The Eight International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

BUSINESS INFORMATION SECURITY CONFERENCE

EMERGING HYBRID THREATS MODELLING & EXPLORATION IN THE NEW MIXED CYBER-PHYSICAL REALITY

ZLATOGOR MINCHEV
Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences, zlatogor@bas.bg

GEORGI DUKOV
Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences, gdukov@bas.bg

Abstract: *The security environment nowadays is producing quite a lot of uncertainties and threats as a result of emerging cyber-physical hybrid clashes phenomena. Adequate exploration of this has to be taken into consideration jointly with future technological progress, combining both social & technological assets. A successful approach for handling the problem is demonstrated in the paper, implementing expert beliefs into an aggregated dynamic system model, together with further exploration, based on system analysis, validation & verification. The obtained results are showing promising holistic solution, giving opportunities for better understanding and countering future hybrid threats in the new mixed cyber-physical reality.*

Keywords: *Hybrid Threats, System Modelling, Validation & Verification, Cyber-Physical Reality*

1. INTRODUCTION

The 21st century digital revolution is nowadays producing numerous opportunities and threats, resulting from human-machine multimodal interaction in the new cyber-physical mixed reality. This practically generates a different environment of living, working, communicating and finally - 'digitizing' the lifestyle as a whole [1].

The development of web technologies, from the other hand, has successfully shifted the human factor behaviour from a passive user of Web 1.0 to an active player in Web 3.0. This active behaviour, jointly with Artificial Intelligence (AI) advancing and Internet of Things (IoT) concept integration boom, could bring, in the near future, a different social evolution dynamics. An assignment of more active role to autonomous Web 4.0 technologies with multiple output soft- and hardware effectors, instead of people only, have to be expected [2].

Meeting these progressive results in a suitable manner is quite a challenging task because it moves notions like: 'privacy', 'reliability', 'culture' and 'ethics' on a new cyber-physical level of understanding.

Concerning the human factor transformation in the upcoming digital reality, it will inevitably emerge novel, hybrid threats, posted in the present and future social resilience context [3], [4].

The paper initially outlines digital threats hybrid evolution perspectives in the new cyber-physical world, forming the modern mixed environment. A further practical approach for threats proactive exploration, using system analysis with results validation & verification, is also given for acheiving a comprehensivene outlook to the problem.

2. EMERGING THREATS EVOLUTION

The new security landscape, though difficult to be uniquely described, requires proper futuristic understanding. Adequately facing the new threats hybrid evolution from human - technologies clash is a rather challenging task.

A graphical generalization in this context for year 2020, originating from an extended recent survey [5] among more than 400 representatives from academia, universities, defence community and industry is given in Figure 1.

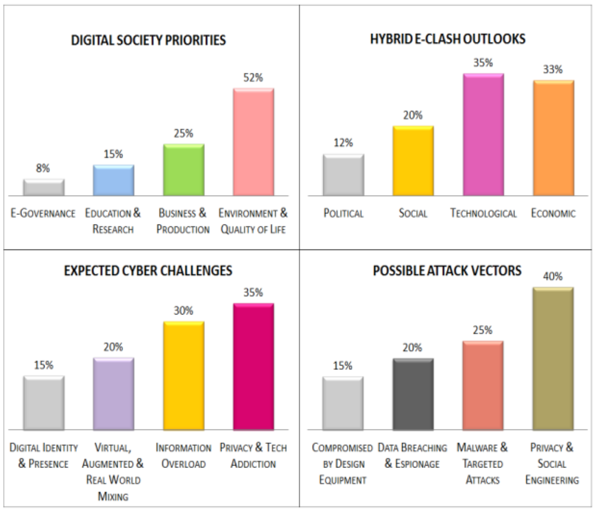


Figure 1: Expected digital society priorities, outlooks, challenges and attack vectors up to year 2020

Several major conclusions could be drawn from the presented results for both human and technologies evolution perspectives: (i) *Environment and Quality of Life* – 52%, *Business & Production* – 25%, *Education & Research* – 15% are expected to be top priorities in the next five years of the new digital era; (ii) *Technological* – 35%, *Economic* – 30% and *Social* – 20% outlooks will be considered as the e-clash assets, generating cyber challenges towards: (iii) *Privacy & Tech Addiction* – 35%, *Information Overload* – 30% and *Virtual, Augmented & Real World Mixing* – 20%, expected from several attack vectors: (iv) *Privacy and Social Engineering* – 40%, *Malware & Targeted Attacks* – 25%, *Data Breaching & Espionage* – 20%.

