Modern Social Networks Emerging Cyber Threats Identification

A Practical Methodological Framework with Examples

Zlatogor Minchev
IT for Security Department, JTSAC
Institute of ICT, Bulgarian Academy of Sciences
Sofia, Bulgaria
zlatogor@bas.bg

Suzan Feimova
IT for Security Department, JTSAC
Institute of ICT, Bulgarian Academy of Sciences
Sofia, Bulgaria
sfeimova@gmail.com

***Abstract* — The paper is considering some of the emerging trends in cyber threats identification implementing an ad-hoc practical methodological framework. An accent on the social networks problems progressing severity in the evolving smart environment of communication and living is given. The framework is encompassing the national academic experience in the area gathered in the past four years from both international and national joint research. Four key phases of organization are utilized: (i) Cyber threats identification, (ii) Context definition, (iii) Analysis, (iv) Validation. In practice, an implementation of morphological and system analysis together with agent-based modeling and constructive simulation, followed by human factor biometrics validation is used. Several illustrative empirical case studies addressing the problem are also considered in the paper.**

***Index Terms* — cyber security, social networks, cyber threats identification framework**

I. Introduction

Modern social networks have become a key enabler for todays' innovative web technologies developments. The new fast progressing mobile smart devices, apps and services are already provoking a visible change in the way of using and understanding social interaction activities.

The nowadays role, importance and understanding for digital social communication is obviously progressing and with the improved network services, embedded software, AI and innovative natural interface designs.

Being quite common for the humans' social nature from one hand, and thus extremely popular from another, social networks have successfully entered the cutting innovative technological focus with few billion of users, accessing large data amounts, for less than ten years development period [1].

This social networks technological boom is opening and a number of obvious and hidden emerging cyber threats for the technologies users (creators) in the new digital society.

A comprehensive recent study on the problem is outlining a few cybersecurity challenges related to users' privacy, data control together with new devices reliability [2].

From user perspective, accents related to emotional & behaviour responses [3], digital culture and legal regulations necessities [4] are giving a final touch to this problem space comprehensive understanding.

Further on, in the paper, a brief overview of a practical methodological framework, concerning social networks emerging cyber threats identification accents will be given.

II. Methodological Framework

The implemented methodological idea has been developed for progressive studying of digital world cyber threats in partnership with EU SysSec (www.syssec-project.eu) consortium efforts since 2010.

Social network accent was given in the framework of DMU 03/22 (www.snfactor.com) research project.

Generally, the idea is implementing experts' alternative futures analysis (morphological and system one), followed by human factor biometrics monitoring validation.

Four key phases of organization have been utilized (see Fig.1): (i) *Cyber threats identification*, (ii) *Context definition*, (iii) *Analysis* and (iv) *Validation* [5].

III. Practical Implementation

Cyber threats identification phase is accomplished through collecting users' focus group data gathered from brainstorming, discussions and further filtered via q-based surveys [6].

As in the next five years ICT trends will be basically related to Web 3.0 technologies developments [2], a recent survey related to popularity of social networks together with types of information exchanged and user activities concerning smart devices have been performed amongst 250 participants from the smart environment of living perspective [7].

Partial generalization of the results could be briefly summarized as follows: the top four most popular social networks are *Facebook* (90%), *LinkedIn* (30%), *Google+* (20%) and *YouTube* (15%), where the users exchange basically *Text messages* (70%) and still less *Multimedia contents* (20%) for *Communications* (90%) and *Entertainment* (30%). The percentages sum is over a hundred, as the participants were allowed to give more than one answer.

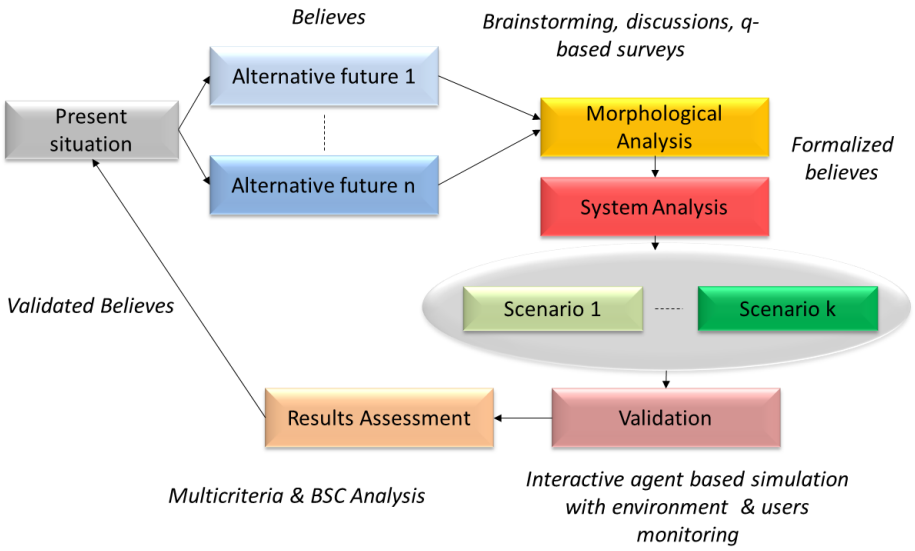

Fig. 1. Graphical representation of the methodological framework for emerging cyber threats identification.

