Information & Security: An International Journal

Zlatogor Minchev, v.34:2, 2016, 123-136 https://doi.org/10.11610/isij.3405

CHALLENGES TO HUMAN FACTOR FOR ADVANCE PERSISTENT THREATS PROACTIVE IDENTIFICATION IN MODERN SOCIAL NETWORKS

Zlatogor MINCHEV

Abstract: The paper looks into the issue of proactive advanced persistent threats (APTs) identification in modern social networks. As these threats are quite unnoticeable and require a long-term, comprehensive monitoring of both technologies and users, a hybrid methodological framework is proposed. A combination of: experts' knowledge and beliefs, system analysis and real environment interactive validation is presented to meet practical APT challenges. The obtained results provide an explanatory foundation for a better understanding the interaction process of the human factor with future technological developments and resulting evolution of threats in cyber space.

Keywords: social networks, human factor, cyber space, advanced persistent threats, proactive identification.

1. Introduction

Today's digital world is generating numerous cyber threats as a result of the human-machine interaction. Though there are some recent reports on increasing risks related to artificial intelligence (AI),[1] the human factor still takes responsibility of the interaction effects in the 'machine-to-machine' independent cooperation.

Modern cyber landscape is a complex mixture of technologies, people and digital environment, encompassing numerous regular activities with resulting planned and unplanned security gaps. The big problem behind is that the IT revolution happens at a fast pace and provides fascinating opportunities in the form of new services and technologies. These have nurtured an environment conducive to the evolution of cyber-threats that is difficult to be countered or foreseen.[2]

An indispensable part of the problem is the regular competition among governments, companies and people, resulting into espionage activities that are difficult to cope with, especially such carried out by insiders.

Looking at this problematic field from the Advanced Persistent Threats (APTs) perspective,[3] many practical examples from the last few years could be listed – starting from the Aurora operation, going through WikiLeaks and Stuxnet, to VISA/Master credit cards and US OPM data leakages, celebrity images hacks, mobile ransomware, botnets attacks, joined with hacktivist groups and finishing with social engineering multimedia posts.

APTs are everywhere and are constantly evolving from a technological perspective, mostly targeting large organisations and groups.[4] So, guessing when next 'zero day attack' will be and what technological and user digital components are going to be affected becomes a rather ambiguous and complex task.

From another perspective, the focus on communication in our millennium has shaped the phenomenon of social networks: a digital billion users' community that in the Web 3.0 era, until 2020 will be mobile-advanced, privacy-threatening, reality-mixed and connected gadgets'-flooded.[5] This unfortunately produces fruitful soil for APTs' growth and successful negative implementation.

What is proposed next in the paper is a hybrid (human-machine) methodological framework that was successfully used for proactive exploration of complex cyber threats.

2. Framework for APTs Proactive Exploration

The proposed hybrid methodological framework (see Figure 1) was initially developed and tested for identification of cyber threats to social networks and smart homes.[6]

Further on, with some modification, it was applied to explore multimedia[7] and hybrid threats.[8] What is important to note here is the modification, related to the establishment of problem space. In earlier works of the author[9] and similarly to the present approach, an experts-defined multidimensional matrix is used. This approach is static in comparison to the one described in another publication by Minchev,[10] where the dynamics is implemented through selected but unscripted users' scenario activities. Thus a certain degree of interactiveness is added here, during the validation phase, using dynamic simulation scenario script.[11] This also provides synchronisation between the monitoring of the human factor's response and the 'zero days' events, observing simultaneously the activities, related to APTs' attacks.

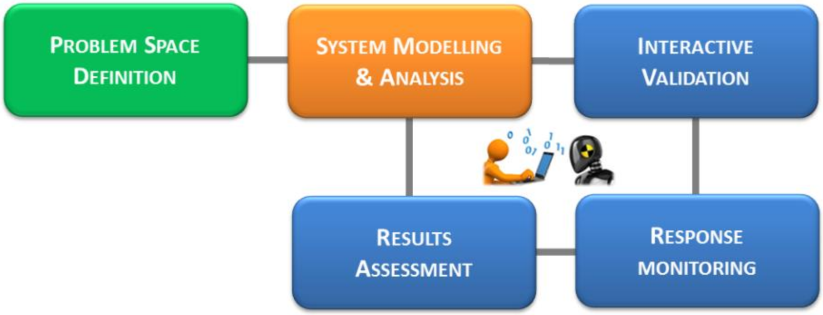


Figure 1. Hybrid methodological framework for APTs proactive identification.

