ANALYTICAL CHALLENGES TO MODERN DIGITAL TRANSFORMATION

Zlatogor Minchev

Institute of ICT/Institute of Mathematics & Informatics
Bulgarian Academy of Sciences
zlatogor@bas.bg

Abstract: *Todays' digital world is inevitably changing our style and ecosystem of living, transforming human factor understandings, feelings and behaviour. These findings however are difficult to be identified for both tangible and intangible challenges that needs a suitable analytical approach. The paper outlines a practical framework for modern ICT technologies and services study implementation for better understanding of digital future objectives in nowadays Fourth Digital Revolution era. A suitable analytical framework is presented for both static and dynamic risks & challenges landscape system coping. Results trends are further validated, using both expert beliefs and probabilistic machine simulation. Finally, a practical verification is outlined via interactive gaming exercise.*

Keywords: *digital transformation, tangibles & intangibles analysis, framework implementation*

1.Introduction

The new, Fourth Digital Revolution is naturally producing changes in present and future world [1]. Being at the transition of industrial to information age change, this creates a new, challenging ecosystem [2] of fast evolving people and technologies coexistence. At the same time, the new comprehensive change also generates numerous tangible and intangible issues from both technological and social origins.

In todays' Web 2.0 social networks connected world, the near future is expected to be given to "Internet of Everything" Web 3.0 concept that will shape the new digital people's everyday lifestyle in a rather frightening way of Web 4.0 technologies super embodiment [3].

The biggest unknowns so far are 'How' and 'Why' to keep the human factor advantages in this fast progressing smart environment, or in other words - assure [illegible]nected smart ecosystem of the digital future.

In this context, whilst technologies are exponentially advancing towards autonomy (from multiple viewpoints: energy, existence, intellect, etc.), speed and scale of the upcoming quantum computing, the human factor and other living creatures abilities for reasonable adaption are becoming quite limited [4].

Nowadays Y-generation (following X-, Y- & Z- generations theory, initially marked for USA [5]) influence feedbacks are reckoning to phenomena like: informational overload, attention deficit, digital dementia, digital fatigue, hostility, alienation, overexcitement, parallel existence, etc.

Here it should be noted one of the greatest unknowns of the future social resilience establishment, addressed towards the growing up Z-generation, but: successful digital adaptation in this highly sophisticated smart ecosystem of living, keeping at the same time human rational traits and necessities of: privacy, emotions, cognition, creativity, innovativeness in a highly connected and rather rushed digitally transformed reality [1].

The modern technologies artificial perfections are still creating only a mimic of the living organisms' behaviour and intelligence that is not operational at the level of being completely autonomous.

Not quite near future prognosis of 2050 [6], [7] demands more specific address to the upcoming transformed world of technological multiple obsessions towards living creatures, that is expected to produce a new, highly interactive and integrated heterogeneous mix of digital and living matter.

Further on, an analytical framework for progressive exploration of this phenomena with practical implementations will be outlined.

2. Analytical Framework

The idea behind the presented threefold framework (see Fig. 1) benefits from more comprehensive solutions like [8], [9]. The different context here however is noted from the dynamic perspective that in practice provides an opportunity for better exploration of future dynamics in the new, transforming digital world.

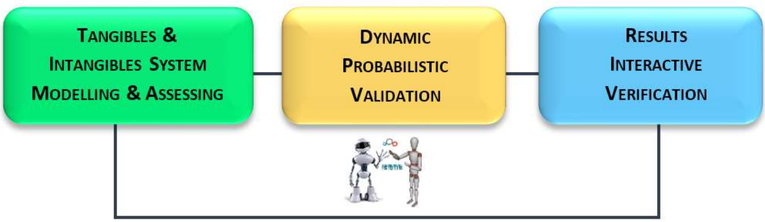

Fig. 1. An analytical framework for dynamic exploration of new digital transformation.