The *Context definition* phase is in fact experts' based ranking of the identified threats and selection of "driving factors" around future scenarios producing a "plausible future" scenario set [6].

Further structuring around these "driving factors" is performed at the *Analysis* phase, encompassing both morphological and system analysis, supported by I-SCIP-MA-SA software environment [6].

The morphological analysis is producing initial relatively weighted positive (negative) context scenarios classification placed in a cross-consistency matrix (containing *Dimensions* - columns and mutually exclusive *Alternatives* - columns' cells).

An example [3] concerning a morphological analysis for social networks context scenarios matrix (with N=2016 combinations) in I-SCIP-MA is given at Fig.2.

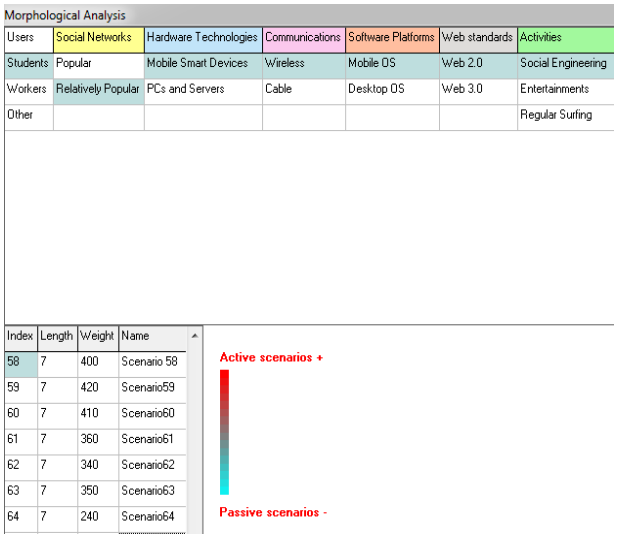

Fig. 2. A screen shot from I-SCIP-MA of morphological cross-consistency matrix with N = 2016 scenario combinations for social networks cyber threats exploration [3].

The detailed implementation of the selected "driving factors" role is determined next in I-SCIP-SA, through system analysis by using *Influence* (*x*), *Dependence*, (*y*) and *Sensitivity* (*z*) ratio "Sensitivity Diagram" (SD) classification in four sectors: green (bottom-left zone, buffering), red (bottom-right zone, active), blue (top-left zone, passive) and yellow (top-right zone, critical). All entities from the system analysis model are visualized in SD with indexed balls [6].

An example concerning a system analysis for social networks driving factors understanding regarding "Entertainment" and "Social Engineering" users' activities in I-SCIP-SA is given on Fig.3.

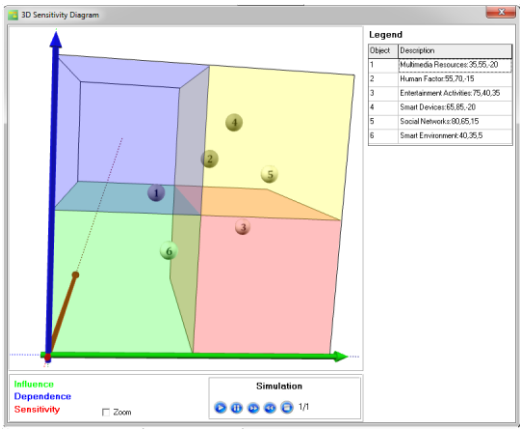

Fig. 3. A screen shot from I-SCIP-SA model resulting classification for social networks driving factors classification regarding "Entertainment" and "Social Engineering" users' activities.

The results from Fig.3 give a profitable classification of model entities, outlining the "Human Factor" as a critical entity together with "Smart Devices" and "Social Networks". The "Entertainment Activities" are noted as active entity and "Multimedia Resources" as passive one, thus suitable for social engineering exploration [3]. "Smart Environment" is a buffering entity, assuming neutral influence in the current model.

Finally, the *Validation* phase is concerning structured and analyzed experts' believes testing and results assessment. Currently, the modeling and simulation during this phase is based on multiagent interactive simulation in I-SCIP-SA with human-in-the-loop participation in an experimental smart test bed environment [7].

