BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **15**, No 7
Special Issue on Information Fusion

Sofia • 2015

Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2015-0090

Multiple Human Biometrics Fusion in Support of Cyberthreats Identification

Zlatogor Minchev

Institute of Information and Communication Technologies, BAS, Acad. Georgi Bonchev Str., Bl 2, 1113 Sofia, Bulgaria
Email: zlatogor@bas.bg

Abstract: *The paper is outlining an experimentally created framework for multiple human biometrics fusion in support to constantly evolving complex cyberthreats landscape identification. A "scenario method" approach, in combination with experts' based decision support and users' biometric "validation-in-advance", are considered. Practical examples are also given to the proposed ideas, providing a comprehensive outlook to the problem.*

Keywords: *Biometrics fusion, complex cyberthreats identification, scenario method, decision support, validation-in-advance.*

1. Introduction

Modern digital world is constantly evolving and generating as a result of this numerous cyberthreats evolving landscape. Whilst some of these threats are mostly related to the technological part of the cyber space, others, that are more complex, consider the human factor itself. The latter could be generalized around the "Advanced Persistent Threats" – "APTs" class [1] and are outlining phenomena like "social engineering", encompassing the human-machine interaction.

Regarding these, an adequate evaluation of the human factor response in the cyber space is of vital importance for establishing the social agility and building social resilience in the new digital 21-st century realities.

Studying the human-machine interaction, by means of APTs phenomena in general, is inevitably a rather ambitious task. Multiple understanding aspects of the problem, like social engineering, espionage, embedded security, mixed realities, etc., data breaches could be noted here [2, 3]. Since this is intuitively easily transformable towards the "scenario method" application [4], a practical implementation will be

given, combining multiple situational scenarios, human biometrics monitoring with empirical results assessment, following [5].

What is however important to note in the overall framework is the production of a formal information fusion understanding for the cybersecurity complex problems. A possible useful benefit from the fusion perspective will be the evaluation of the biometrics sources coupling, provoked by external APT's influences. Apart of this, the further selected biometrics feedback controlled influence (like audio-visual entrainment), could also change the initial human factor response and thus trying to tackle modern society painful problems like stress, ADHD and digital dementia [6, 7].

These problems solving are of vital importance for the proper understanding of modern people adaptation process in the flooded by information and technological gadgets nowadays cyber world.

Further on, a brief overview of the methodological framework for biometrics fusion in support of cyberthreats identification will be given with more details.

2. Methodological framework

The ideas behind the proposed framework are a generalization of the Joint Training Simulation and Analysis Center national and international research efforts in the cybersecurity field, recently outlined in [5]. However, the present approach is focusing on biometrics' fusion cumulative assessment, concerning specific human factor activities, regarding the selected situational scenario context.

A graphical illustration of the methodological framework for multiple biometrics fusion, using the "scenario method" in support to cyberthreats identification is given in Fig. 1.

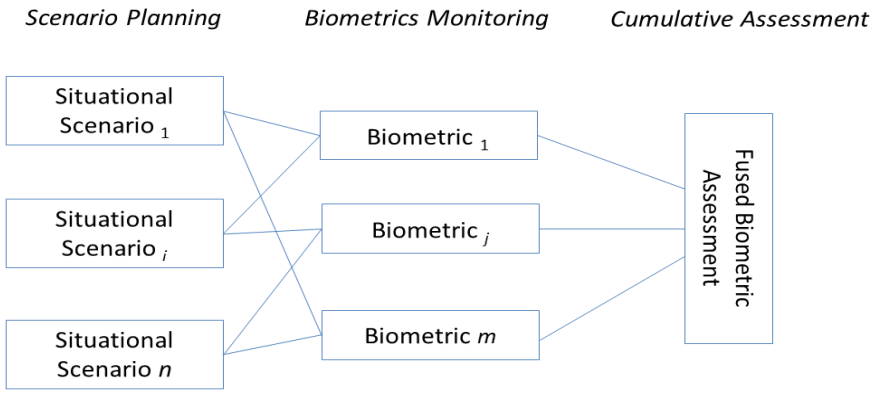

Fig. 1. General representation of the methodological framework for biometric fusion in support of cyberthreats identification, using the "scenario method"

As it is clear from Fig. 1, the framework is encompassing two main components: (i) *Scenario Planning* and (ii) *Biometrics Monitoring*.

