CYBER THREATS IDENTIFICATION IN THE EVOLVING DIGITAL REALITY

Zlatogor Minchev

Institute of ICT/Institute of Mathematics & Informatics
Bulgarian Academy of Sciences,
zlatogor@bas.bg

Abstract: *Modern web technologies have already become an indispensable part of our everyday life, shaping a new, overlaid tech-social reality. This however generates numerous cyber opportunities & threats, produced as a result of the evolving human-machine and machine-to-machine interactions. The paper outlines a comprehensive, practical solution for meeting these problems from the cybersecurity perspective. A fourfold methodological approach to digital reality cyber threat landscape understanding is presented through: (i) Cyber Threat Landscape Definition, (ii) System Modelling & Analysis, (iii) Hybrid Simulation, (iv) Results Validation & Verification within multiple successful case studies.*

Key words: *cyber threats, proactive identification, digital reality, web technologies*

1. Introduction

Proper and adequate securing of the new progressive tech-social reality is inevitably producing a significant challenge to modern cyber world. The dynamically evolving digital realm is presently overlaying the social reality, using web technologies and services, ranging today from smart mobile social communications to assisting avatars and behavior monitoring systems.

This defines a naïve user attraction towards innovative technological e-lifestyle, providing opportunities with multiple e-services and smart technological gadgets. Numerous unknowns from the security perspective are also produced in this new and complex mixed digital reality.

Achieving a suitable reaction in this sense is a quite challenging task. Taking into account the new understandings for ‘privacy space’ and hybrid phenomena like: ‘Advanced Persistent Threats’ and ‘Compromised-by-Design’ the new cyber world looks rather ambiguous and not quite certain [1], [2]. This directly reflects to a fast evolving cyber threats landscape for the human factor and environment of living.

Moreover, one of the most arguable problems that stay under discussion is also related to the digital evolution and IoT AI embedding [3].

Practically this generates both – ethical and security challenges, positioning 21st century digital users in a new, unexplored environment, requiring at the same time, a suitable social resilience establishment [4].

Further on, the paper will outline a fourfold methodological approach, for cyber threats proactive exploration, encompassing: (i) *Cyber Threat Landscape Definition*, (ii) *System Modelling & Analysis*, (iii) *Hybrid Simulation*, (iv) *Results Validation & Verification* within multiple successful case studies, concerning the fast progressing digital reality.

2. Methodological Approach

The graphical representation of the methodological approach for proactive exploration of the cyber threat landscape in the evolving digital environment is depicted in Figure 1.

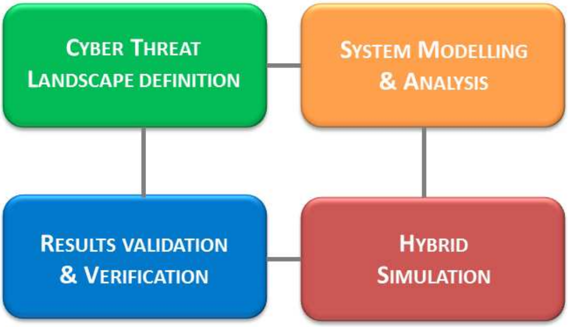

CYBER THREAT LANDSCAPE DEFINITION
SYSTEM MODELLING & ANALYSIS
RESULTS VALIDATION & VERIFICATION
HYBRID SIMULATION

Figure 1. Methodological approach for cyber threat landscape proactive exploration

It should be noted here that the presented approach has been successfully developed and tested during the last five years in different cyber fields, ranging from social networks to smart environments [4], implementing multiple IoT gadgets [5], [6] and used in several security roadmaps preparation for Republic of Bulgaria, EU and NATO [2].

The key ideas behind are accomplishing: system modelling (based on expert knowledge), further analyzed in the discrete case and simulated in mixed reality environment [6], [7]. The obtained results are validated with human biometrics monitoring, probabilistic assessment and questionnaire based multicriteria evaluation.

Finally, the validated results are also verified in different digital reality projections (encompassing multiple scenarios, concerning real, virtual and mixed experimental worlds) and are expected to be practically applied with overall global cyber trends landscape analysis, achieving proactive understanding of future cyber threats evolution.