3. A SYSTEM ANALYSIS PERSPECTIVE

More detailed understanding of the outlined hybrid threats cyber-physical nature outlooks from Figure 1, is possible to be obtained with further system analysis implementation.

In the present study interviews and expert opinions data were used. The gathering process was based on: 14 nations during 'Cyber Forum DESSERT B2S – S2B', May, 2016 and 21 industrial companies, provided by Association of Communication & Information Specialists in the framework of 'HEMUS 2016' military exhibition and 'Defend IT', TeleGroup Workshop dedicated to IT Security, June, 2016.

Input data was generalized in I-SCIP-SA v.2.0 software environment. The application is specifically designed for multiple problems system exploration, based on complex discrete systems, machine Entity-Relationship (E-R) representation, organized over a weighted graph [6].

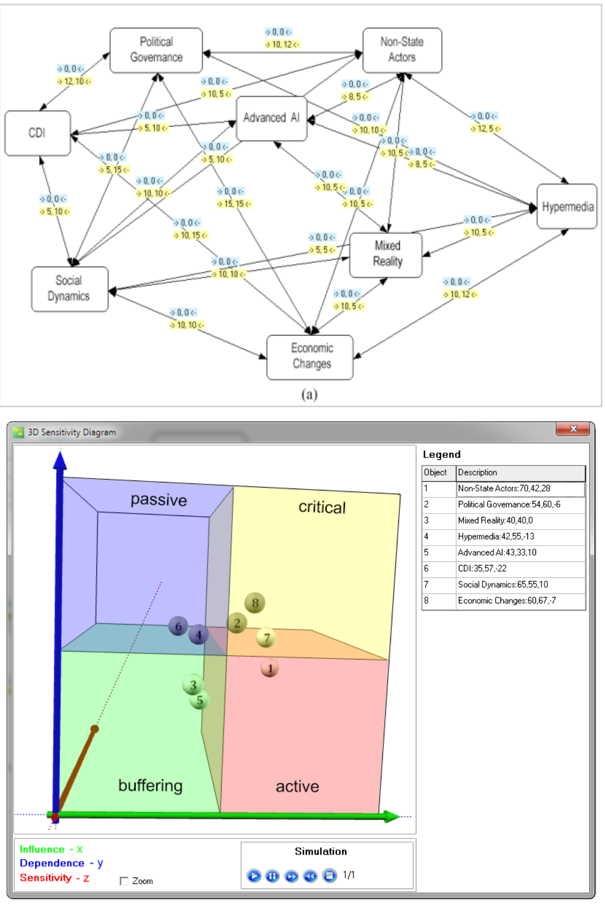
The resulting classification of model entities is visualized in 3D Sensitivity Diagram (SD) in accordance with relations weights (defined as single or multiple array values and measured in percentages from the interval [0, 1]): Influence – x (feed–forward), Dependence – y (feed–backward) and their relation – Sensitivity – z.

Four main sectors are defined in the 3D SD, following x and y values: buffering – green, active – red, passive – blue, critical – yellow. The model z values determine additional sub–classification of: active (z > = 0) and passive ($z < 0$) entities in every SD sector.

A graphical interpretation of future hybrid threats exploration model (a) and resulting analysis classification (b) in I-SCIP-SA, v.2.0 environment is depicted in Figure 2.

The system model is encompassing eight generalized entities, separated in two main parts: social ('Political Governance', 'Social Dynamics', 'Non-State Actors', 'Economic Changes') and technological ('Mixed Reality', 'Advanced AI', 'Hypermedia', 'Critical Digital Infrastructure' – CDI).

The entities from Figure 2a are next classified, following the input expert data initial assumptions as follows: critical: 'Political Governance' – 2, 'Economic Changes' – 8, 'Social Dynamics' – 7; passive: 'CDI' – 6, 'Hypermedia' – 4; active: 'Non-State Actors' – 1; buffering: 'Mixed Reality' – 3, 'Advanced AI' – 5.