As it is clear from Figure 1, the proposed framework encompasses three basic stages of human-machine cooperation: (2.1) *Problem Space Definition*, (2.2) *System Modelling & Analysis*, (2.3) *Interactive Validation*. Additionally, the validation process is also involving: (2.3.1) *Response Monitoring* and (2.3.2) *Results Assessment*.

Details with real examples for practical framework implementation will be given further in the paper.

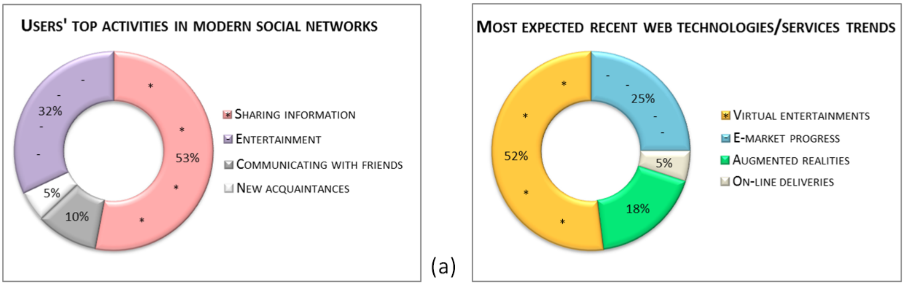
2.1. Problem Space Definition

Defining the problem space for APTs identification is a complex and challenging task. Practically, it could be served by collecting experts' qualitative opinions in focus groups, using different techniques: brainstorming, backcasting, discussions, questionnaire based surveys or other similar approaches.[12]

One such study was organised in 2015, with approximately 300 students from the University of National and World Economy, Sofia. The students were asked to respond to questionnaires aimed at identifying multiple digital activities and technological trends in the next five years. A summary of the results, specifically users' top activities in social networks and web technologies/services trends are given in Figure2a.

Another study with more than 100 national and international experts was recently organised, preparing analysis for 'Bulgarian Cyber Security Strategy 2020'.[13]

Both studies were also enriched with a solid research in the field by EU SysSec Network of Excellence in System Security[14] and their Red Book.[15] The aggregated results were summarized into a matrix of expected APTs and developing technological areas up to 2020 (see Figure 2b).



(a)

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*

(b)

Figure 2. Aggregated results of future social network users' activities and technological trends (a); a matrix of expected APTs for fast developing technological areas (b) up to 2020.

As it is clear from Figure 2a, the most expected areas of technological progress are related to: *Virtual and Augmented Realities* together with *E-market Progress*. In the Web 3.0 era these will definitely be a vector of evolution of the social networks. Concerning users' expected activities, preference is given to: *Sharing of Information* and *Entertainment*. Going further, *Transformed Privacy*, *Biometric Disturbances* and *Espionage* are rated as the most serious influencing APTs for the whole fivefold 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. Within this context, the recent outlook of Ponemon Institute and ZDNet[16] on cyberthreats and cyberattacks should also be noted, supporting our findings so far.

As these results are quite general, a more detailed analysis will be provided in the next paragraph. A special focus is given to the evolution of the social networks, their billions of users and the relationship with the already noted technological sets of interests.