The framework is encompassing: (i) *Tangibles & Intangibles System Modelling & Assessment* that gives an expert opportunity for holistic future assessment, implementing a system based dynamic modelling approach for risk assessment. Further on, the obtained results are validated during (ii) *Dynamic Probabilistic Validation*, using trends forecasts, expert beliefs and machine simulations. Finally, some (iii) *Results Interactive Verification* is added to achieve comprehensiveness of the presented ideas, providing interactive assessment in the transformed digital reality with active human factor role.

A more detailed description will be given next in the paper for the briefly outlined framework three analytical stages.

2.1. Tangibles & Intangibles System Modelling & Assessing

The presented tangible and intangible system modelling & initial assessment were performed, using some preliminary assumptions and user expectations.

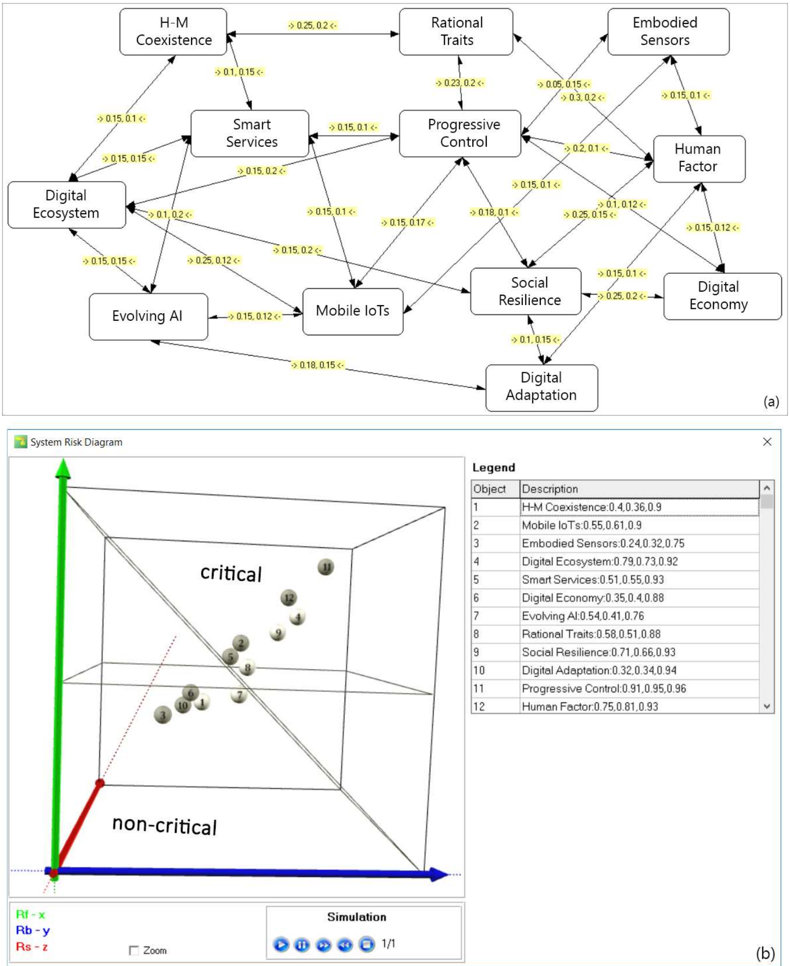

Fig. 2. Digital future tangibles and intangibles system risks modelling (a) and resulting *Rs* classification SR Diagram (b) in I-SCIP-RA environment [12].

The data was gathered during "Security foundations in Cyber Space" training course [10] and enriched from IFIP TC13-TC14 open symposium discussions [11]) that were further aggregated in I-SCIP-RA environment [12].

The modelling approach is implementing a system holistic 'Entity-Relationship' causality concept over a weighted graph. All entities (graphs nodes) are marked with labelled round rectangles, and relations (arcs) with dual headed arrows, signed with probabilistic weights values. A resulting 3D System Risk Diagram (SR Diagram) is produced, identifying both 'critical' and 'non-critical' entities clusters (marked with indexed balls, spread around north-west/south-east main diagonal). Additional 'active' or 'passive' subclusters are assumed with white or grey colours for the model entities. The classifications are based on aggregated system risk – *Rs* (*z* - axis), resulting from: forward – *Rf* (*x* - axis) and backward – *Rb* (*y* - axis) risk values combination, following [12].