The *Fused Biometric Assessment – Z*, depending on the scenario matrix *S*, connected towards a selected biometrics matrix *B*, could be defined as follows:

(1) $$Z = \sum_{i=1}^{n} p_i S_i \times \sum_{j=1}^{m} q_j B_j,$$

where p_i is the weighting coefficient, defining the significance of the *i*-th scenario ($i = 1, \ldots, n$, n – number of the used scenarios) and q_j – the weighting coefficient, defining the significance of *j*-th biometrics ($j = 1, \ldots, m$, m – number of implemented biometrics).

As this formulation of the fusion process is dependable on experts' beliefs, concerning the selected context scenario set, it is producing a real combinatorial boom. Luckily, experts' evaluation filtering is practically applicable [8]. The limited availability of the biometric sources is also boundering the overall *Z* assessment.

In general, the coefficients, aggregated in matrices *P* and *Q* could be defined, following a certain distribution trend [9] or dynamic models [10] forecasting. However, this approach is producing suitable results for events with apriori known future behaviour. In order to achieve forecasted results "validation-in-advance", an experimental practical approach is further described.

3. Practical implementation

In this section more details will be given to *Scenario Planning* (Section 3.1) and *Biometrics Monitoring* (Section 3.2) framework components noted in Fig. 1.

3.1. Scenario planning

This component is concerning the working context for complex cyberthreats landscape exploration. The accent will be given to experts' beliefs and real data cyber incidents implementation.

The practical realization is using the "scenario method", organized with adequate analysis. The resulting context and situational scenario sets are produced, concerning future cyberthreats evolution. Different methods of high-level experts' knowledge extraction [11], namely: discussions, interviews, brainstorming, etc., have been used [5].

Since the general context is difficult to be outlined in details, high-level prognoses have been recently successfully implemented in support to EU Roadmap for System Security Research 2020 [12]. Further Roadmap updates [13], used also in the Cybersecurity Strategy 2020 preparation for the Council of Ministries, Republic of Bulgaria [14] were also proposed.

The graphical representation of these prognoses generalization is provided in a matrix form (Fig. 2) within four-level granulation ("strong", "moderate", "weak" and "uncertain").

According to these experts' beliefs, the upcoming threats landscape in the cyber space for the next five years (up to year 2020) will be strongly influenced by: *Transformed Privacy*, *Biometric Disturbances* and *Espionage*, concerning the complete studied technological set ("IoT Gadgets", "Mixed Realities", "Advanced Communications", "Enhanced Multimedia" and "e-Trading").

Whilst *Social Engineering* and *Advanced Malware* are quite uncertain; *Data Breaches* are expected to be weakened as a threat, being already a quite exploited one.

THREAT/AREA	IOT GADGETS	MIXED REALITIES	ADVANCED COMMUNICATIONS	ENHANCED MULTIMEDIA	E-TRADING
TRANSFORMED PRIVACY	**	***	**		**
BIOMETRIC DISTURBANCES	***	**		**	*
SOCIAL ENGINEERING			*	**	***
ADVANCED MALWARE		**	*		***
DATA BREACHES	*	***	**	*	
ESPIONAGE	**	***	***	*	**

Legend:
*** – STRONG
** – MODERATE
* – WEAK
– UNCERTAIN

Fig. 2. Matrix representation of experts' beliefs for cyberthreats landscape evolution up to 2020 [14]

Following the proposed context of Fig. 2, multiple human factor activities could be defined, concerning different situational scenarios.

Briefly, the idea is to implement a system modelling with multiple digital environments [14], assessing the possible entities of potential cyber risks. The "Entity-Relationship" representation is used, implementing I-SCIP-SA environment [15].

"Entities" are represented as labelled round rectangles, while "Relations" as weighted bi-directional headed arrows. The resulting entities classification is provided, using the expert based evaluation of Influence/Dependence weights of the relations in a "3D Sensitivity Diagram – SD" with four sectors: "buffering", "active", "passive" and "critical".

Two illustrations of situational scenarios models and SD results, supporting the cyber risks identification trends from Fig. 2 will be given.