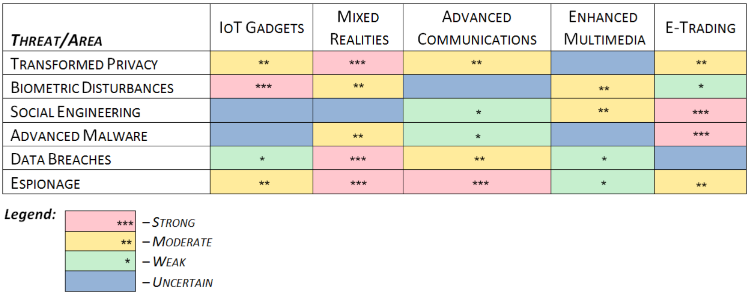
More details of the outlined methodological approach will be given in the next paragraph.

3. Practical Implementation

Proper understanding of the proposed methodological framework for cyber threat landscape identification in the evolving digital environment (see in Section 2) with real examples, concerning the different framework components are presented hereafter.

3.1. Cyber Threat Landscape Definition

As cyber threat context definition is difficult to be outlined, regarding its future evolution, several high-level prognoses have been successfully implemented. To mention: EU Roadmap for System Security Research 2020 [8] with its further update [9] and the ongoing Cybersecurity Strategy 2020 preparation for the Council of Ministries, Republic of Bulgaria [2].



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*

Figure 2. Cyber threat landscape evolution up to 2020, after [2]

According to these expert beliefs (see Figure 2), the upcoming threats landscape in the cyber space (up to year 2020) will be strongly influenced by: *Transformed Privacy*, *Biometric Disturbances* and *Espionage*, regarding 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 threat, being already a quite exploited one.

Being a priority for the near future technological progress a IoT threats questionnaire based survey up to year 2020 was also recently organized among 350 students from University of National & World Economy and Plovdiv University ‘Paisii Hilendarski’.

Selected generalizations (see Figure 3), concerning IoT trends findings are giving priorities in the following areas: *Expected New Web Services* (with ‘Advanced Multimedia Entertainment’ – 35%, ‘Improving Quality of E-life’ – 30%, ‘Advanced AI’ – 20% and ‘Automated Bio Identification’ – 15%); *IoT Application Trends* (with

‘Augmented Reality & Social Networks’ – 40%, ‘Virtual Entertainments’ – 35%, ‘Smart Urban IoT Services’ – 15% & ‘Drone Integrated Services’ – 10%).

Priority for the *Most Expected Threats* is given to: ‘Privacy & Tech Addiction’ – 35% and ‘Information Overload’ – 30%, together with: ‘Virtual, Augmented & Real World Mixing’ – 20 %, ‘Digital Identity & Presence’ – 15%.

Concerning *Possible Cyber Attack Vectors*, threats of: ‘Privacy & Social Engineering’ – 40%, ‘Malware & Targeted Attacks’ – 25%, ‘Data Breaches & Espionage’ – 20% and ‘Compromised Devices’ – 15% are noted.

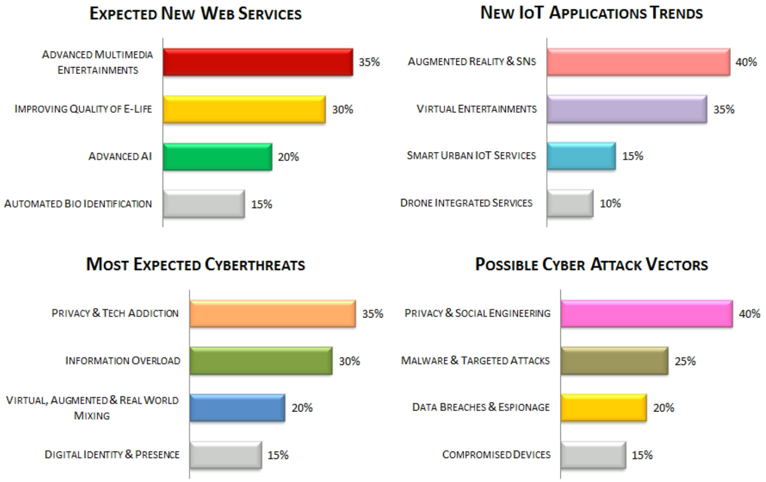


Figure 3. IoT survey results generalization for services, apps, threats & attack vectors expectations up to year 2020

Evidently, the upcoming virtual entertainments and E-life improvements within augmented reality IoT gadgets and social networks will generate new threats towards: privacy, technological addiction and information overload, mainly using the complex attack vectors of social engineering, malware and targeted attacks.