The current model SR Diagram classification is obtained from a priori expectations for the 2021 digital future, concerning non-critical (tangible) but *active* entities: 'Human-Machine Coexistence' – 1, 'Evolving AI' -7 and *passive* ones: 'Embodied Sensors' – 3, 'Digital Economy' – 6, 'Digital Adaptation' – 10. The rest model entities are expected to be assessed as critical, i.e. intangible for the near future but *active*: 'Digital Ecosystem' – 4, 'Rational Traits' – 8, 'Social Resilience' – 9 and *passive*: 'Mobile IoTs' – 2, 'Smart Services' – 5, 'Progressive Control' – 11, 'Human Factor' –12.

As far as normally, such classification inevitably generates multiple questions and claims for subjectiveness, some additional clarifications are also given:

- The probabilistic system risk assessment that provides tangible and intangibles conditional clustering is in a static context (simulation steps = 1), without taking into account possible unexpected but dynamic changes;
- The aggregated list of implemented model entities has been designed with the idea of possible extension and relations reassessment by means of *Rs* resulting values.

The dynamic probabilistic validation will be outlined from a holistic perspective in the next paragraph.

2.2. Dynamic Probabilistic Validation

As the presented tangibles & intangibles system identification mainly depends on expert knowledge and beliefs, the current approach is trying to provide more clarification of the extrapolation process from two perspectives: (i) evaluating the probability dynamics, using trend values forecasting from system perspective; (ii) implementing the results from stage (i) into a suitable probability distribution in order to position the forecasted expert value into future dynamics trend.

Being generally outlined, these ideas for dynamic validation will be further described in more details.

2.2.1. Evaluating probability dynamics from system perspective

The proper understanding of this approach requires an ergodic assumption of the studied system [13], that is used for non-linear forecasting, implementing a multidimensional simplex L, projected in time [14].

The main idea is to assess an average weighted value for a selected entity *K* risk probabilities (*Rf*, *Rb*, *Rs*), assumed to be a part of the simplex L of size *n*, following a system model interpretation in time *t* and multidimensional *n* distance norm *d* (e.g. Euclidean one or some of its generalizations). The resulting *K*' risk probabilities values (*Rf'*, *Rb'*, *Rs'*) of L' in the new *t'* time moment are the one of interest for further work considerations.

An aggregated example of 'H-M Coexistence' entity risk probability *Rs* (*H-M Coexistence*, *t*), forecasting from time *t* (year 2017) to *t'* (year 2021), using the related ones (see Fig. 2a): *Rs* (*Smart Services*, *t*), *Rs* (*Digital Ecosystem*, *t*) & *Rs* (*Rational Traits*, *t*) risk probabilities values from L and *Rs'* projections from L' is depicted in Fig. 3.

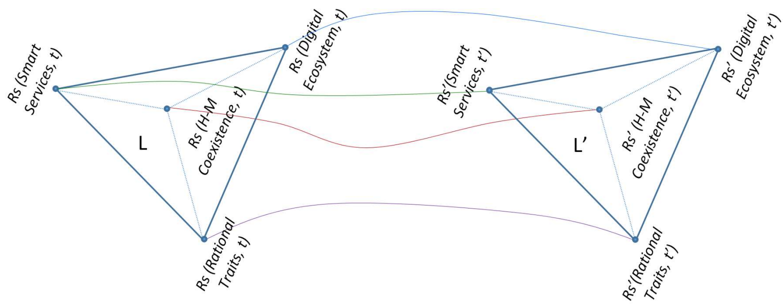

Fig. 3. An aggregated example of non-linear forecasting of a prori expert system risk *Rs* of 'H-M Coexistence', following the model relations from Fig. 2a up to *Rs'* for year 2021.

2.2.2. Combining the results with probability distribution

The idea is following the concepts from [15], implementing future expert beliefs, taking the general assumption of complex systems behaviour dynamics exploration, ranging from growth (both positive & negative) towards equilibrium or instability [16], [17].