2.2. System Modelling & Analysis

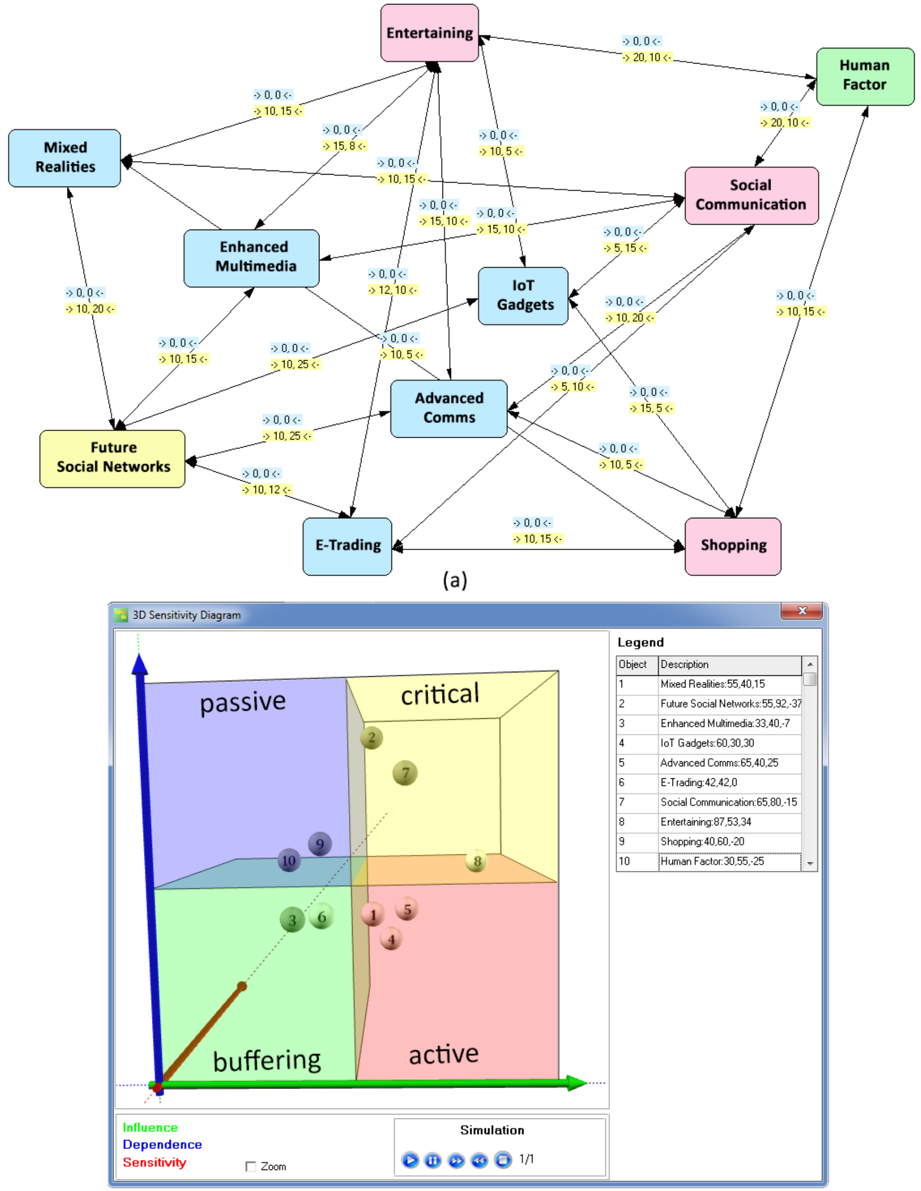
Proper understanding of complex environments requires a suitable approach for modelling and analysis. Bertalanffy's General Systems Theory[17] and its further dynamic generalisation of Vester[18] are a good starting point for this.

The process was implemented with numerous cyber threats[19] in I-SCIP-SA software environment.[20] The approach is using graphical interpretation of Chen's 'E-R' paradigm,[21] describing elements as related entities in the model. All relations (uni- or bi-directional) are weighted and time dependent (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, labeled for both weight (yellow) and time (blue). Model assessment is based on experts' beliefs for the relations weight and their time trends, implemented into a three dimensional Sensitivity Diagram (SD), using: influence (*x*), dependence, (*y*) and sensitivity (*z*) values. SD is providing 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 a certain sector is also accomplished. This is directly related to sensitive elements' evaluation towards the *z* axis. All entities from the model are visualised in SD with indexed balls.