In this context, the recent broader outlook of Ponemon Institute [10] and ZDNet [11] on cyber threats and cyber attacks should also be noted, supporting the findings so far.

As these cyber threats discoveries are based on expert assumptions and technical observations, a better interconnected problem coping is practically achievable with detailed system modelling and analysis, providing more understandable cyber threats and attacks exploration.

3.2. System Modelling & Analysis

Proactive identification of cyber threats complex evolution requires a suitable approach for modelling and analysis. These ideas were already successfully used in multiple digital environments cyber threats exploration through discrete systems modelling & analysis [4].

A practical implementation in I-SCIP-SA software environment [7] is describing elements as related entities in the developed models. All relations among the entities (uni- or bi- directional) are weighted and time delayed (times equal to 0 concern static models, whilst arrays of time values with certain functional – relate to dynamic ones).

Graphically, entities are noted with labeled rectangle or circle and relations, with arrows, marked for both weight (yellow) and time (blue).

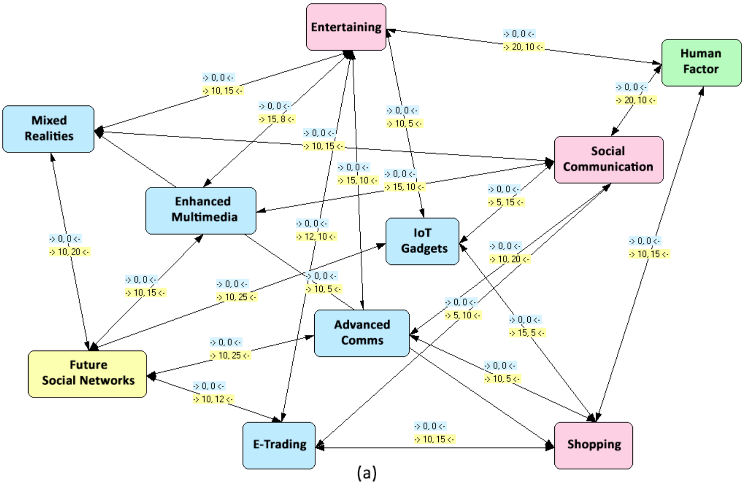
Model analytical assessment is based on expert beliefs for the relations weight and their dynamic trends, generalized into a three dimensional Sensitivity Diagram (SD), using: *Influence* (*x*), *Dependence* (*y*) and *Sensitivity* (*z*) values.

SD is using a four-sector entities classification (in accordance with *x*, *y*, *z* values): green – ‘buffering,’ red – ‘active,’ blue – ‘passive’ and yellow – ‘critical’. Additional, ‘active’ (white, positive *z* values) and ‘passive’ (grey, negative *z* values) reassessment for each of the entities in certain sector is also accomplished. This is directly related to sensitive elements’ evaluation towards the *z* axis. All entities in the model are visualized in SD with indexed balls.

