DIGITAL TRANSFORMATION DISRUPTIVE THREATS IDENTIFICATION

Assoc. Prof. Luben Boyanov PhD[1], Assoc. Prof. Zlatogor Minchev PhD[2]
University of National and World Economy, Sofia, Bulgaria [1]
Institute of Information and Communication Technologies, Bulgarian Academy of Sciences [2]

lboyanov@unwe.bg, zlatogor@bas.bg

Abstract: *Modern gadgets or IoTs miniaturization and embodiment into new technological users are inevitably producing numerous opportunities and disruptive threats towards digital transformation of their lifestyle, behaviour and understandings. The paper outlines a snapshot of user beliefs implemented in an analytical system model. The obtained results, matching with numerical stochastic simulations is further given in regards to potential disruptive threats proactive identification. Possible further verification is finally discussed.*

Keywords: DIGITAL TRANSFORMATION, DISRUPTIVE THREATS, SYSTEM ANALYSIS, STOCHASTIC VALIDATION, INTERACTIVE VERIFICATION

1. Introduction

The Fourth digital revolution is already a fact that is producing numerous opportunities. They are enormous, and so is the projected growth of Internet of Things (IoT) – the number of connected “things” is expected to be between 20 and 30 billion by the year 2021 [1], [2]. At the same time, together with the opportunities - new threats emerge [3]. In this context it is important to note the ubiquitous role of innovations for the societal development acceleration and establishment of new ‘ecosystem’ of living. This practically, generates a disruptive transformation to the social well-being and industry that from a technological view point is rather challenging [4].

Two important facts have to be noted here: speed and scale. With the new hardware and software technologies, interactive progress and IoT integration, during the next decade the surrounding digital world will become a mixture of living organisms and technology interacting on a new, unknown so far level. Here is important to note here the results for the societal dynamic transformation from human factor perspective in the digital age [5].

Further on, in the paper, a modelling approach for exploring these phenomena from a security perspective, together with possible results proactive validation are presented.

2. Exploration Approach

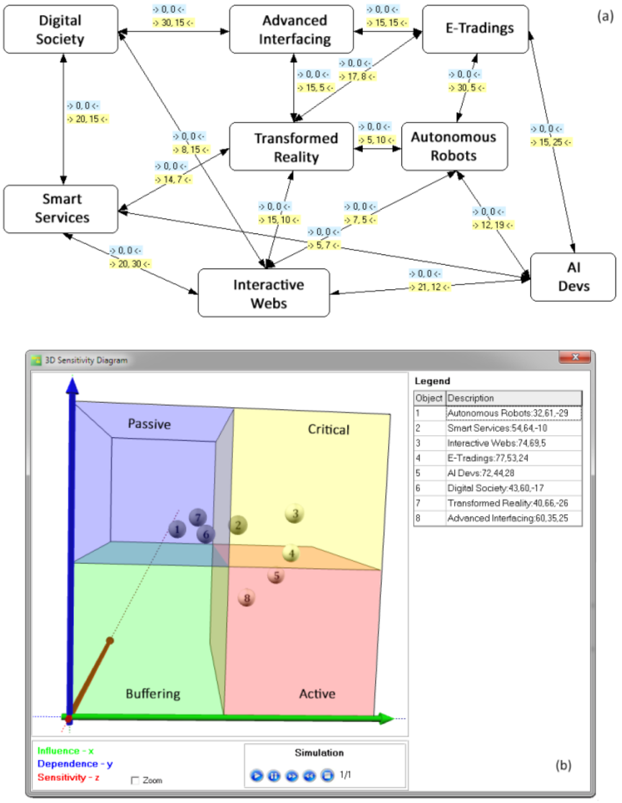
The main idea of the presented approach for exploring the societal dynamic transformations in the new digital age is to (i) proactively implement expert beliefs into a system model. Results are (ii) further validated for future expectations, using stochastic machine simulation. These ideas though rather flexible are lacking easy comprehensive accuracy criteria definition, concerning their futuristic address. In regard to the disruptive challenges proactive identification, a useful mechanism could be (iii) verification support via hybrid interactive simulation.