The practical application of I-SCIP-SA environment system modelling and classification of future social networks interrelations with human factor activities and new technological trends up to 2020 (see Figure 3) was successfully prepared with the support of *Problem Space Definition* stage and EU ACDC project final conference discussions.[22]

As could be observed in Figure 3, the resulting static model classification is defining as critical the following user activities: 'Future Social Networks' – '2,' 'Social Communications' – '7' and 'Entertaining' – '8.'

These critical entities were also studied and in other similar publications.[23] Active entities are: 'Mixed Realities' – '1,' 'Advanced Comms' – '5' and 'IoT Gadgets' – '4.' Passive ones are: 'Human Factor' – '10' and 'Shopping' – '9.' Finally, 'Enhanced Multimedia' – '3' and 'E-Trading' – '6' are buffering.



(a)

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 3. System model (a) and resulting SD assessment (b) of future social networks aggregated interrelations with human factor activities and new technological trends up to 2020.

As the proposed system analysis classification is based on experts' beliefs, users' and literature data, a practical dynamic results validation would be of great value. This was organised in the final, third stage, trough *Interactive Validation*, providing experimental observations, concerning different APTs with real devices, environment and evaluation of human-in-the-loop responses.

2.3. Interactive Validation

Generally, the validation stage is a multidimensional issue, depending mostly on the human factor, so this stage was organised as a three-fold one: (2.3.1) *Computer Assisted eXercise* (CAX) *Simulation* with human-in-the-loop active role, implementing: (2.3.2) users' direct and indirect *Response Monitoring* and (2.3.3) *Results Assessment*.

2.3.1. CAX Simulation

The simulation has been successfully implemented for a dynamic study of APTs, following the ideas for CAX interactive organisation[24] and several practical implementations in the cyber space.[25] The framework architecture encompasses an agent-based paradigm (see Figure 4a), using organisation of negotiations[26] around a 'Coordinating agent' and being closer to the real working conditions in the digital environment. As the study is for selected APTs (see Figure2b), a specific agents' scenario script was implemented.

Two important moments in this script preparation have to be noted: the selection of driving factors (key objects)[27] and the type of cyberattacks.[28] At the same time, the APTs require a dual role for the human factor, both 'Playing agent$_{k,}$' (k – number of playing agents, $k \in$ N) and 'Attacking agent' have to be actively involved as 'moderators' and 'users,' following the idea, proposed by the author in previous works.[29] Cyberattack events are notified by an 'Alarming agent.' All the results from the simulation are observed by a 'Monitoring agent' and archived by 'Storing agent'. The supporting information is provided by 'Assisting agent.'

The proposed architecture was recently tested in 'Academic Cyber CAX 2015' (see Figure 4), during the training course 'Security Foundations in Cyberspace'[30] of Plovdiv University 'Paisii Hilendarski'.

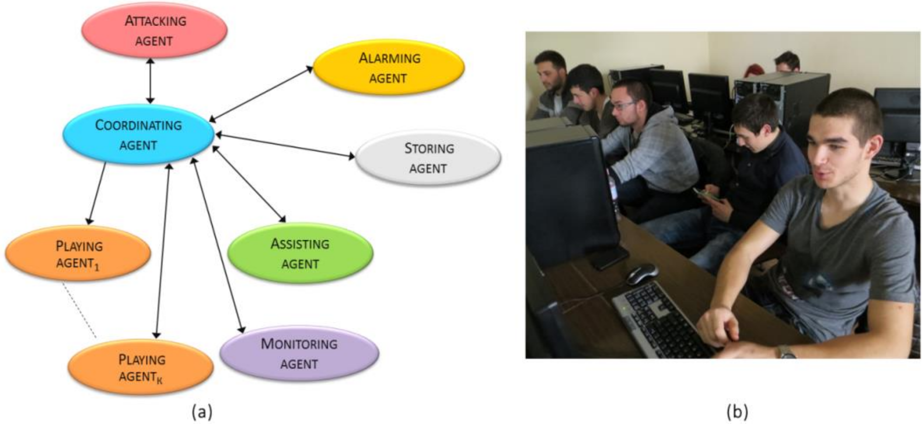


Figure 4. Cyber CAX agent-based framework architecture (a) and moments of its practical implementation during 'Academic Cyber CAX 2015' (b).