The first one is presented in Fig. 3 and it considers a social engineering model [16]. The entities' resulting in SD classification provides a capability for better understanding of terrorism, regarding social engineering in the digital space. Evidently, the active entities, related to: "Non-state Actors" (indexed ball "10"), "Social Conflicts" (indexed ball "8") and "Hacking" (indexed ball "5"), addressing both: "Human Factors" (indexed ball "9") and "Digital Environment" (indexed ball "2"). The critical ones have to be considered with high attention, regarding: "Organized Crime" (indexed ball "12"), "Violence and Extremism" (indexed ball "11"), as obvious threats. At the same time, carefully observation of hidden passive threats sources, like: "Radicalization" (indexed ball "1"), "Emigration" (indexed ball "7"), "Critical Infrastructure" (indexed ball "3") and "Grievances" (indexed ball "6") has to be performed.

Thus, as a conclusion of the proposed model, the terrorism in today's social engineering sense is related to complex threats sources with both technological and social aspects.

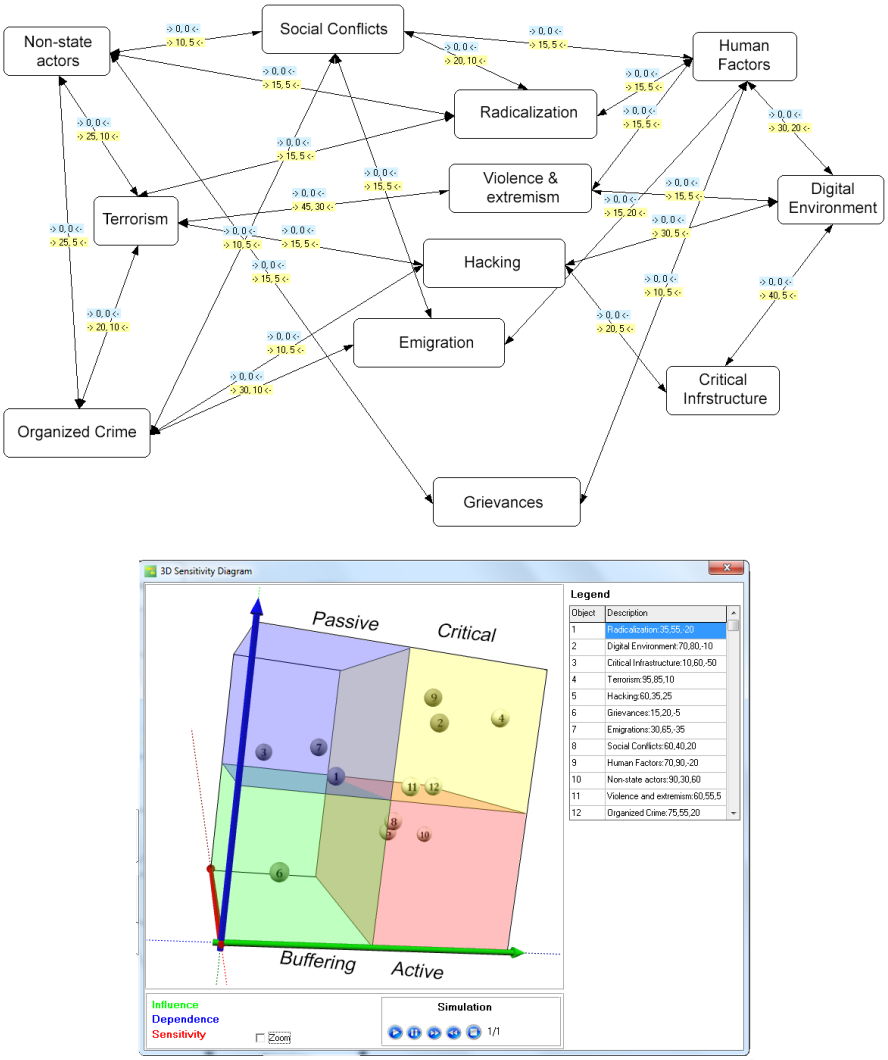

Fig. 3. Graphical illustrations of the situational scenario for social engineering experts' cyber risks assessment in I-SCIP-SA environment [16]

The second model illustration for IoT (Internet-Of-Things) usage in smart environments, noting the multimedia influence [17] (see Fig. 4) is extending the technological findings, adding Web 3.0 technologies interrelations towards social networks and the human factor. The resulting SD are defined as critical: "Smart Devices" (indexed ball "4"), "Social Networks" (indexed ball "5") and "Human Factor" (indexed ball "2"). "Entertainment Activities" are active (indexed ball "3"), generating hidden cyber threats from the expected "Multimedia" (indexed ball "1") evolution.