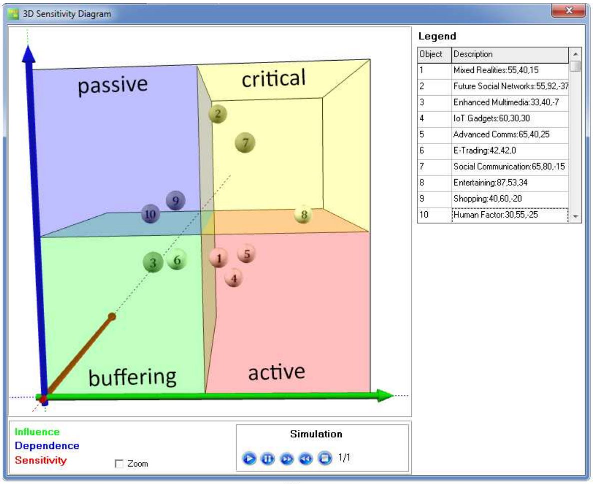
A practical application of I-SCIP-SA environment for modelling and analysis of future cyber threats potential sources, encompassing: social networks communication environment, human factor activities and new smart technological trends up to year 2020 was successfully developed and presented at NATO ARW ‘Encouraging Cyber Defence Awareness in the Balkans’ in March, 2015 [12].

As it could be concluded from this modelling & analysis (see Figure 4) the resulting static model entities classification is finding as critical the following entities: ‘Future Social Networks’ – ‘2,’ ‘Social Communications’ – ‘7’ and ‘Entertaining’ – ‘8.’

These critical entities were also studied and in other similar publications [4]. Active entities are: ‘Mixed Realities’ – ‘1,’ ‘Advanced Comms’ – ‘5’ and ‘IoT Gadgets’ – ‘4.’ Passive ones: ‘Human Factor’ – ‘10’ and ‘Shopping’ – ‘9.’ Finally, ‘Enhanced Multimedia’ – ‘3’ and ‘E-Trading’ – ‘6’ are buffering.



(a)



Legend

Object	Description
1	Mixed Realities:55,40,15
2	Future Social Networks:55,92,-37
3	Enhanced Multimedia:33,40,-7
4	IoT Gadgets:60,30,30
5	Advanced Comms:65,40,25
6	E-Trading:42,42,0
7	Social Communication:65,80,-15
8	Entertaining:87,53,34
9	Shopping:40,60,-20
10	Human Factor:30,55,-25

(b)

Figure 4. System model (a) and resulting SD analytical assessment (b) of future cyber threats potential sources up to year 2020 [12]

As the proposed system modelling & analysis ideas are based on expert beliefs, questionnaires and literature data, practical results dynamic evaluation would be of significant importance.

This was performed next via *Hybrid Simulation*, providing experimental observations of already identified cyber threats.

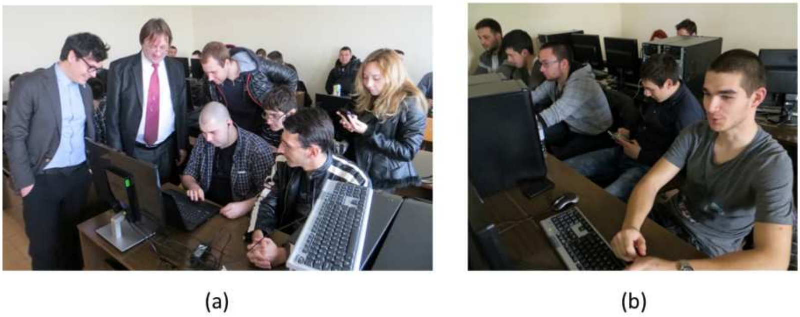
3.3. Hybrid Simulation

In fact, the simulation in itself is a quite useful solution that however is also limited by modelling formalism. As far as the present approach is using, a system interpretation, suitable dynamic simulation implementation is the interactive ones [13]. This provides an opportunity to combine the benefits of active human factor role with smart machine-to-machine communications.

As however the main objective of the present section is related to proactive cyber threats understanding a mixed reality polygon (combining: real, multiple gadgets augmented and virtual by nature) simulation with planned and unexpected events (implemented in a scenario play script), overall reckoned as 'hybrid' is used.

The practical realization of these ideas was successfully organized, using the already noted hybrid simulation approach and the experience from organizing other full-scale Computer Assisted eXercises [14] as proven instrument for exploration vague and uncertain security problems [15]. Here it should be noted that similar approaches are also used by other research groups (see e.g. CCDCOE exercise page [16]).

Two case studies will be further noted: Academic Cyber CAX 2015 & CYREX 2016 (see Figure 5). Both were organized at Plovdiv University 'Paisii Hilendarski' by Joint Training Simulation and Analysis Center as a successor of the 'Security Foundations in Cyber Space' training course [17].