In practice, the already marked risk system modelling classification of critical & non-critical risks assessment (see Fig. 2b) is used as system model behaviour objectives exploration area, combined with probability distribution change forecast.

The distribution shape parameters modification could have different nature but more interesting is the chance for possible results extrapolation, due to this change.

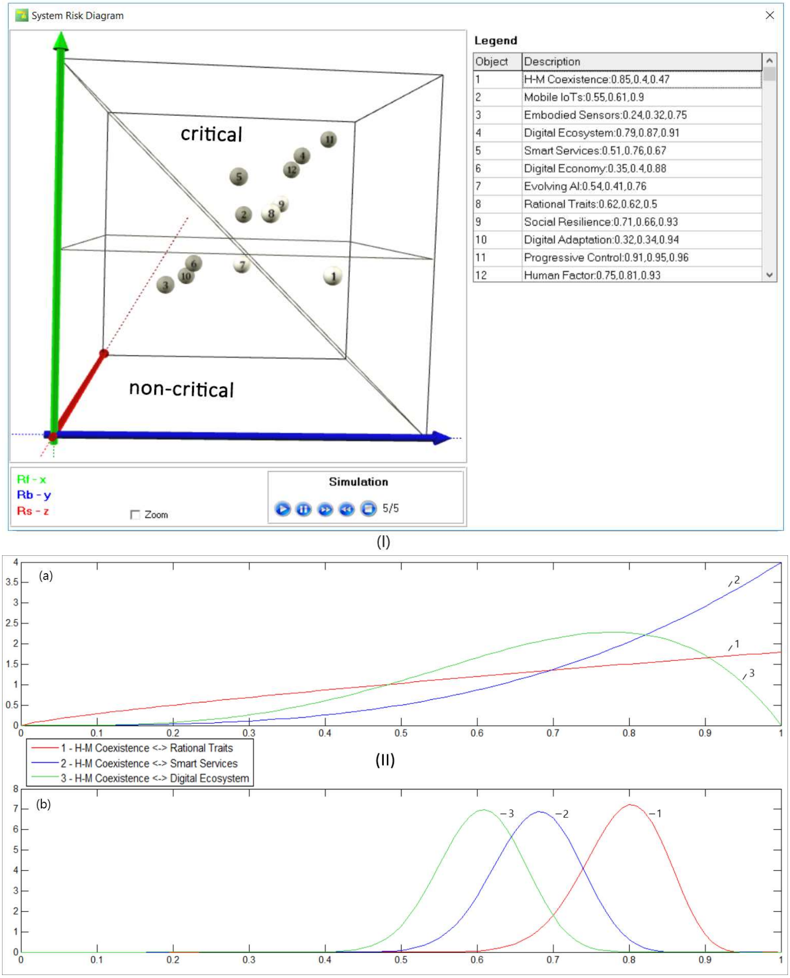

Fig. 4. A probabilistic validation, combining expert beliefs *Rs'* (I) and numerically simulated a priori (a) & a posteriori (b) probabilistic risks *Rs''* (II) for 'H-M Coexistence' up to year 2021.

In brief, the concept is trying to provide a dynamic forecast of a selected model entity a priori risk – *Rs* (resulting from both *Rf* and *Rb*, [12]), following the probability trend, defined over the other related entities from the model, using expert beliefs and machine simulation for the resulting weighted system risk *Rs** (*Rs** = *a*.*Rs' x b*.*Rs''*, *Rs"* – risk correction, after desired expert risk prognosis *Rs'; a* and *b* – risk weighting coefficients), providing computational assessment support to expert a priori beliefs.

Being rather complex, this explanation is also illustrated with graphical example for 'H-M Coexistence' of Fig. 2a, following the ideas of 2.2.1 on Fig. 4.

Evidently, what is important to note here is the holistic change that not only modifies the 'H-M Coexistence' disposition (from non-critical to critical in SR Diagram) but also transforms some other connected entities classification, compared to Figure 2b: 'Digital Ecosystem' – 4 (*Rb'* > *Rb*, transforming also the entity active role to passive ones), 'Smart Services' – 5 (*Rb'* > *Rb*) and 'Rational Traits' – 8 (*Rf'* > *Rf, Rb'* > *Rb*).

