МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2017
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2017
Proceedings of the Forty-sixth Spring Conference
of the Union of Bulgarian Mathematicians
Borovets, April 9–13, 2017

HYBRID THREATS IDENTIFICATION IN THE NEW TRANSFORMED REALITY*

Zlatogor Minchev

An ad hoc study approach on securing transformed reality is presented as an innovative field of research in the digital era. Initially, a multiple attack scenarios are defined via hybrid threats landscape matrix establishment, using expert beliefs and structural analysis. Results are further explored, using complex discrete systems modelling and holistic assessment, providing a better understanding of hybrid threats nature. A machine simulation is finally used for possible probabilistic validation. The conclusion at the end gives concerns about the outlined research progressive development towards advanced handling of the new digital challenges.

I. Introduction. A proper understanding of the 4^{th} digital revolution is a rather ambitious task, concerning innovative technologies integration in the cognitive reality of social well-being maximizing. Numerous interpretations of the new digital lifestyle evolution, encompassing activities of living, working and entertaining could be provided [1]. The overlaid establishment of this social digitalization is presently combining 'virtual', 'augmented' and 'mixed' environments [2]. Some short notes on this realities mixture will be further given for better 'transformed reality' concept explanation.

Generally, the 'virtual reality' is a computer generated, interactive environment, artificial simulation with human-in-the-loop immersive presence, mainly addressing training and entertainment activities.

The next 'augmented reality' progressive step is the real physical world sensor-machine live mediated augmentation with numerous everyday life utility applications.

The overlaid merging of virtual, augmented and physical environments is finally producing a live, flexible combination of different systems (biological, physical, virtual) interactive co-existence, blended in a new 'mixed reality'.

These assumptions are however observable at the epoch of Web 3.0 era only via supportive mobile smart gadgets (googles, helmets, suits, phones, tablets, bracelets, etc.) and require ad-hoc created software applications with no holistic implementation but targeting only specific ones (e.g. navigation, entertainment, shopping, etc.).

The 'transformed reality' concept, though quite disputable for altering users' perceptions [3], could be rather influential in the upcoming Web 4.0, especially due to 'Internet-of-Things' (IoT) fast development, miniaturization and intelligence embodiment towards changing the biological systems way of living.

* **2010 Mathematics Subject Classification:** 65C20, 68T30, 97P70.
Key words: transformed reality, securing digital future, threats analysis, probabilistic validation.

As every innovative idea it will inevitably produce new opportunities and plenty of uncertainty shifts (cultural, ethical, technical, etc.). Special focus is expected to be given to normal presence and acceptance in the human bodies of high-end bioimplants and wearable skin-like flexible biosensor patches [4].

At the moment these technological solutions are mainly oriented to some chronic diseases experimental coping (e.g. diabetes, cardiac insufficiency, Parkinson, etc.), military applications and science fiction movies.

Thus the 'transformed reality' valuable extensions towards 21st century quality of life changes with numerous agile digital services and opportunities are just a question of near future progressive evolution.

What however stays uncertain in this new reality is the sustainable changes of the digital citizens' behavior, feelings and opportunities address to their new, transformed digital lifestyle [5].

The biggest uncertainty here is the embedded artificial intelligence evolution, expected in Web 4.0 that will definitely transform the new digital society values, understandings and objectives.

Handling these problematic issues is a rather arguable and quite fascinating area that has to be adequately oriented also toward the security of human beings, environment and technologies. In this sense it is important to note the potential threats from hybridization, originating from multidimensional clashes, related to human-machine interaction phenomena like: joint embodiment, multiple cooperation, successful co-existence and societal acceptance.

The paper will briefly outline how to secure the near-future-transformed reality by implementing a trilateral study approach as follows: (i) Establishment of hybrid threats analytical landscape; (ii) Detailed exploration of the identified threats through system analysis; (iii) Final probabilistic validation of the obtained results as a foreseeing address towards future transformed reality advanced understanding.