(a) (b)

Figure 5. Hybrid simulation events CYREX 2016 (a) and Academic Cyber CAX 2015 (b)

Academic Cyber CAX 2015 [12] was with total duration of approximately three hours. A closed group on Facebook (comprising 30 students in computer science, at an age 23 +/- 2 years) was accomplised, together with: some augmented reality multiple smart gadgets (tablet, smartphone, i-pod, ultrabook), regular desktop PCs, LAN Wi-Fi router (for easy private network establishment and events logging/storing), private mail server and standard SMS notifications. A social engineering complex cyberattack, using: multimedia, data encryption, malware, insiders and data breaching were trained. The experiment in practice covered most of the social network APTs evolution prognostic trends [2].

CYREX 2016 [18] was an extended version of Academic Cyber CAX 2015, using international scale with industrial, IFIP & NGO support, taking approximately four hours duration time and using more complex hybrid simulation reality. Phablets, QR codes, video mobile streaming, Zoobe avatar messaging together with Skype, Viber and Dropbox cloud services were extending the hybrid simulation environment. Additional DDoS on selected participants IPs were implemented in an industrial espionage and hacktivism based simulation scenario.

What however stays important to note here is the measurements of the effect of mixed virtual reality on the trainees results in order to properly evaluate the digital influence from cyber threats perspective.

In the next section this vast problematic area will be briefly outlined, together with some useful achievements.

3.4. Results Validation & Verification

Effective validation of the obtained so far results is in fact a quite challenging task, especially concerning future cyber threats evolution. Moreover suitable results verification requires multiple scenarios & environments implementations and production comparison.

Practical support in this sense was achieved via monitoring of user multiple biometrics, Balanced Score Card post simulation assessment and probabilistic machine simulation of cyber attacks [12], [19].

Below these three approaches will be given with more details, regarding some successful implementation examples.

3.4.1. Biometrics Support

Both psychological and physiological assessment of user complex characteristics, like: emotions and behavior was organized for reliable hybrid simulation evaluation within different situational scenarios.

Personality assessments of temperament, depression and sensation seeking evaluation of motivation have been also applied. Additional stress assessment has been studied through monitoring trainees’ response times. This is in close relation with human neural dynamics observations of different training process aspects in digital space [12].

Some illustrations of selected successful psychophysiological correlates usage are provided in Figure 6.

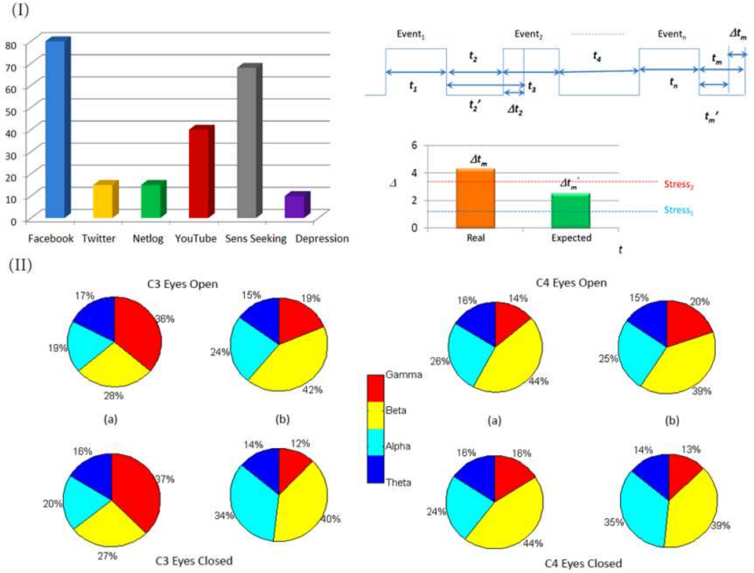


Figure 6. Selected psychophysiological correlates for validation of user response within hybrid simulation environments, after [12]

3.4.2. Balanced Score Card Assessment

The approach is extending the Balanced Score Card – BSC tool with questionnaire-based assessment and Delphi filtering, similar to other security exercises assessment [20].