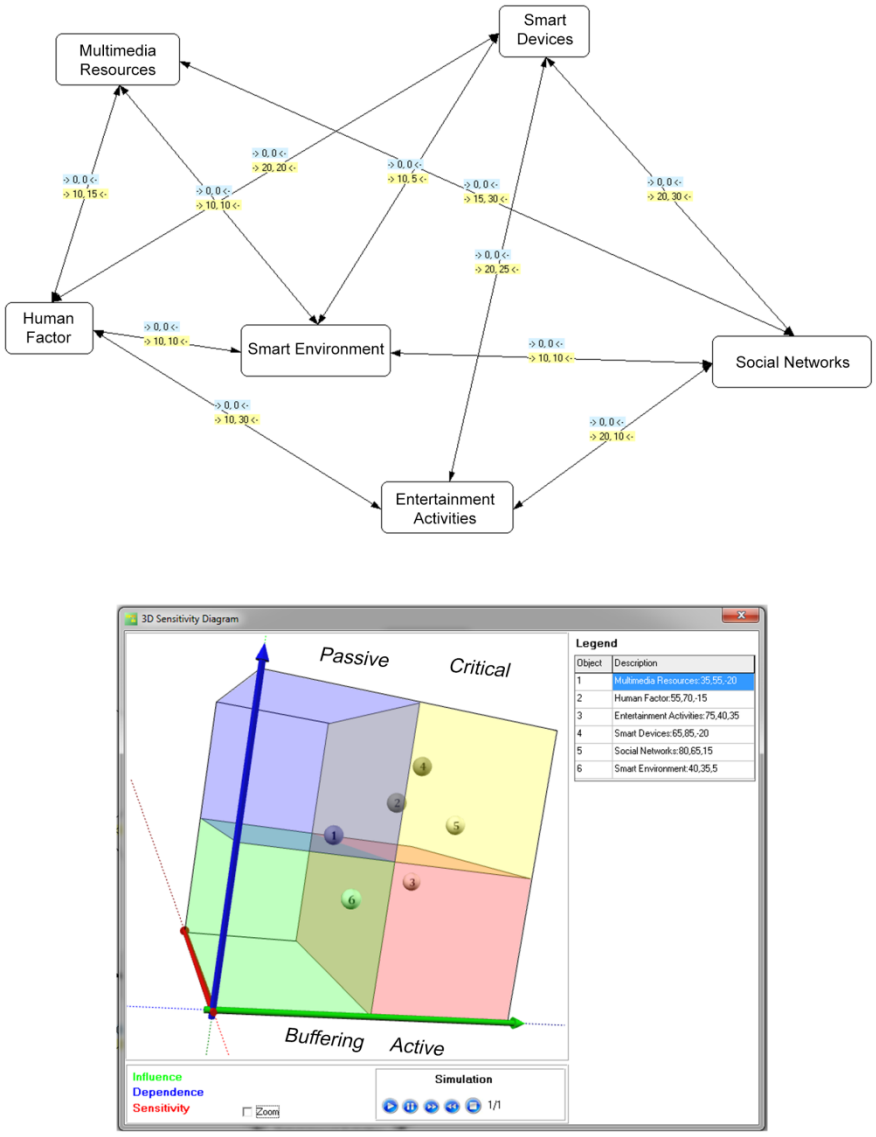

Fig. 4. Graphical illustrations of situational scenario for IoT usage in smart environments, experts' cyber risks assessment in I-SCIP-SA environment [17]

Though the presented situational scenario analytical examples (see Figs 3 and 4) expose reasonable expectations towards both technological and human factors, a possible "validation-in-advance" will be a valuable further step.