(a)

Legend

Object	Description
1	Non-State Actors:70,42,28
2	Political Governance:54,60,-6
3	Mixed Reality:40,40,0
4	Hypermedia:42,55,-13
5	Advanced AI:43,33,10
6	CDI:35,57,-22
7	Social Dynamics:65,55,10
8	Economic Changes:60,67,-7

(b)

Figure 2: System model for future hybrid threats exploration (a) and resulting analysis 3D classification (b) in I-SCIP-SA, v.2.0 environment

Generally the obtained initial classification is giving priority to social factors importance versus the technological ones. However, it should be clearly noted that these model entities classifications are just introductory and static ones. So, for achieving comprehensiveness they have to be studied further and in the dynamic context, giving the presented system model a real forecasting value.

4. MACHINE VALIDATION

Concerning the validation necessities of the system analysis results both time series dynamics implementation [7] and stochastic modelling [8] are applicable.

The idea for system analysis studying, based on discrete approximation is generally providing a suitable approach for multiple scenarios evolution [4]. In this sense several good examples from the digital space, encompassing environment of living and sensors integration could be given [9], [10].

One of the major problems in this sense that have to be noted is connected to different speeds of dynamics that the real world entities (system variables) are generically interacting. This in fact is of significant importance in complex social systems proper modelling and thus for the new cyber-physical mixed reality exploration. A useful solution in this sense was proposed by Vester, using time delays [11].

Another more complex problem is the system stability that is difficult to be directly assessed and forecast without algebraic model representation. Furthermore, the problem with system reliable control in non-stationary (chaotic) mode stays open.

As far as real system models are usually both non-linear and non-stationary ones, a stochastic approach based on probability trends distribution expert assumption and further risk assessment, about system entities connectivity is presented.

The idea behind is using Beta distributions that are a priori defined over model entities interconnectivities. This approach provides enough flexibility to easily implement prognosis of different shapes, similar to other popular social dynamics descriptions [12], modifying just *alpha* and *beta* parameters [13] of the curves families.

A follow-up a posteriori probability assessment of entities interrelations' risk is calculated implementing the stochastic approach with suitable parametric models [8].

An illustration example of practical machine validation in Matlab R2011b environment for 'Hypermedia' interrelations probabilistic risk assessment from the model of Figure 2a is given in Figure 3.

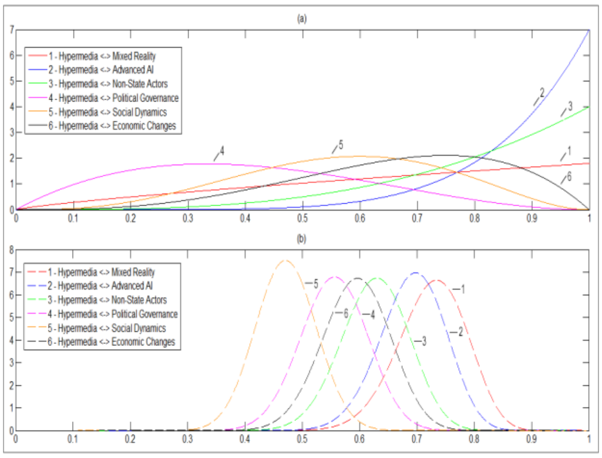


Figure 3: Probabilistic validation for 'Hypermedia' *a priori* (a) and *a posteriori* (b) trends in future hybrid threats study model (see Figure 2a)

What should be drawn as a conclusion of the proposed validation approach, based on stochastic simulation over the possible trends progress, are some difficulties for holistic system evolutionary assessment.

Concerning the expert based E-R model input this problem could be further translated into a multidimensional exploration space.

Following the system holistic nature principal assumption, this provides an opportunity for generalized measuring of the proposed E-R model system nature, using trends forecasting approach, similar to [7] but normally with some limitations that could be bypassed, following the proposed probabilities distributions implementation [8].

Finally, a practical mixed reality observation is added as a verification mechanism, providing an active role for the human factor future uncertain influence coping.