During this process practical organization an important note is the participant motivation for proper questionnaires treating. Unfortunately it is difficult to be directly measured and checked, together with correct question understanding. This naturally generates noisy data results from the user response monitoring perspective.

A useful support in this sense could be the combination with indirect user feedback, based on stored activities biometrics analysis (see Section 3.4.1), or other bench mark machine simulation results (see Section 3.4.3).

Selected post-simulation results from CYREX 2016 are provided (see Figure 7) for both organizational and technical aspects.

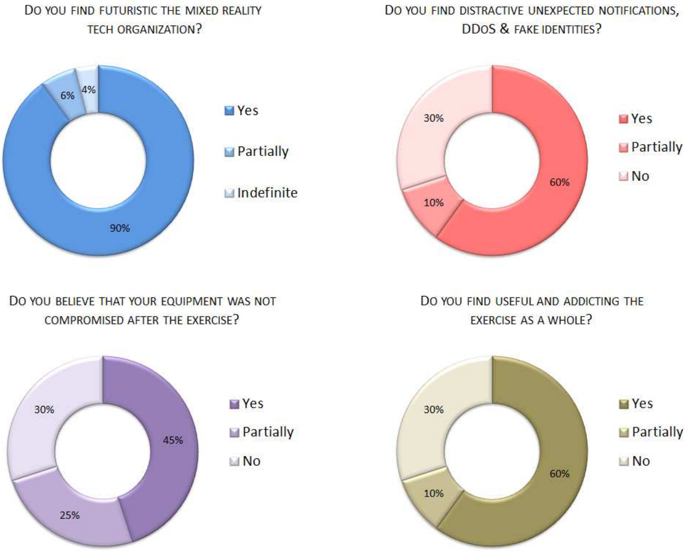


Figure 7. CYREX 2016 post simulation selected BSC assessment results

3.4.3. Probabilistic Machine Simulation

Another rather flexible validation & verification approach, concerning cyber threats future prognosis is achievable through probabilistic cyber attacks machine simulation [21].

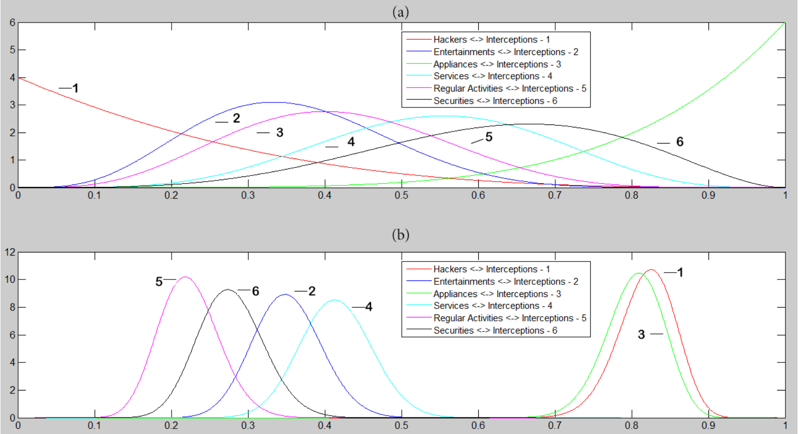


Figure 8. Probabilistic machine simulation example in Matlab R2011b environment with ‘a priori’ (a) and ‘a posteriori’ (b) beliefs for cyber threats identification, after [21]

A combination of system analysis entities of interest and a suitable probability distribution, implementing expert beliefs for ‘a priori’ assessment is initially used. These are further validated through agent-based cyber attacks probabilistic closed loop simulation (see Figure 8).

The approach is providing ‘a posteriori’ probabilities simulated assessment, using hypothetical evolution scenarios and somewhat neutral (concerning the subjective human factor role) machine results cyber threats verification.

4. Discussion

Obviously, todays’ digital reality is constantly evolving and producing enormous new opportunities and threats towards both users and technologies. The presented methodological approach for proactive identification of new cyber threats possible sources and influences is based on noisy expert beliefs and literature data input. Thus, a rather complex analysis, validation and verification have to be further applied for effective treating. What however stays uncertain is directly related to the development of general overall trend assessment approach.