II. Establishment of Hybrid Threats Analytical Landscape. Initial prognostic exploration of hybrid threats landscape (with five years horizon up to year 2021) was produced using some BISEC 2016 [6] data from academia & industry with more than 500 sources from 14 countries [7]. Further data enrichment was organized during the discussions of IFIP ICAICTSEE 2016 [8] conference with international communities' feedbacks from Asia, Europe and North America with 7 more countries. Final results processing was performed via structural (morphological) analysis and I-SCIP-MA environment. The approach is a well-known successor for unstructured and partially uncertain data processing and is based on multidimensional mutually exclusive alternatives aggregation in a cross-consistency multiple scenario matrix space representation. Both positive and negative scenarios are implemented, following an expert cumulative alternatives' interrelations assessment, based on Relative Common Weight – RCW [9].

In the present study 5 dimensions ('Digital Services', 'Human-Machine Interfacing', 'Hybrid Threats', 'Tech Challenges', 'Social Issues') with different alternatives number (between 3 and 5) were used. The total cross-consistency scenario matrix (see Figure 1) combinations number is calculated as: $N = 5 \times 5 \times 3 \times 4 \times 4 \times 3$, $N = 3600$. Using expert support, 93 of them were selected as follows: 58 active (RCW > 0), 7 neutral (RCW $= 0$) and 21 passive (RCW < 0) scenarios.

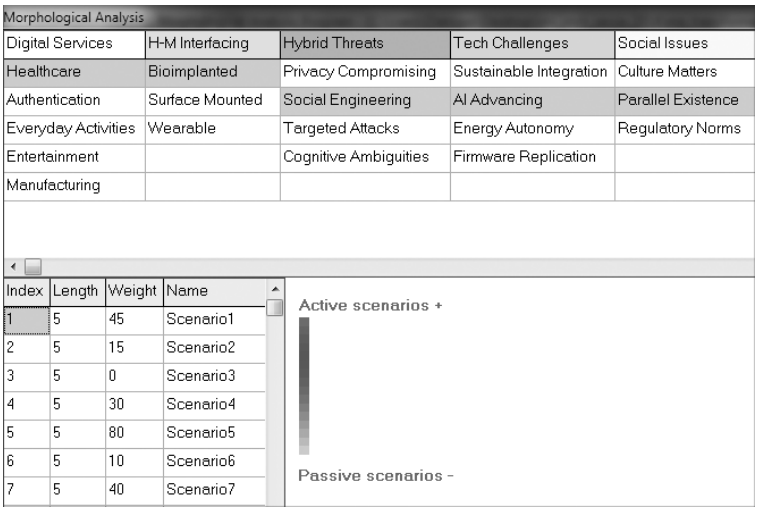

Fig. 1. A screen-shot of the cross-consistency scenario matrix for transformed reality hybrid threats analytical landscape establishment in I-SCIP-MA environment

The summarized results from the morphological analysis of the threat landscape are defining tangible, i.e. active scenario expectations towards hybrid threats like: 'Targeted Attacks' and 'Cognitive Ambiguities', originating, technologically from: 'AI Advancing' & 'Firmware Replication', that are socially influenced by: 'Parallel Existence' and 'Regulatory Norms. The considerations are encompassing: 'Healthcare', 'Manufacturing' and 'Entertainment' digital services through 'Bioimplanted' and 'Wearable' H-M interface.

At the same time, unexpected, hidden threats have to be studied with care for their intangibility via social issues like: 'Cultural Matters' and 'Parallel Existence' with technological challenges of: 'Energy Autonomy' and 'Sustainable Integration'. These are expected to influence future digital users with: 'Social Engineering' and 'Privacy Compromising', using 'Wearable' and 'Surface Mounted' H-M interface towards services like: 'Everyday Activities', 'Authentication' and 'Entertainment'.

Being somewhat overlaid and ambiguous, by means of threats hybrid origins roots, the established landscape is further studied in detail, implementing detailed system analysis exploration.

III. Threats System Analysis Exploration. The idea of this paragraph is to create a system model of future transformed reality that will support the identification of hybrid threats sources, implementing both social and technological aspects and assessing their sensitivity from a holistic perspective on the basis of previous paragraph data. The working hypothesis is following Vester's interpretation of complex discrete dynamic systems [10], practically incorporated with I-SCIP-SA environment. This solution has numerous proven successful stories during the last 10 years with different problem areas, mainly from the security field [11].