Taking into account the experts' results overall prognostic nature, the "validation-in-advance" could be performed with human factor multiple biometric monitoring.

More details, regarding successful biometric monitoring quantitative measuring discoveries will be given in the next section.

3.2. Biometrics monitoring

Because the human factor is with a rather complex nature in general, it has been studied from both psychological and physiological perspectives. This provides a suitable approach for complex characteristics, like emotions and behaviour evaluation in the digital space.

Personality assessments of users' temperament, depression and sensation seeking evaluation of motivation have been initially applied [18]. Additional stress assessment has been studied, monitoring complex social engineering training via CAX [19], using participants' response time monitoring [20]. This is in close relation to the human neural dynamics observations of different training process aspects in the digital space [21].

Some illustrations, concerning the psychometrics implementations are provided in Fig. 5.

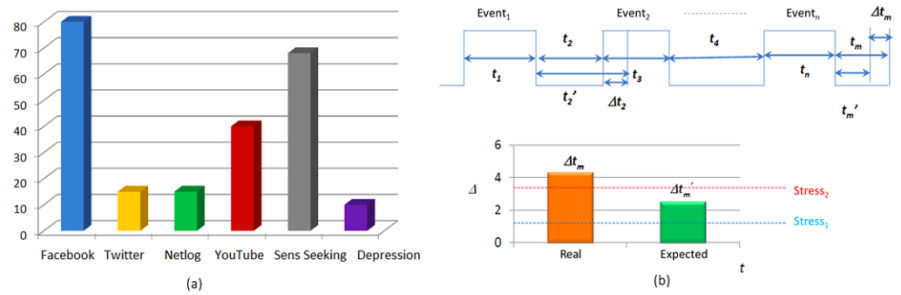

Fig. 5. Psychometric implementations for social network users' assessment [18] (a), and stress evaluation idea during simulated social engineering exercise Academic Cyber CAX 2015 [20] (b)

Further on, selected physiological correlates, like: electrical brain activity – EEG, galvanic skin response – GSR, electrocardiography – ECG, electromyography – EMG, postural center of pressure – COP, body temperature, connected with the human factor responses have been embedded for selected situational scenarios sets [5].

One of the key challenges during multiple physiological biometrics analysis, was to find a suitable measuring set in order to produce an adequate and useful "validation-in-advance" monitoring.

Successful metrics have been discovered experimentally in the time-frequency analysis, implementing: Relative FFT Power Spectrum of EEG, providing visible qualitative multimedia influences in multiple situational scenarios [5, 18, 22].

Another useful approach was the S-transform of COP dynamics [22] and EMG time series of selected mimic face muscles [23].

Finally, the fractal nature of GSR [5], EEG [16, 22] and ECG R-R intervals [23] were also implemented.

Some illustrations, concerning successful physiological correlated implementations, are provided in Figs 6 and 7.