As far as the proposed validation concept is generally missing, an ability for meeting complex changes and uncertainties (not included in the system tangibles & intangibles model or requiring new entities and relations creation) in the next paragraph an interactive results verification with human factor active role will be finally added for achieving framework comprehensiveness.

2.3. Results Interactive Verification

The proper and comprehensive digital future exploration, even in a modelling context, requires also a suitable verification. As quite ambitious, this task could practically implement experience from multiple simulation games approaches [18] and Computer Assisted Exercises [19], [20].

The present one is based on an interactive simulation game, organized during CYREX 2017, encompassing both people and technologies into a new transformed digital reality [21].

The event was conducted for the third year and hosted by Plovdiv University "Paisii Hilendarski" as part of the training course "Security Foundations in Cyber Space" [10].

In 2015 was organized the exercise predecessor simulation game – "Academic Cyber CAX 2015". The event has an international scale for the second time – starting with CYREX 2016 [22].

Main CYREX 2017 organizer was Joint Training Simulation and Analysis Center, Institute of ICT, Bulgarian Academy of Sciences in cooperation with: IFIP, TC 14, Military Academy "Gen. Mihailo Apostolski", Republic of Macedonia, Association of Communication & Information Specialists – Bulgaria and University of National and World Economy.

During the 180 minutes exercise, a simulation scenario script, encompassing: industrial espionage, social engineering, malware and targeted attacks of different type were studied for experimentally understanding the future cyberthreats and challenges expectations.

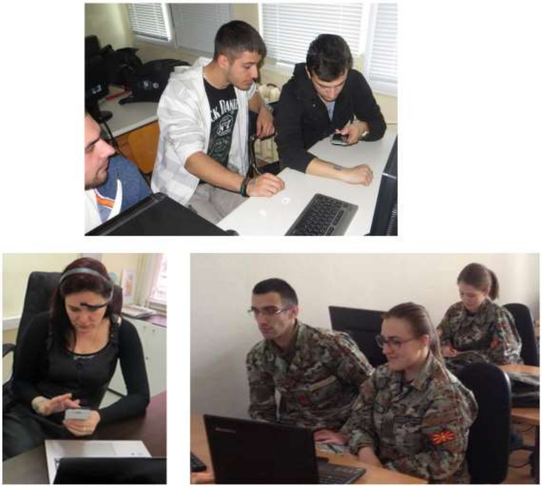

Fig. 5. Moments of CYREX 2017 interactive gaming simulation [21].

The futuristic scenario encompassed innovative technological entertainment gadget of a start-up company that is trying to be controlled from both hacktivist group and multinational corporation for providing bio connectivity between both users and machines. Other supportive NGO and public bodies are also included in the simulation scrip for achieving multirole gaming realism.

The participants used numerous smart gadgets (phablets, tablets, smart watches and bands), desktop and mobile computers, numerous open cloud services, e-mail accounts, chat services, multimedia data, avatars, encryption, decryption and QR codes, organized around closed social network group and accessed via private wireless network in order to experimentally create and study an ad-hoc transformed reality. Their activities were further explored via scenario events playing script and participants' response time delays comparison.

Additionally, selected participants were equipped with smart stickers for temperature and galvanic skin response together with brain activity monitoring that are able to provide a deep analysis for players' physiological responses.

Finally, a q-based survey was also performed among the participants in order to assure comprehensiveness for the exercise evaluation process.

The exercise feedbacks provide a positive overall training assessment but though rather interesting the experimental environment was found somewhat complex for the users. These requires a longer event duration and possible preliminary education with the innovative technological apps and smart gadgets prototypes for social engineering, targeted attacks and biomonitoring handling.