2.1. System Modelling

The idea for system modelling, using expert beliefs is generally implementing, with some data presented in [6], and is further aggregated in disruptive technologies sense, using the approach for model graphical and analytical representation built-in I-SCIP-SA software environment [7].

All model entities are marked with labeled round rectangles, interconnected bilaterally. Weight and time parameters are used for resulting entities classification (visualized as indexed balls) into a four-sector (green – ‘buffering’, red – ‘active’, blue – ‘passive’ and yellow – ‘critical’) 3D Sensitivity Diagram (SD), using: Influence (x), Dependence, (y). Additional, ‘active’ (white, positive z values) and ‘passive’ (grey, negative z values) reassessment for each of the entities in a certain sector, regarding Sensitivity (z) is also accomplished.

A practical modelling result of ‘Digital Society’, disruptive effect from ‘Advanced Interfacing’ , ‘E-Tradings’, ‘Autonomous Robots’, ‘Smart Services’, ‘AI Devs’ and ‘Interactive Webs’, concerning ‘Transformed Reality’ is given in Figure 1a.



Legend

Object	Description
1	Autonomous Robots:32,61,-29
2	Smart Services:54,64,-10
3	Interactive Webs:74,69,5
4	E-Tradings:77,53,24
5	AI Devs:72,44,28
6	Digital Society:43,60,-17
7	Transformed Reality:40,66,-26
8	Advanced Interfacing:60,35,25

Figure 1. *A system model for disruptive threats exploration in the new transformed digital reality (a) and the resulting sensitivity diagram (b).*

The resulting SD (see Figure 1b) is producing the following classification for model potential sources of disruptive threats: critical: ‘Smart Services’ – ‘2’, ‘Interactive Webs’ – ‘3’ and ‘E - Tradings’ – 4; active: ‘AI Devs’ – ‘5’ and ‘Advanced Interfacing’ – 8; passive: ‘Autonomous Robots’ – ‘1’, ‘Transformed Reality’ – ‘8’ and ‘Digital Society’. No buffering entities were used.

A further results probabilistic assessment is accomplished as the identified threats would be interesting for future dynamics trends evolution.

2.2. Probabilistic Assessment

Due to the subjective and static nature of results from section 2.1, the studied processes have to be considered and in the dynamic context. This practically, could be achieved, following the ideas from [8], implementing both expert beliefs and development trends as a priori landscape.

Additional further validation via agent-based simulation of possible hybrid attacks towards selected relations of a certain entity of interest is performed. This provides a posteriori simulated probabilities change by assessing hypothetical evolution scenarios.

Five trends have been considered (‘Smart Services’, ‘Digital Society’, ‘Transformed Reality’, ‘Autonomous Robots’, ‘AI Devs’), regarding ‘Interactive Webs’ from the presented in section 2.1. model.

A resulting simulation from Matlab R2011b environment, using Beta distribution with five-years’ time horizon is provided in graphical form on Figure 2.

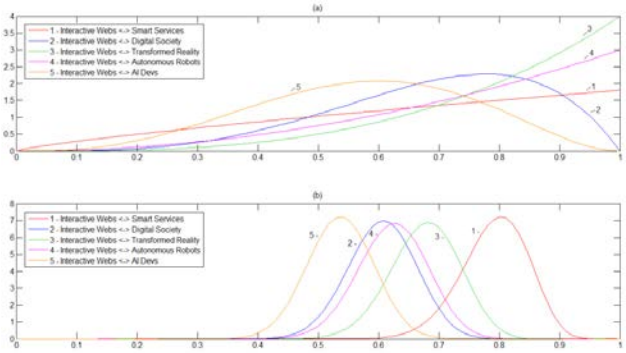


Figure 2. *A generalization of experts’ a priori (a) and simulated a posteriori (b) probabilities for hybrid attacks to ‘Interactive Webs’.*

According to the presented simulation results, ‘Smart Services’, ‘Transformed Reality’, ‘Autonomous Robots’ and ‘Digital Society’ (see Figure 2) are expected to be most probable (M > 0.5) for future hybrid attacks in the new, mixed and transformed digital reality environment, still giving uncertainty to ‘AI Devs’.