A closed group on Facebook (comprising 30 students in computer science, at an age 23 +/- 2 years), some augmented reality multiple smart gadgets (tablet, smartphone, i-pod, ultrabook), combined with regular desktop PCs, LAN Wi-Fi router (for easy private network establishment and events logging/storing), private mail server and standard SMS notifications were used.

Using this CAX organization, 'Entertaining' and 'Social Communication' activities of the participants were studied, being classified as critical (see Figure 3b). A social engineering complex cyberattack,[31] using: multimedia, data encryption, malware, insiders and data breaching were accomplished. This in practice covers mostly of the social networks' APTs evolution prognostic trends (see Figure 2). The total duration of the exercise was approximately three hours.

The results of the CAX simulation could be evaluated, following the next two-substage methodology, using participants' direct and indirect feedback. Further on, some practical experience will be shared for solving this rather ambitious task.

2.3.2. Response Monitoring

The monitoring of the users' direct feedback is performed with a selected biometrics battery. It was successfully tested during this stage, evaluating the motivation behind the users' behavior and their emotions in social networks and smart environments.[32] Personality assessments of the users' temperament, depression and sensation seeking were also measured. Additional battery of physiological parameters for brain, heart, posture and skin response dynamics were studied for different situational scenarios of multimedia influence.[33]

As a result of the biometric battery's direct feedback application, several quantitative proofs of negative multimedia modifications, providing possible social engineering support via audio-visual users' entrainment have been discovered,[34] confirming this approach's practical significance for APTs exploration in the context of *IoT Gadgets*, *Mixed Realities*, *Enhanced Multimedia* and *Advanced Communications* (see Figure 2a). The *E-Trading* was not specifically explored in the study, though found as a possible hidden cyber threat driver (see Figure 3b).

Next, regarding the APTs investigation through an interactive cyber CAX, the users' response time to events was also studied, following the idea of time stamping, to be found in the exercise's script.[35] This represents an indirect observation of the users' during the simulation process. The main objective is to evaluate the participants' stress levels (see Figure 5).

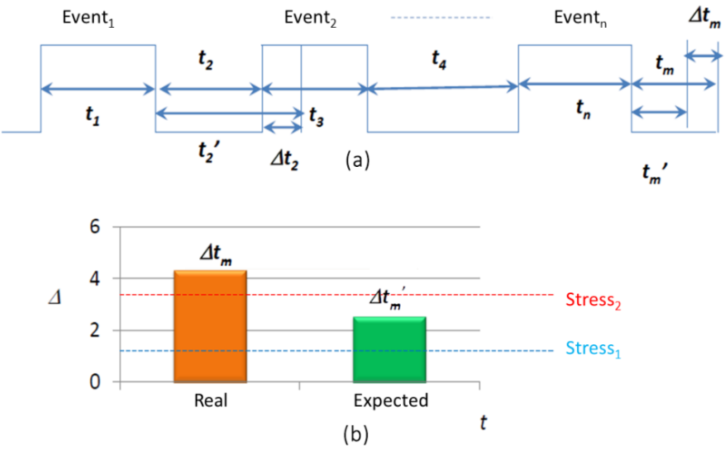


Figure 5. Cyber CAX events timeline example (a) vs their response time delays and averaged participants' stresses assessment (b).

The experiments in this context during 'Academic Cyber CAX 2015' have clearly demonstrated successful monitoring via the 'Coordinating agent' and 'Storing agent' and dominating response time delays – Δt_m (m – number of observed delays, $m \in$ N) for most of the participants that clearly outlines a successful ambiguity inclusion due to multiple injection events. The registered response delays fluctuations are closely related also to the stress level (either augmented or diminished, see Figure 5b) that is rather important for successful exercise application. This practically changes the prioritisation of tasks of the participants in the exercise, due to the events' dynamics and to new events' being of greater interest for the trainees.

Thus, in practice, a clear demonstration of the negative effect of social engineering multimedia, data encryption, malware, insiders and data breaching has been successfully observed.