5. RESULTS VERIFICATION

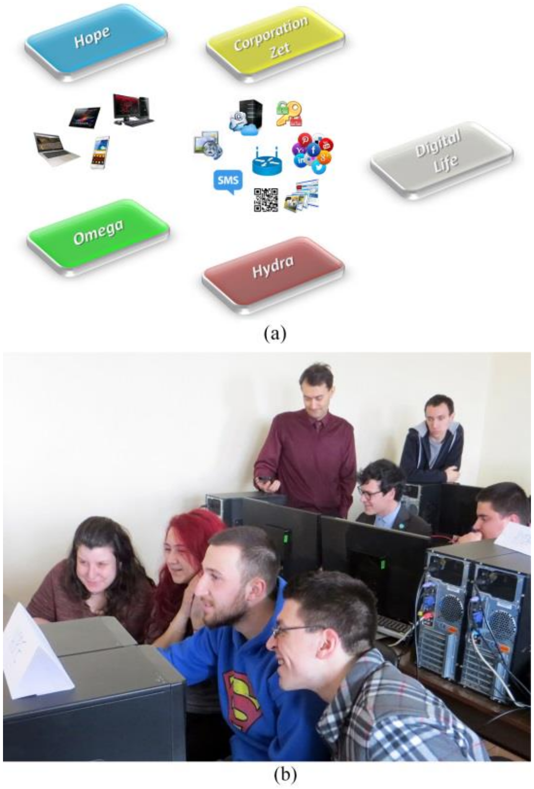
The presented idea is attempting to extend the overall described concept for hybrid threats adequate coping in the new digital reality. The results verification is mainly giving a possibility for better prognosis exploration in a semi-real environment. The assumed practical implementation in this paper is using a mixed cyber-physical reality (real, virtual & augmented ones combination) for interactive simulation with human-in-the-loop extension.

Different fictitious exercise scenarios are tested within this idea, using expected and unexpected event- driven exercise scripts and measuring, at the same time, trainees' group selected psycho-physiological responses [14]. This practically provides an opportunity for future environments reliable exploration with the active role of the human factor.

In general the concept is based on broader security problems exploration solid approach via Computer Assisted eXercises [15], [16] including the cyber space [5], [17].

Here it should be noted that more simplified approaches like: table-top exercises or other multirole high-level games are also applicable in support of the presented solution. They however lack the technological part and could be used only as preparatory ones.

The main idea, encompassed in the present CAX based approach, was taken alive during the international Cyber Research Exercise – CYREX 2016, organized by Joint Training Simulation & Analysis Center at Plovdiv University 'Paisii Hilendarski' [18].



(a)

(b)

Figure 4: Organizational architecture (a) and selected moments (b) of international exercise CYREX 2016

The trainees were organized in Facebook closed group environment, connected with a mixed reality cyber-physical polygon (encompassing: tablets, phablets, smartphones, i-pods, ultrabooks, laptops and desktop machines) interconnected via LAN (both cable and wireless) from a private router (used also for easy event log recording).

Additional ad-hoc configured e-mail server accounts, SMS notifications and avatar Zoobe based messaging were implemented, together with Skype, Viber & Dropbox services.

DDoS selected participants IP attacks, encryption of messages, malware sources, augmented QR codes realities extensions with hidden information were also used for complex social engineering simulation motivated with hacktivism and industrial espionage ideas.

The participants (30 students, 20 years +/- 2, including 8 observers from academia, industry and abroad from both Republic of Macedonia & IFIP scientific community) were practically organized for approximately three hours in five teams (see Fig. 4) as follows: 1 – 'Motivators' – 'White' (a non-governmental organization 'Digital Life', trying to regulate the new digital society), 2 – 'Hacktivists' – 'Green' (non-formal hackers group 'Omega', fighting for justice in the digital space), 3 – 'Insiders' – 'Blue' (a start-up company 'Hope' established by 'Omega' for corporate espionage), 4 – 'Investigators' – 'Red' (a multinational cybercrime investigation and control organization 'Hydra') and 5 – 'Corporates' – 'Yellow' (a multinational 'Corporation Zet' suspected in terrorism funding and criminal connections).

The response times and impressions of all five teams were gathered individually (using router logs and self-reporting digital questionnaires) during and after the exercise.

Several important facts and hypothesis were found and proved from CYREX 2016 successful conduction, regarding the future hybrid threats successful exploration:

– A practical discovery of hypermedia important place in modern cyber-physical reality;

– The progressing share of Critical Digital Infrastructure was also confirmed, facing multiple smart devices and web services for advanced communication in the near future;

– Dual social dynamics and non-state actors' significant roles, concerning criminal activities, terrorism & hacktivism, for the new challenges of the Advanced Persistent Threats (like: social engineering & espionage, see e.g. [19]) proper meeting.

5. DISCUSSION

The fast technological progress in the digital era is generating new, unstudied hybrid threats from both technological and human perspectives. This creates unforeseen possibilities for influencing human behaviour and emotions via the digital component that have to be expected in the next years.