Being a rather ambitious task, the practical solution in this context could be achieved with mathematical techniques for trends analysis with suitable time delays and joint dimension scales matching.

Hopefully, the evolution of machine-to-machine AI interaction will also provide an added value towards proper coping of this problem area. The necessity for establishment of predictable technological environment with autonomous context dynamics (fitting to a reasonable extent the future technological users’ needs, emotions and feelings) is a real challenge in the new digital age.

References

1. Wrightson, T. Advanced Persistent Threat Hacking, McGraw-Hill Education, 2015.
2. Minchev, Z. Future Threats and Challenges in Cyberspace, CSDM Views, No. 31, Centre for Security and Defence Management, Sofia, June, 2015, http://it4sec.org/bg/system/files/views_031_0.pdf
3. Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Elsevier, 2014.
4. Minchev, 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, pp. 377 - 402, 2015.
5. Boyanov, L. & Minchev, Z. Virtual Assisting Agents & Internet of Things, KSI Journal of Knowledge Society, no.1, pp.3-5, January, 2015.
6. Minchev, Z. & Boyanov, L. Augmented Reality and Cyber Challenges Exploration, In Proceedings of IV International Conference 'Technics. Technologies. Education. Safety', 1-3 June, 2016 (in press)

7. Minchev, Z. Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems, In Proceedings of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev, Sofia, IMI-BAS, pp.102-110, 2016.
8. Balzarotti, D. & Markatos, E. (Eds), The Red Book – A Roadmap for Systems Security Research, SysSec Consortium, 2013, http://red-book.eu
9. Balzarotti, D. Final Report on Threats on the Future Internet: A Research Outlook, SysSec Consortium, September 30, 2014, http://goo.gl/gQiCWV
10. 2015 Global Megatrends in Cybersecurity, Ponemon Institute, 2015, http://goo.gl/H1auq9
11. The top security threats of 2016, ZDNET, 2016, http://goo.gl/GrwlFh
12. Minchev, Z. Challenges to Human Factor for Advance Persistent Threats Proactive Identification in Modern Social Networks, In Proceedings of NATO Advanced Research Workshop “NATO ARW: Encouraging Cyber Defence Awareness in the Balkans”, Skopje, Macedonia, March 17-19, Published by ‘Information & Security. An International Journal’, vol.34, 2016 (in press).
13. Borschev, A. The Big Book of Simulation Modeling, AnyLogic, North America, 2013.
14. Kick, J. Cyber Exercise Playbook, The MITRE Corporation, 2014, https://goo.gl/SOkkw6
15. Minchev, Z. & Shalamanov, V. Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach. In Proceedings of SAS-081 Symposium on Analytical Support to Defence Transformation, RTO-MP-SAS-081, Sofia, NATO RTO ST Organization, 22-1-22-16, 2010.
16. NATO Cooperative Cyber Defence Center of Excellence Web Page, https://ccdcoe.org/
17. Minchev, Z. Security Foundations in Cyber Space, Training Course Selected Materials, http://dox.bg/files/dw?a=f42e63cffd
18. CYREX 2016 Facebook News Post, February 26, 2016, https://goo.gl/Pa8ArN
19. Minchev, Z., Dukov, G., Ivanova, T., Mihaylov, K. Boyadzhiev, D., Mateev, P., Bojkova, M., Daskalova, N. Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, FASTUMPRINT, pp. 85-92, 2015.
20. Shalamanov, V., et al, Security Research and Change Management in the Security Sector, Change Management Series, Institute for Parallel Processing, G. C. Marshall Association – Bulgaria (in Bulgarian), Demetra Ltd., Sofia, 2008, http://gcmarshall.bg/wp-content/uploads/2015/11/11.-secres.pdf
21. Minchev, Z. & Boyanov, L. System Modelling & Experimental Assessment of IoT Cyberthreats in Future Smart Homes, In Proceedings of ICAICTSEE – 2015, Sofia, UNWE, 2016 (in press)