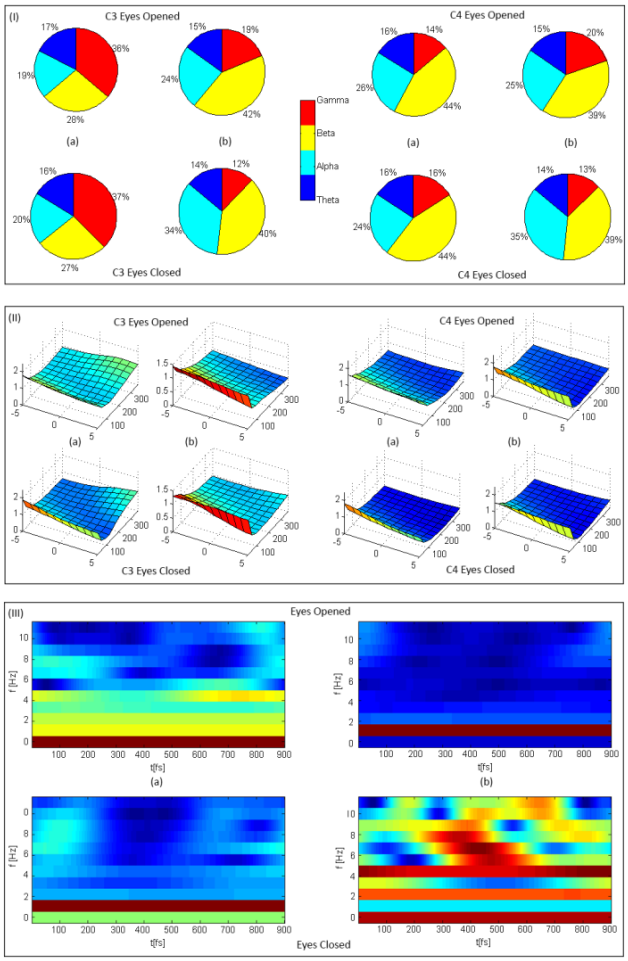

Fig. 6. EEG C3 and C4 lead FFT Relative Power Spectra (panel I), Multifractal Spectra (panel II) and COP S-transform dynamics (panel III), before (a) and 10 min after (b) an AV social training [22]

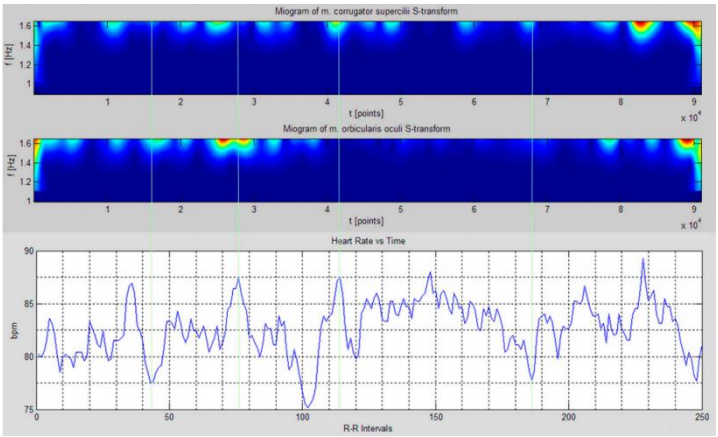

Fig. 7. EMG envelope S-transform of *m.corrugator superscilii*, *m.orbicularis oculi* correlations with R-R intervals, during Facebook multimedia gallery exploration [23]

The proposed biometrics correlates from Figs 5-7 demonstrate clear "validation-in-advance" successful implementations, using empirical selection and testing. What however is important to note here are the multiple biometrics cumulative assessment coefficients matrices *P* and *Q*. These are practically difficult for analytical precalculations, requiring experimental validation for scenario combinations and successful biometrics measurement. Both are not unique, especially for future cyberthreats forecasting, requiring multiple combinations studying.

4. Discussion

Evidently, nowadays and future cyberthreats landscape identification and forecasting is a complex context dependable task. Apart of this the "validation-in- advance" of the obtained results practically benefit from the human factor biometrics fusion in multiple scenario combinations.

The proposed experimental framework is outlining a comprehensive research outlook towards the problem of future cyberspace threats evolution and countering. Further progress is planned towards: (i) the organization of statistically significant big data of numerical experiments for generating probabilistic models that will provide a comparative base towards apriori biometrics matrix coefficient assessments; (ii) exploring multiple biometrics fusion at the level of selected metric characteristics coupling (e.g., phase synchronization of different biometric trends dynamics, similar to dynamic systems coupling) or even cause-effect proportional functional discoveries.

These will support the development of a reliable social cyber resilience, though the expected human-machine interaction fast progressing technological trends are not completely certain in general.

References

1. W r i g h t s o n, T. Advanced Persistent Threat Hacking. McGraw-Hill Education, 2015. 434 p.
2. 2015 Data Breach Investigation Report, Verizon.
   http://www.verizonenterprise.com/DBIR/2015/
3. A. Kayem, C. Meinel, Eds. Information Security in Diverse Computing Environments, AISPE Book Series, IGI Global, 2014. 354 p.
4. N g u y e, M-T., M. D u n. Some Methods for Scenario Analysis in Defence Strategic Planning. Australian DoD, Joint Operations Division, Defence Science and Technology Organisation, DSTO-TR-2242, 2009.
   http://goo.gl/f4vkkt
5. M i n c h e v, Z. Human Factor Role for Cyber Threats Resilience. – In: Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare. Chapter 17. IGI Global. 2016. 583 p. (in Press).
6. P e p e r, E. Support Healthy Brain Development: Implications for Attention Deficit/Hyperactivity Disorder. – Psychophysiology Today, Vol. **9**, 2014, No 1, pp. 4-15.
7. S w i n g l e, M. i-Minds: How Cell Phones, Computers, Gaming, and Social Media Are Changing Our Brains, Our Behavior, and the Evolution of Our Species. Inkwater Press, 2015. 268 p.
8. J. Armstrong, Ed. Selecting Forecasting Methods. – In: Principles of Forecasting. Handbook for Researchers and Practitioners. Kluwer Academic Publishers, 2001. 849 p.