The presented methodological approach clearly refers to the indisputable necessity for comprehensive coping of the problem in the new and fast evolving cyber-physical mixed reality.

Furthermore the described ideas could be extended from both validation & verification perspectives, implementing micro sensors data (from participants and environment) and more detailed cyberattacks models, including distributed computational powers and big data on-line analysis.

This will provide an opportunity for using the digital environment both as a source and consumer of data, giving a possibility of better understanding the technological evolution in the new digital century.

6. ACKNOWLEDGEMENTS

The authors give special appreciations for the expert & experimental support to: Association of Communication & Information Specialists – Bulgaria, Plovdiv University 'Paisii Hilendarski', Cyber Forum 2016 DESSERT B2S – S2B and CYREX 2016 sponsors and collaborators.

REFERENCES

[1] L. Floridi, "The Fourth Revolution (How the Infosphere is Reshaping Human Reality)", 1st ed., Oxford University Press, 2014.

[2] N. Choudhury, "World Wide Web and Its Journey from Web 1.0 to Web 4.0", Int. Journal of Computer Science and Information Technologies, vol. 5 (6), pp. 8096–8100, Nov-Dec. 2014.

[3] K. Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond", World Economic Forum, Jan. 2016, Available at: https://goo.gl/e1Kc3F

[4] Z. Minchev, "Human Factor Role for Cyber Threats Resilience", in Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, 1st ed., M. Hadji-Janev & M. Bogdanoski, Eds. IGI Global, 2015, pp. 377–402.

[5] Z. Minchev, "Cyber Threats Identification in the Evolving Digital Reality", in Proc. of Ninth National Conference "Education and Research in the Information Society", Plovdiv, Bulgaria, May 26-27, 2016, pp. 011–022.

[6] Z. Minchev, "Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems", in Proc. of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev, IMI-BAS, Sofia, Bulgaria, 2016, pp. 102–110.

[7] Z. Minchev, & V. Shalamanov, "Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach", in Proc. of SAS-081 Symposium on Analytical Support to Defence Transformation, RTO-MP-SAS-081, Sofia, NATO RTO ST Organization, 2010, pp. 22–1 – 22–16.

[8] Z. Minchev, G. Dukov, et al, "Cyber Intelligence Decision Support in the Era of Big Data", in ESGI 113 Problems & Final Reports Book, 1st ed., Sofia: FASTUMPRINT, 2015, pp. 85–92.

[9] Z. Minchev, & L. Boyanov, “Smart Homes Cyberthreats Identification Based on Interactive Training”. in Proc. of ICAICTSEE – 2013, 2014, pp. 72–82.

[10] Z. Minchev, & L. Boyanov, “Augmented Reality and Cyber Challenges Exploration”, Nauchni Izvestia, issue 9 (195), 2016, pp. 28–30.

[11] F. Vester, “The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity”, München: MCB–Verlag, 2007.

[12] C. Sergio, S. Bertuglia, & F. Vaio, “Nonlinearity, Chaos & Complexity (The Dynamics of Natural and Social Systems) ”, Oxford University Press, 2005.

[13] A. Gupta, & S. Nadarajah, “Handbook of Beta Distribution and Its Applications”, 1st ed., New York: CRC Press, 2004.

[14] Z. Minchev, “Multiple Human Biometrics Fusion in Support of Cyberthreats Identification”, Int. Journal Cyberetics & Information Technologies, vol. 15 (7), pp. 67–76, Dec. 2015.

[15] V. Shalamanov, T. Tagarev, Z. Minchev, et al, “Security Research and Change Management in the Security Sector”, 1st ed., G. C. Marshall Association – Bulgaria, Sofia: Demetra Publishing House, 2008. (in Bulgarian)

[16] E. Cayirci, D. Marincic, “Computer Assisted Exercises and Training: A Reference Guide”, 1st ed., Wiley-Blackwell, 2009.

[17] L. Kick, “Cyber Exercise Playbook”, The MITRE Corporation, 2014, https://goo.gl/SOkkw6

[18] CYREX 2016 Facebook News Post, February 26, 2016, https://goo.gl/Pa8ArN

[19] T. Wrightson, “Advanced Persistent Threat Hacking”, 1st ed., McGraw-Hill Education, 2015.