Discussion

The presented framework approach results for the upcoming digital future transformation from tangibles & intangibles perspectives could be generalized as follows:

- The anticipations for joint human-machine autonomous coexistence is expected to be significantly speeded up after year 2021, together with the relevantly evolved AI. Thus the necessary digital and social adaptation and regulation is in process of development as sensors miniaturization and embodiment is expected for booming in Web 4.0 era;

- One of the major problems of future digital world will be the progressive control of the evolving digital ecosystems and economy, providing a rather strong uncertainty from the upcoming active people generation response. Smart services and IoTs will be an important part of the new transformed reality, which will be still quite unfinished, regarding social resilience, due to the slow adaptation of human factor rational traits, behaviour and understandings, strongly influenced by fast progressing digital markets.

- Being rather fascinating, these findings have provoked a recent development of web portal (Secure Digital Future 21, [23]) for a broader topic formalized discussions on the digital future. At the moment, the portal already encompasses about 60 experts from 27 countries throughout the world that hopefully will enrich the current objectives and discoveries towards a larger audience, taking into account the significance of the problem from both technological and social perspectives.

Bibliography

1. Floridi, L. The Fourth Revolution (How the Infosphere is Reshaping Human Reality), 1st ed., Oxford University Press, 2014
2. Schwab, K. The Fourth Industrial Revolution: What It Means, How to Respond, World Economic Forum, May 9, 2017, https://goo.gl/e1Kc3F
3. Choudhury, N. World Wide Web and Its Journey from Web 1.0 to Web 4.0, Int. Journal of Computer Science and Information Technologies, Vol. 5, No. 6, Nov-Dec. 2014, pp. 8096 – 8100
4. Leonhard, G. Digital Transformation: Are You Ready for Exponential Change?, TFAStudios, May 11, 2016, https://youtu.be/ystdF6jN7hc
5. Strauss, W., and Howe, N. Generations: The History of America's Future, 1584 to 2069, New York, Harper Perennial, 1992
6. Built Environment 2050. A Report on Our Digital Future, BIM 2050 Team, 2014, Available at: https://goo.gl/iSqnm6
7. Digital Futures Final Report – A journey into 2050 visions and policy challenges, European Commission DG CNECT, 2016, https://ec.europa.eu/futurium/en/system/files/ged/futurium_scientific_report_v10revcl_v2_0.pdf

8. 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
9. 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
10. Minchev, Z. Security Foundations in Cyber Space, PU "Paisii Hilendarski" Training Course Selected Materials, http://dox.bg/files/dw?a=f42e63cffd
11. IFIP TC13 & TC14 Open Symposium 2017 Web Page, http://ifip-tc13.org/ifip-tc13-tc14-open-symposium-2017-march-22th-2017/
12. Minchev, Z., Dukov, G., Boyadzhiev, D., Mateev, P. Future Cyber Attacks Modelling & Forecasting, ESGI 120 Problems & Final Reports Book, Chapter 5, Fastumprint, pp.77-86, 2016
13. Hazewinkel, M. (Ed.) Encyclopaedia of Mathematics, Springer Netherlands, 1994
14. Minchev, Z. & Shalamanov, V. 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.
15. Minchev, Z., Dukov, G., et al. Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, Fastumprint, pp. 85-92, 2015.
16. Meadows, D., & Randers, J., Meadows, D., Limits to Growth: The 30-Year Update, Chelsea Green Publishing Company, 2004.
17. Panchev, S. The Theory of Chaos (With Examples & Applications), Academic Publishing House "Prof. Marin Drinov", 2001.(in Bulgarian)
18. Georghiou, L., Harper, J., Keenan, M., Miles, I., Popper, R. (Eds) The Handbook of Technology Foresight: Concepts and Practice, Edward Elgar Publishing, Massachusetts, 2008.
19. Cayirci, E., Marincic, D., Computer Assisted Exercises and Training: A Reference Guide, Wiley-Blackwell, 2009.
20. Kick, L. Cyber Exercise Playbook, The MITRE Corporation, 2014, https://goo.gl/SOkkw6
21. CYREX 2017 Web Page, https://goo.gl/sBvVWW
22. CYREX 2016 Web Page, https://goo.gl/PFcpwL
23. Secure Digital Future 21 Web Page, http://www.securedfuture21.net