The model is presented in Figure 2a using an Entity-Relationship causality paradigm over a weighted graph with 10 nodes and 22 dual arcs. Entities are presented as labeled round rectangles, while relations are uni- or bi-directional headed arrows (noting *Influ-*

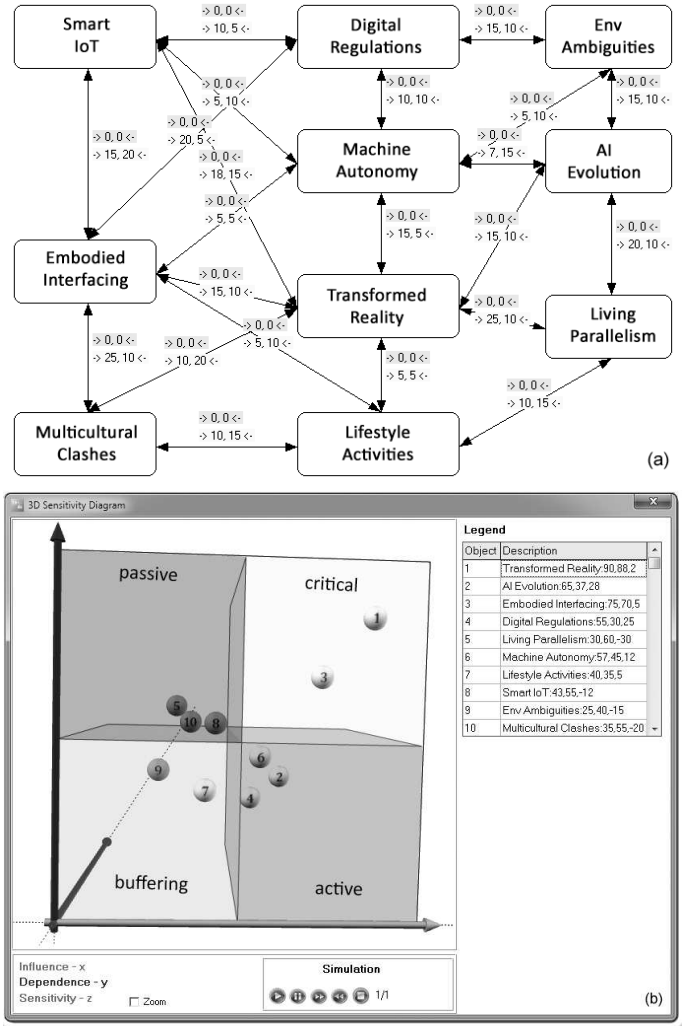

Fig. 2. System model for future transformed reality exploration (a) and resulting 3D Sensitivity Diagram (b) in I-SCIP-SA environment

ence – forward x relation and *Dependence* – backward y relation). *Sensitivity* – z is also calculated via *Influence*/*Dependence* ratio, noting both active (positive, white) and passive (negative, light grey) indexed entities.

Model relations are weighted either with singular or multiple array values, marked with two separate labels for their number – M (the upper ones, marked with small inscribed dark grey rectangles, $M = 0$ for the present model, having static representation that is concerning present moment understandings for the studied problem at hand) and weight – W (the bottom ones, marked with light grey, W is measured in percentages from the interval [0, 1]).

Resulting entities classification is visualized after *Influence*, *Dependence* and *Sensitivity* parameters values in a cubic 3D Sensitivity Diagram (see Figure 2b), incorporating four sectors: *active*, *passive*, *critical* and *buffering*.

The presented model entities are outlining the following allocations: *active*: 'AI Evolution' – 2, 'Digital Regulations' – 4, 'Machine Autonomy' – 6; *passive*: 'Living Parallelism' – 5, 'Smart IoT' – 8, 'Multicultural Clashes' – 10; *critical*: 'Transformed Reality' – 1, 'Embodied Interfacing' – 3; *buffering*: 'Lifestyle Activities' – 7, 'Env Ambiguities' – 9.