9. G a r d i n e r, G. Stochastic Methods: Handbook for the Natural and Social Sciences. Springer, 2009. 447 p.
10. M o r r i s o n, F. The Art of Modeling Dynamic Systems: Forecasting for Chaos, Randomness and Determinism. Dover Publications, 2008. 414 p.
11. M o r e n o, D. Selecting Software Requirements Elicitation Techniques: A Contextual Framework. LAP LAMBERT Academic Publishing, 2011. 220 p.
12. D. Balzarotti, E. Markatos, Eds. The Red Book – A Roadmap for Systems Security Research. SysSec Consortium, 2013.
http://red-book.eu
13. B a l z a r o t t i, D. Final Report on Threats on the Future Internet: A Research Outlook. SysSec Consortium, 30 September 2014.
http://goo.gl/gQiCWV
14. M i n c h e v, Z. Future Threats and Challenges in Cyberspace. CSDM Views, Centre for Security and Defence Management, Institute of ICT, Sofia, No 31, 2015. 6 p.
http://it4sec.org/system/files/views_031.pdf
15. M i n c h e v, Z., M. P e t k o v a, Information Processes and Threats in Social Networks: A Case Study. – In: Proc. of Conjoint Scientific Seminar Modelling and Control of Information Processes, Sofia, College of Telecommunications & Post, 2010, pp. 85-93.
16. M i n c h e v, Z. Human Factor Dual Role in Modern Cyberspace Social Engineering. – In: Proc. of NATO ATC "Terrorist Use of Cyberspace", Ohrid, Macedonia, 8-12 December 2014, Published in: Series NATO Science for Peace and Security Series D: Information and Communication Security Ebook, Vol. **42**, Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses, 17 September 2015, pp. 116-128.
17. B o y a n o v, L., Z. M i n c h e v. Cyber Security Challenges in Smart Homes. – Cyber Security and Resiliency Policy Framework, NATO Science for Peace and Security Series. D: Information and Communication Security. Vol. **38**. Amsterdam, The Netherlands, IOS Press, 2014, pp. 99-114.
18. M i n c h e v, Z. Cyber Threats in Social Networks and Users' Response Dynamics. Institute of ICT, IT4SEC Reports, No 105, 2012.
http://dx.doi.org/10.11610/it4sec.0105
19. S h a l a m a n o v, V. Computer Assisted Exercise Environment for Terrorist Attack Consequence Management. – In: Proc. of RTO-MP-MSG-045 Meeting Proceedings, Rome, Italy, 4-7 October 2006, pp. 22-1-22-18.
20. M i n c h e v, Z. Challenges to Human Factor for Advance Persistent Threats Proactive Identification in Modern Social Networks. – In: Proc. of NATO ARW "Encouraging Cyber Defence Awareness in the Balkans", Skopje, 17-19 March 2015 (in Press).
21. Brain Waves Module 2: Neuroscience: Implications for Education and Lifelong Learning. The Royal Society, 2011.
https://goo.gl/j32krt
22. M i n c h e v, Z., E. K e l e v e d j i e v, P. G a t e v. Audio-Visual Entrainment Influence on Postural Dynamics. – In: Proc. of International Workshop "Posture, Balance and the Brain", Tessaloniki, Greece, 13 September 2014, Published 24 May 2015, pp. 55-60.
23. M i n c h e v, Z., P. G a t e v. Psychophysiological Evaluation of Emotions due to the Communication in Social Networks. – Scripta Scientifica Medica, Vol. **44**, 2012, No 1, Supplement 1, pp. 125-128.