2.3. Results Verification

This final stage was organized, using an interactive hybrid simulation gamming approach, following the experience from [9]. The ideas were practically implemented into CYREX 2017 (see Figure 3), involving university, academic, NGO and industrial participants [10].

The main objective was to experimentally study the future of digitally transformed reality threats and challenges, using different smart gadgets, biomonitoring, popular social networks, cloud services, encryption and original training methodological framework.

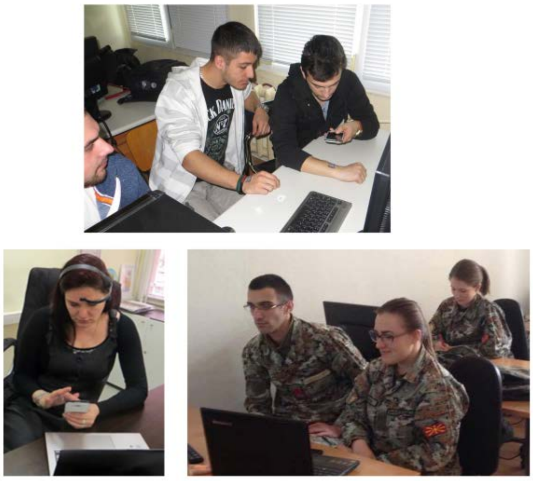


Figure 3. *Moments of CYREX 2017 verification event [10].*

Generally, the overall verification results have shown a significant interest from the participants’ side, regarding the improvised transformed reality, innovative gadgets and gaming exploration approaches. Additionally, though distributed by nature the CYREX 2017 was rather realistic, useful and intriguing according to the participants self-reporting.

4. Conclusion

The described exploration idea of digital world disruptive hybrid threats identification is producing a useful address toward future societal digital progress, encompassing both human and machines complex mixture in a new transformed reality. Being to some extent subjective the presented results are just outlining the near future plausible expectations, providing at the same time a reliable fundament for analysis and complex hybrid threats origins understandings. The further given validation and verification of the obtained results are finally establishing a valuable moment to the proposed initial system modelling ideas.

References

[1] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, November 2015, http://www.gartner.com/newsroom/id/3165317 [Online]

[2] Ericsson Mobility Report, On the pulse of the networked society, November 2015, https://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf [Online]

[3]. Floridi, L. The Fourth Revolution (How the Infosphere is Reshaping Human Reality), 1st ed., Oxford University Press, ISBN: 9780199606726, 2014. 272 p.

[4]. Bradley, J., Loucks, J., Macaulay, J., Noronha, A., Wade, M. Digital Vortex (How Digital Disruption Is Redefining Industries), Global Center for Digital Business Transformation, June, 2015, Available at: http://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf

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

[6]. Minchev, Z. Hybrid Threats Identification in the New Transformed Reality, In Proc. of 46 Spring Conference of UBM ‘Mathematics & Education in Mathematics’, Borovets, Bulgaria, pp. 194-200, 2017, Available at: http://www.math.bas.bg/smb/2017_PK/tom_2017/pdf/194-200.pdf

[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, IMI-BAS, Sofia, Bulgaria, pp. 102 - 110, 2016

[8]. Minchev, Z., Boyanov, L. Predictive Identification Approach for Emerging IoT Hybrid Threats, In Proc. of ICAICTSEE – 2016, Sofia, UNWE, December 2-3, 2016 (in press)

[9]. Minchev, Z. 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, pp. 011 - 022, 2016

[10]. Cyber Research Exercise – CYREX 2017 Web Page, https://goo.gl/sBvVWW