A final validation and another source of direct feedback were structured through additional participants' multidimensional self-assessment.

2.3.3. Results Assessment

The idea behind is quite comprehensive, implementing the questionnaire based (q-based) assessment[36] and its systematisation with techniques like 'Delphi method'[37], following the Balanced Score Card approach[38] and application experience from the security area.[39]

Selected aggregated results are provided (see Figure 6) in this context for communication environment, implementing threats, attacks, and exercise usefulness, gathered from the event participants after 'Academic Cyber CAX 2015.'

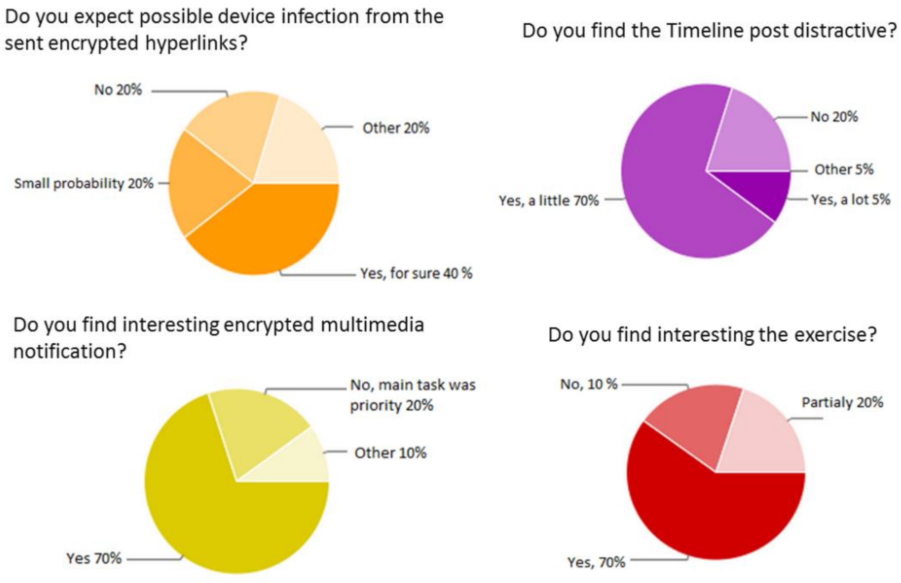


Figure 6. Selected results for 'Academic Cyber CAX 2015' participants' q-based assessment.

An important aspect of the practical implementation of the assessment process is the participants' motivation for filling-up questionnaires with proper information. Unfortunately, it is difficult to be achieved and checked, together with correct questions understanding. This naturally generates noisy data results from the users' response monitoring perspective that have to be used only in combination with the indirect feedback data.

Thus achieving comprehensive and, at the same time, realistic overall proactive future APTs identification requires a complex and dynamic validation stage.

Conclusion

Obviously modern digital environment will be constantly evolving in the next five years with web technologies as an environment shaper of the human-machine interaction process. This will definitely generate a number of new cyberthreats and attacks for the modern digital users, being to certain level, closely related to APTs' evolution.

The near future's social networks are expected to implement new smart gadgets and advanced AI in the communication and entertainment environment. These will make them more attractive for their billion users' community. Further on, the e-trading is also expected to evolve jointly with the advertisement progress.

Concerning this complex environment, the presented hybrid methodological framework for identifying APTs by means of a multistage approach, combining technological and human factor capacity, is quite suitable and promising for proactively meeting new challenges to the digital society.

However, it is still important to understand the digital environment 'moderators' objectives and motives that practically produce new cyberthreats. A further methodology development in this direction, is the integration of multiple mobile sensors for smart monitoring of both the environment and the human factor.

This hopefully will provide an advanced understanding of the 'human-machine' interaction in modern social networks, outlining the demanding proactive role of the human factor, both as a 'user' and 'moderator,' especially noting the expected 'machine-to-machine' interaction fast evolution, that needs to be adequately used and controlled in the modern digital society.

Notes:

[1] Global Risks 2015, 10th Edition, World Economic Forum, 2015, available at: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf; Technology Trends to Watch 2015, CEA, 2015, available at http://content.ce.org/PDF/2014_5Tech_web.pdf.