Additional monitoring of external environment characteristics like temperature, humidity, dust, etc. is also implementable for the smart environment of exploration [7].

As our study is accentuating on the importance of the human factor response, simultaneous multimodal biomonitoring of users' activities in social networks (in accordance with the preliminary defined scenario driving factors set) is performed [3], [8] (see Fig 4.).

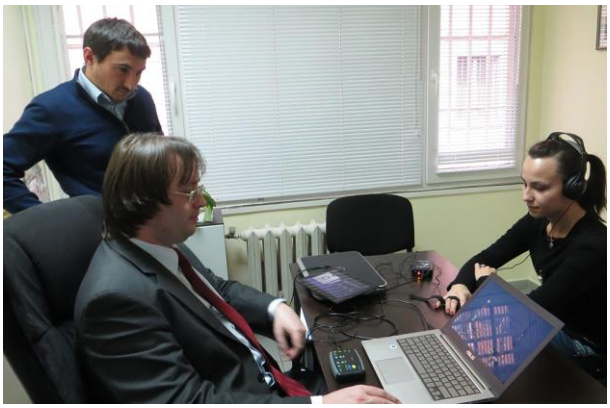

Fig. 4. Moments of the *Validation* phase experiments.

Further, audio-visual biofeedback users training through a specialized methodological protocol [9] and balanced score card multicriteria experts' evaluation of the obtained results is accomplished [10].

IV. Discussion

Nowadays the modern social networks and web technologies developments are opening a number of cyber threats to their users. As some of them are quite obvious, other related to entertainment and users' emotional and behavior responses are producing a lot of hidden ones. Examples for such cyber threats are basically related to different multimedia applications in the social engineering processes.

A suitable framework approach for studying these problems is the combination of experts' believes data, analysis, modelling, users and environment monitoring, as well as, practical validation through real constructive experimental simulation. This does not assure comprehensiveness, but at least provides plausibility of the obtained results.

Acknowledgements

The authors express a special gratitude for the financial support to: A Study on IT Threats and Users' Behaviour Dynamics in Online Social Networks, DMU03/22, Bulgarian Science Fund, Young Scientists Grant, 2011-2014, www.snfactor.com.

Explicit thanks for future cyber threats context definition and analysis methodological support to: EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet – SysSec, FP7 Grant Agreement No. 257007, 2010 – 2014, www.syssec-project.eu.

References

[1] M. Stelzner, Social Media Marketing Industry Report, 2013, http://www.socialmediaexaminer.com/SocialMediaMarketingIndustryReport2013.pdf

[2] E. Markatos, E., et al., The Red Book. The SysSec Roadmap for Systems Security Research, The SysSec Consortium, 2013, http://www.red-book.eu/m/documents/syssec_red_book.pdf

[3] Z. Minchev, Cyber Threats in Social Networks and Users' Response Dynamics, IT4SEC Reports, No. 105, http://www.it4sec.org/bg/system/files/IT4Sec_Reports_105_2.pdf

[4] F. Schreier, B. Weekes, T. Winkler, "Cyber Security: The Road Ahead", DCAF Horizon 2015 Working Paper no.4, 2011.

[5] Z. Minchev, "Security of Digital Society. Technological Perspectives & Challenges", In Proceedings of New Bulgarian University Jubilee International Scientific Conference book 'Ten Years Security Education in New Bulgarian University: Position and Perspectives for the Education in a Dynamic and Hardly Predicted Environment', Sofia, Planeta 3 Publishing House, 2013, pp. 438-444.

[6] Z. Minchev, V. Shalamanov, "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, Boyana, April 26 – 28, 2010, pp. 22-1 – 22-16.

[7] L. Boyanov, Z. Minchev, A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes, DFNI T01/4 National Science Fund Project Technical Report, Part I, Institute of ICT, Bulgarian Academy of Sciences, December, 2013.

[8] Z. Minchev, "2D vs 3D Visualization & Social Networks Entertainment Games. A Human Factor Response Case Study", In Proceedings of 12th International Conference, ICEC 2013, São Paulo, Brazil, October 16-18, 2013, Lecture Notes in Computer Science, vol. 8215, 2013, pp. 107-113.

[9] A. Dejnowicz, Multimodal Beeofeedback. Methodology & Application, DMU 03/22 Study Report, Bulgarian Association on Biofeedback, ADEA Ltd., Sofia, Bulgaria, 2013

[10] Z. Minchev, et al, Joint Training Simulation & Analysis Center, Technical Report, Institute for Parallel Processing, Bulgarian Academy of Sciences, 2008.