The obtained results from the system analysis are raising generalized attention towards smart IoT gadgets as a hybrid threats generator with multiple environment ambiguities. These are actively influenced by machine multiaspect autonomy evolution and producing, at the same time, real world living parallelism social phenomenon for the new multicultural transformed reality.

Suitable regulations are also expected to be developed, concerning the increased IoT gadgets users' embodiment due to the future transformation of present digital lifestyle with numerous new, convenient and addictive activities and services.

This analysis outlined a rather comprehensive transformed reality understanding due to the system modelling holistic nature.

The next section, will describe a prognostic validation of these analytical findings, using a probabilistic approach and trying to create a dynamic outlook towards the future transformed reality threats identification.

IV. Probabilistic validation. A concluding moment of the presented transformed reality hybrid threats identification is the machine probabilistic validation of the obtained analytical results. This creates a foreseeing address towards future advanced understanding.

The solution presented here incorporates a probabilistic a priori Beta distribution that is assumed to mirror selected trends progressive beliefs from an expert based system model graph interpretation, taking into considerations the Forester's social dynamics growths (both positive and negative) assumptions [12] towards equilibrium or chaos [13].

Further on, using machine random generation and assuming deterministic problem nature the a priori distribution parameters are modified (using Monte-Carlo methods or other similar ones) for obtaining a posteriori future evolution results with a reasonable simulation time frame, concerning possible hybrid attacks simulation, similar to [14].

An experimental validation, using Matlab R2011b and the 'Transformed Reality' entity interconnected relations trends (see Figure 2a) are presented in Figure 3. The aggregated results from the validation process are giving future priorities up to year 2021 (with $P > 0{,}6$) to: 'Embodied Interfacing' – 1, 'Smart IoT' – 3, 'AI Evolution' – 6, 'Machine Autonomy' – 4, 'Multicultural Clashes' – 2. 'Living Parallelism' – 7 and 'Lifestyle Activities' – 5 being also important are not expected to be on a reasonable level of progressive development for establishing significant influence towards transformed reality users' present lifestyle.

Conclusion. Todays' digital revolution is establishing a new transformed reality, combining ICT-, physical- and bio- systems. This new environment has already started a fast progressive development, due to Internet-of-Things booming and will luckily blossom in the Web 4.0 epoch of the autonomous Artificial Intelligence. It also inevitably generates numerous hybrid threats that are difficult to be identified and coped at the

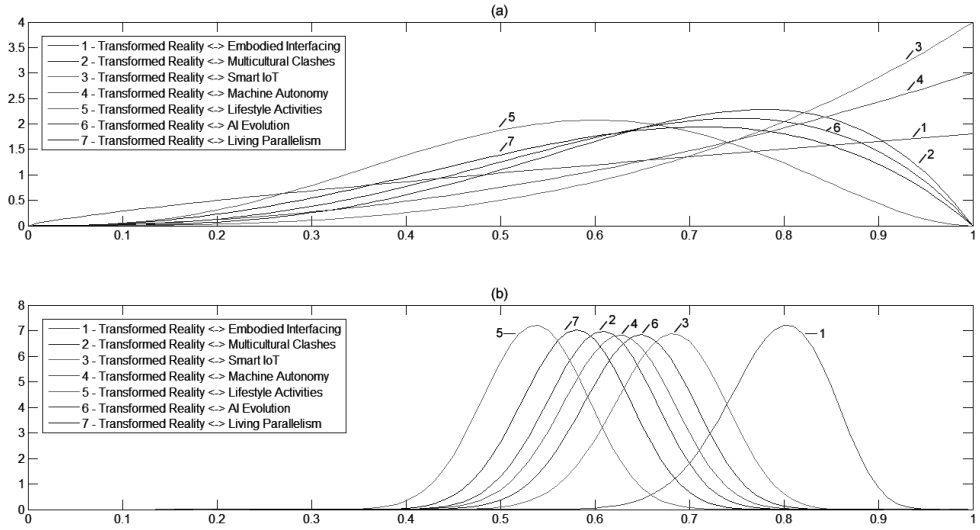

Fig. 3. Matlab R2011b validation screenshots for 'Transformed Reality' a priori (a) and a posteriori (b) hybrid threats sources probabilistic evolution, following the model of Figure 2a

moment, being rather innovative by nature.