[2] Zlatogor Minchev, "Human Factor Role for Cyber Threats Resilience," *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, 2015.

[3] Tyler Wrightson, *Advanced Persistent Threat Hacking*, McGraw-Hill Education, 2015.

[4] *2015 Global Megatrends in Cybersecurity*, Ponemon Institute, 2015, available at: http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

[5] Zlatogor Minchev, "Future Threats and Challenges in Cyberspace," CSDM Views, 31, CSDM, Institute of ICT, Bulgarian Academy of Sciences, 2015, available at: http://it4sec.org/bg/article/prognozni-zaplahi-i-predizvikatelstva-v-kiberprostranstvoto.

[6] Zlatogor Minchev, "Cyber Threats in Social Networks and Users' Response Dynamics," *IT4SEC Reports* 105, available at: http://dx.doi.org/10.11610/it4sec.0105; L. Boyanov and Zlatogor Minchev, "Cyber Security Challenges in Smart Homes, Cyber Security and Resiliency Policy Framework," *Cyber Security and Resiliency Policy Framework* 38, NATO Science for Peace and Security Series, D: Information and Communication Security (Amsterdam, The Netherlands: IOS Press, 2014).

[7] Zlatogor Minchev, "Cyber Threats Analysis in On-Line Social Networks with a Study on User Response," *IT4SEC Reports* 115, available at: http://dx.doi.org/10.11610/it4sec.0115.

[8] Zlatogor Minchev et al, "Hybrid Challenges to Cyberspace and the Role of the Human Factor," *Proceedings of International Scientific Conference "South-East Europe: New Threats for the Regional Security,"* New Bulgarian University, June 2015, https://goo.gl/lXFeRz.

[9] Zlatogor Minchev, "Cyber Threats Analysis in On-Line Social Networks with a Study on User Response;" Zlatogor Minchev et al, "Hybrid Challenges to Cyberspace and the Role of the Human Factor."

[10] Zlatogor Minchev, "Human Factor Role for Cyber Threats Resilience."

[11] Zlatogor Minchev et al, "Hybrid Challenges to Cyberspace and the Role of the Human Factor."

[12] Luke Georghiou, Jennifer Cassingena Harper, Michael Keenan, Ian Miles, and Rafael Popper, eds., *The Handbook of Technology Foresight: Concepts and Practice* (Cheltenham, UK: Edward Elgar Publishing, 2008.

[13] Zlatogor Minchev, "Future Threats and Challenges in Cyberspace," *CSDM Views* 31, CSDM, Institute of ICT, Bulgarian Academy of Sciences, 2015, available at: http://it4sec.org/bg/article/prognozni-zaplahi-i-predizvikatelstva-v-kiberprostranstvoto.

[14] SysSec Network of Excellence Home Page, available at http://www.syssec-project.eu/.

[15] Davide Balzarotti and Evangelos Markatos, eds., *The Red Book – A Roadmap for Systems Security Research*, SysSec Consortium, 2013, available at http://red-book.eu.

[16] *2015 Global Megatrends in Cybersecurity; Cybersecurity in 2015: What to expect?* ZDNET, 2014, available at http://www.zdnet.com/article/cybersecurity-in-2015-what-to-expect/.

[17] Ludwig von Bertalanffy, *General System Theory: Foundation, Development, Applications* (New York: George Braziller, 1968).

[18] Frederic Vester, *The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity* (München, MCB-Verlag, 2007).

[19] 2015 Global Megatrends in Cybersecurity, Ponemon Institute; Zlatogor Minchev *et al.*, "Hybrid Challenges to Cyberspace and the Role of the Human Factor."

[20] Zlatogor Minchev, "Intelligent Scenario Development for CAX," *Proceedings of NATO ARW: "Scientific Support for the Decision Making in the Security Sector," Velingrad, Bulgaria, 21-25 October 2006*, NATO Science for Peace Security Series, D: Information and Communication Security 12 (Amsterdam: IOS Press, 2007); Zlatogor Minchev and M. Petkova, "Information Processes and Threats in Social Networks: A Case Study," *Conjoint Scientific Seminar 'Modelling and Control of Information Processes',* Sofia, Bulgaria, November, 85-93, 2010.

