

One of the divergences between Humint practitioner and those who work in the cyber security field is the necessity to contain the research areas, create subsets, clusters of data directly congruent or non-congruent. The human being is still able to process and analyze multiple information, even in non-logic or non pre-determined ways. The human being do not need the so-called "circle closure", if a human being ready to be close will not be created.

The machine can help in finding solutions, specifically in analyzing suspects, searching characteristics always and only if there is a human being – that have worked in the field- that train technicians about what they have to search for.

Two figures that complement each other, human being and the machine, but always and only human being's experiences will be the ones able to set guidelines for the machine in order to find solutions.

A change of perspective that has to become a constant component of the academic courses of all young people, so they can have an appropriate knowledge and education relevant to the new threats related to computer science. Ultimately, our young people

---

[4] Human intelligence, in short way Humint, is one of the basic intelligence functions that act collecting and processing information from human sources.

which are our valuable resources as well as our future citizens and managers – destined to do politics, to manage strategic sectors of the System-Nation, to work in companies, in Ministries, in the Armed Forces, etc. … - they will be able to bring in dowry the digital knowledge that they acquired today.

All this with a view on the fact that for the safeguarding of the security – and especially the National one – we are all insiders, without exception: responsibility belongs to everybody.

This paper ends with an aphorism trusting in the opening of minds for its interpretation: *"The perfect dictatorship will have the appearance of a democracy, a prison without walls, in which the prisoners would not even dream of escaping. A system of slavery where, through consumption and entertainment, the slaves would love their servitudes"*, Aldous Leonard Huxley.

References

1. Battagliese, G., Lombardo, C.: L'attentional bias nella psicopatologia. Psicoterapia Cognitiva e Comportamentale Vol. 17, n.1, 2011 (pp.75-98), Edizioni Erickson Trento (2011).
2. Bellomo, D.: What is biased can be unbiased: the neurological process of identification and elimination of biases held by professionals and victims. Study conducting using subject's brain mapping to evaluate biases caused by trauma, culture or education EVAWI International Conference, Chicago, USA (2018).
3. Bisiach, E., Luzzatti, C.: Unilateral neglect of representational space. Cortex (1978).
4. Bond, M.S.: Hybrid war: a new paradigm for stability operations in failing states. Carlisle Barracks, PA, USAWC, Strategy research project U.S. Army War College (2007).
5. COPS - Community Oriented Policing Servicies: US Department of Justice, Washington DC, USA (2016).
6. Department of the Army US: U.S. Army Special Forces Guide to Unconventional Warfare: devices and techniques for incendiaries (2011).
7. Ehlers, V.J.: Information Warfare and Internationale Security. Science and Technology Committee. IWS-The information warfare site (1999).
8. Falchini, L., Riggio, F.: Terrorismo e bambini. L'impianto del seme dell'odio attraverso i cartoni animati. Il fenomeno ghost splash. EUIEdizioni, Rome (2016).
9. Focus Storia,: The mind is like a parachute, it only functions if open. Cited by Albert Einstein (1879 – 1955). N. 63, gennaio, p. 77. Arnoldo Mondadori Editore (2012).
10. Globalytica LLC: Glossary of cognitive biases and misapplied huristics. Globalytica, USA (2017).
11. Haselton, M.G., Nettle, D., Andrews, P.W.: The evolution of cognitive bias. The Handbook of Evolutionary Psychology. Hoboken, NJ, US: John Wiley & Sons Inc. pp. 724–746 D. M. Buss edizioni (2005).

12. Hutton, J.S., Dudley, J., Horowitz-Kraus, T., TomDeWitt, Holland, Scott K.: Associations Between Screen-Based Media Use and Brain White Matter Integrity in Preschool-Aged Children JAMA - Journal of American Medical Association (2019).
13. Heintschel von Heinegg, W.: Asymmetric Warfare. Oxford Public International Law (2010).
14. Heuer Jr, R.J., Pherson, R.H.: Structured Analytic Techniques for Intelligence Analysis. CQ Press second edition (2014).
15. Liang, Q., Xiangsui, W.: Unrestricted Warfare [original title in chinese – literally "warfare beyond bounds"] nella versione italiana curata da Mini, F. (2001) Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione. LEG Edizioni (1999).
16. Magris, S.: Counterterrorism: new training methods to eliminate biases. Deactivating the terrorist analysing the terrorist's psychological profile. Paper International Association for Intelligence Education (IAFIE) University of Leicester, UK. (2018).
17. Magris, S., Grassi, M., Di Gioia, P.: Intelligence and Counterterrorism: the meaning of words is the right tool to make an efficient analysis when the threat is hybrid. Romanian Intelligence Studies Review No. 19-20/2018 pp. 93-104 Mihai Viteazul National Intelligence Academy – Bucharest ISSN 2393-1450 (2019).
18. Martre, H.: Martre Rapport La Documentation Française (1994).
19. Martre, H. et al.: Intelligence économique et stratégie des entreprises La Documentation Française (1994).
20. Mecacci, L.: Manuale di psicologia generale. Giunti Milano (2001).
21. Piacentini, L., Masci, C.: L'intelligence tra conflitti e mediazione. Cacucci Editore (2010).
22. Piacentini, L., Masci, C: Humint. Questa sconosciuta (funzione intelligence evergreen). Rubettino Editore (2014).
23. Piacentini, L., Masci, C., Bianchi, P., Bussoletti, F: Le criticità dei Big Data: Intelligenza umana vs. Intelligenza Artificiale (AI). Difesa e Sicurezza (2019) https://www.difesaesicurezza.com/difesa-e-sicurezza/le-criticita-dei-big-data-intelligenza-umana-vs-intelligenza-artificiale-ai/ (last access 14 November 2019).
24. Presidenza del Consiglio dei Ministri, Sistema di Informazioni per la Sicurezza della Repubblica: Glossario intelligence (2019).
25. Simons, D., Levin, D.: Failure to detect changes to people during a real-world interaction. Psychonomic Bulletin and Review, 5, 644-649 (1998).
26. Swing, E.L., Gentile, D.A., Anderson, C.A., Walsh, D.A.: Television and video game exposure and the development of attention problems. Pediatrics 126 (2), 214-221 (2010).
27. Ya'alon M.: The cognitive war as an element on national security: based on personal experiences. Memorandum No.197, The Institute for National Security Studies (2019).