An ad hoc digital future securing approach, encompassing expert data processing with structural and system analysis is outlined in the paper. Results are finally validated with machine probabilistic simulation. Though reasonable the proposed ideas for future foreseeing also require a suitable verification. A useful support in this context could be achieved with constructive exercise simulations that allow multiaspect evaluation of interactive human-machine responses in a *polygon-like world*. Hopefully, this will produce a consolidated research advancing towards better understanding of the new digital objectives.

REFERENCES

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

[2] L. Chan. Mixed Reality vs Virtual Reality vs Augmented Reality: What's The Difference?, Tech Times, December 18, 2016, Available at: `https://goo.gl/Qa8hUp`.

[3] Y. Kubota, T. Tezuka. Transformed Reality – Altering Human Perceptions by Computation, Proceedings of International Conference on Culture and Computing, Kyoto, Japan, September 16–18, 2013, 39–44.

[4] A. Williams, D. Nield. Where Phone Meets Body: How People are Making Themselves into Machines, Techradar, April 15, 2016, Available at: `https://goo.gl/HPBSwl`.

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

[6] BISEC 2016 Conference Web Page, `http://bisec.metropolitan.ac.rs/`.

[7] Z. Minchev, G. Dukov. Emerging Hybrid Threats Modelling & Exploration in the New Mixed Cyber-Physical Reality, Proceedings of BISEC 2016, Belgrade Metropolitan University, October 15, 2016, 13–17.
[8] ICAICTSEE 2016 Conference Web Page: http://icaictsee.unwe.bg/.
[9] Z. Minchev, L. Boyanov, S. Georgiev. Security of Future Smart Homes. Cyber-Physical Threats Identification Perspectives, In Proceedings of National Conference with International Participation in Realization of EU HOME/2010/CIPS/AG/019 project, Sofia, Bulgaria, June 4, 2013, 165–169.
[10] F. Vester. The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity, München, MCB–Verlag, 2007.
[11] Z. Minchev. Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems, In Proceedings of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev, IMI-BAS, Sofia, Bulgaria, 2016, 102–110.
[12] J. Forrester. World Dynamics, Cambridge, Massachusetts, Wright-Allen Press, 1971
[13] S. Panchev. The Theory of Chaos (With Examples & Applications), Academic Publishing House 'Prof. Marin Drinov', 2001 (in Bulgarian).
[14] Z. Minchev, G. Dukov, D. Boyadzhiev et al. Cyber Intelligence Decision Support in the Era of Big Data, in ESGI 113 Problems & Final Reports Book, 1st ed. Sofia, FASTUMPRINT, 2015, 85–92

Zlatogor Minchev
Institute of ICT/Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev St, bl. 25A
1113 Sofia, Bulgaria
e-mail: zlatogor@bas.bg

ИДЕНТИФИЦИРАНЕ НА ХИБРИДНИ ЗАПЛАХИ В НОВАТА ТРАНСФОРМИРАНА РЕАЛНОСТ

Златогор Минчев

Представено е специализирано решение за гарантиране на сигурността в трансформираната реалност като иновативно поле на изследване от новата дигитална ера. Посредством установяване на пейзаж на хибридните заплахи и използване на структурен анализ върху експертни вярвания първоначално се дефинира множество от сценарии за възможни атаки. За по-доброто разбиране на произхода на хибридните заплахи, по-нататък те са изследвани чрез системно моделиране на сложни дискретни системи с последващо холистично оценяване. Накрая е разгледана и възможност за вероятностно валидиране на резултатите с използване на машинна симулация. Нуждата от напредничаво разглеждане на новите дигитални предизвикателства в направеното изследване е отбелязана в заключение с някои идеи за бъдещо развитие.
Ключови думи: трансформирана реалност, гарантиране на сигурност в дигиталното бъдеще, анализ на заплахи, вероятностна валидация.