[21] Peter Chen, "The Entity-Relationship Model-Toward a Unified View of Data," ACM Transactions on Database Systems 1, no.1 (1976): 9-36, https://doi.org/10.1145/320434.320440.

[22] Advanced Cyber Defence Centre Home Page, http://acdc-project.eu/.

[23] Zlatogor Minchev, "Cyber Threats in Social Networks and Users' Response Dynamics"; Zlatogor Minchev, "Cyber Threats Analysis in On-Line Social Networks with a Study on User Response."

[24] Zlatogor Minchev and Velizar Shalamanov, "Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach," *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.

[25] Zlatogor Minchev, "Human Factor Role for Cyber Threats Resilience," *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare* (IGI Global, 2015); L. Boyanov and Zlatogor Minchev, "Cyber Security Challenges in Smart Homes, Cyber Security and Resiliency Policy Framework."

[26] Gerhard Weiss, ed., *Multiagent Systems* (Cambridge, MA: MIT Press, 2013).

[27] Zlatogor Minchev *et al.*, "Hybrid Challenges to Cyberspace and the Role of the Human Factor"; Zlatogor Minchev and Velizar Shalamanov, "Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach."

[28] 2015 Global Megatrends in Cybersecurity.

[29] Zlatogor Minchev, "Social Networks Security Aspects. A Technological and User Based Perspectives," *Proceedings of Jubilee National Conference with Foreign Participation 'TELECOM 2012,'* Sofia, October 18-19, 14-21, 2012.

[30] Zlatogor Minchev, Security Foundations in Cyber Space, Training Course Selected Materials, available at http://dox.bg/files/dw?a=f42e63cffd, accessed July 30, 2015.

[31] Christopher Hadnagy, *Unmasking the Social Engineering. The Human Element of Security*, John Wiley & Sons, Inc., 2014.

[32] Minchev, "Human Factor Role for Cyber Threats Resilience."

[33] Minchev, "Human Factor Role for Cyber Threats Resilience."

[34] Zlatogor Minchev, "Cyber Threats Analysis in On-Line Social Networks with a Study on User Response;" Z. Minchev, E. Kelevedjiev, P. Gatev, "Audio-Visual Entrainment Influence on Postural Dynamics," Proceedings of International Workshop 'Posture, Balance and the Brain,' Thessaloniki, Greece, 55-60, 2015, available at: http://www.biomed-data.eu/article/audio-visual-entrainment-influence-postural-dynamics.

[35] Zlatogor Minchev *et al.*, Joint Training Simulation and Analysis Center, Technical Report, Sofia, Institute for Parallel Processing, Bulgarian Academy of Sciences, 2009, http://gcmarshall.bg/wp-content/uploads/2015/11/9.-jtsac_tr.pdf.

[36] Luke Georghiou, Jennifer Cassingena Harper, Michael Keenan, Ian Miles, and Rafael Popper, eds., *The Handbook of Technology Foresight: Concepts and Practice*.

[37] Murray Turoff and Harold Linstone, eds., *The Delphi Method: Techniques and Applications*, 2002, available at http://www.is.njit.edu/pubs/delphibook/.

[38] David Norton and Robert Kaplan, *The Balanced Scorecard: Measures that Drive Performance*, Harvard Business Review, January-February, 71-79, 1992.

[39] Velizar Shalamanov *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.

About the Author

Zlatogor Minchev is an Associate Professor with the Institute of Information and Communication Technologies and the Institute of Mathematics & Informatics, Bulgarian Academy of Sciences. He is also Director of the Joint Training Simulation & Analysis Centre, specialised in applied computer science applications in the security area. His achievements are highly appreciated by UN, EU and NATO. Awarded for his professional and team work by governmental and international bodies throughout the world. Recognized as 'NATO Opinion Leader' on security & cybersecurity problems. Sofia 1113, Acad. Georgi Bonchev Str., Bl. 25A, Bulgaria.
E-mail: zlatogor@bas.bg.