Future Media Security Transformation in the Digital Age

Zlatogor Minchev[1,2,*], Yulian Hristov[1]

[1]Institute of ICT, Bulgarian Academy of Sciences, Acad. Georgi Bonchev Str., Bl. 25A, Sofia, 1113, Bulgaria
[2]Institute of Mathematics & Informatics, Bulgarian Academy of Sciences, Acad. Georgi Bonchev Str., Bl. 8, Sofia, 1113, Bulgaria

Abstract

Modern media reality constantly changes our understandings, needs, perspectives and so significantly affects the overall security transformation in the new digital age. The innovative media accents in this sense are mostly giving priority to the role of AI and audience preferences, together with information reliability and usage from both human and machine perspectives. However, these changes create also numerous security transcendents for the future media environment and society that need to be properly handled. The study combines morphological with system analytical modeling, aiming comprehensive enough scenario-based future exploration of the new media environment. Further, aiming a suitable results verification, some live experiments with an ad-hoc created media environment and a multirole group of trainees is provided in the context of CYREX 2024 event with additional BISEC 2024 round table discussions on the topic extension. The proposed approach is expected to outline some of the future media security transcendents, and thus supports to the establishment of a more innovative, secure and resilient future society in the new digital age.

Keywords

Future media, security transcendents, scenario-based future exploration, analytical modeling, experimental results verification

1. Introduction

Properly understanding of the future media environment is a quite challenging task in the new digital age [1, 2]. In this sense, the process could be directly connected with the web technologies evolution and resulting transformational transcendents, following [3]. Though the idea sounds somewhat interesting, it should be noted that with the appearance of interactive media communication (in Web 2.0 technologies), mostly visible due to blogging, chatting and commenting in modern social networks, the evolution fostered with AI immersion is getting quite strong. Presently, Web 3.0 is mainly related to smart semantic webs and chat bots, but with Web 4.0 evolution the environment is getting even more fascinating due to different IoTs and virtual worlds mixing with the objective reality. The modern Meta Ray-Ban & Oculus, Microsoft HoloLens, HTC or Apple Vision smart VR/AR/MR/XR googles (being an IoT smart devices in general) are already providing this digital immersion quite well. Though so far not quite popular due to different reasons, but still mostly addressing gaming and entertainment industries more successfully [4]. What however is important to note here is the leading role of AI algorithms embraced with avatars and chatbots that have to be significantly marked with attention. The reasons for this are quite complex and could be generalized with two directions: (i) the media bubble profiling of social networks that is even more significant with smart googles and expensive advanced smart phones, and (ii) the evolutionary development of machine-to-machine communications with AI autonomization towards General AI. This practically addresses the next level of machine-to-human communication, being expected with Web 5.0 and BCI that should give consciousness not only to humans but also to machines [5], similar to some sci-fi genre expectations [6]. The already noted trends however are mainly related to human-machine domination competition in the not-so-far future digital society [7] but also reasonably open the media audience debate [8].

From todays' perspective in fact, the process enables indexing bots, chatbots and avatars as modern social and mass media players that could significantly evolve if the limits added to AI evolution are

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia
*Corresponding author.
zlatogor@bas.bg (Z. Minchev); yulian.hristov@iict.bas.bg (Y. Hristov)
0000-0003-2479-5496 (Z. Minchev); 0009-0003-8840-2134 (Y. Hristov)

Morphological Analysis

Drivers	Challenges	Threats	Opportunities	Divides	Gaps
Social Dynamics	Fake Information	Hybrid Attacks	Media Biasing	User Profiling	Info Uncertainties
Climate_Env_Change	Mixed Funding Schemes	Social Media Bubble	Audience Scalability	Rich Info Contradictions	Trust_Credibility
Tech Innovations	H-M Intelligence Conflicts	Cognitive Transformation	Cross Platform Comms	Multigeneration Issues	Digital Ethics
Multicultural Clashes	Intermedia Competition	Digital Overthrust	Media Smart Assistance		

Index	Length	Weight	Name
1	6	65	Scenario1
2	6	-15	Scenario2
3	6	75	Scenario3
4	6	15	Scenario4
5	6	-55	Scenario5
6	6	-15	Scenario6
7	6	75	Scenario7

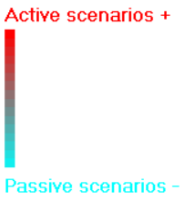


Figure 1: Plausible & implausible cross-consistency scenario matrix of future media security transcendents in I-SCIP-MA.

quite modest in general.

Further in the paper a more comprehensive, systematized exploration of the future media transformation will be given via a three-fold approach: (i) morphological problem space definition, (ii) system analysis deeper risks exploration of the future media security problem at hand (merged with Section 2 & Section 3), followed with final (iii) experimental results verification (outlined in Section 4) and a wrap-up discussion (Section 5).

2. Problem Space Definition

This initial step assumes that a scenario-based planning for the digital future security transformation is accepted. Following the morphological cross-consistency transcendents' matrix representation with a set of dimensions (Drivers, Challenges, Threats, Opportunities, Divides & Gaps) and mutually exclusive alternatives (cells in each dimension, e.g. "Social Dynamics") have been used. The resulting matrix contains both plausible & implausible pools for scenarios [7]. Though certainly not comprehensive enough due to its modelling nature the approach is significantly well-known and quite popular with uncertain and unclear large classification problems initial exploration.

The work here has been significantly fostered with I-SCIP-MA environment, giving a dual classification of *Active* (having aggregated positive weight) and *Passive* scenario combinations. The implemented assessment also gives a possibility to have a *Neutral* ones, whilst taking into account the accepted measuring scale of weights [9].

The presented example in Fig. 1, shows a cross-consistency scenario matrix screenshot from I-SCIP-MA, having N1 = 642 (368 – active, 252 – passive & 22 – neutral), plausible combinations & N2 = 13182 – implausible ones (being somewhat uncertain) of N = 13824 (6 x 4 x 4 x 4 x 4 x 3 x 3) in total.

Below are given some aggregated comments on future transformational transcendents, taking into account the morphological analysis analytical implementation.

- One of the biggest problems for the future media is expected to be related to digital overthrust (as both human and machine conflicts are going to address AI algorithms) with the information gathering & processing. The problem actually comes from the AI biasing that is still difficult to be neutrally handled (as AI is still quite innovative feature for the media field) and also expected to gather fake popularity and thus additional funding that in fact is an intermedia competition in general.
- Another problem is the overall cognitive transformation of future humans due to multiple smart gadgets' assistance comfort and social dynamics technological augmentation. This actually affects mostly new generations to come but also millennial and post-millennial ones.

- The social media bubble that nowadays is getting more and more smart as user profiling is actually producing a biased media that are capable to skilfully play with audience scalability, trust and interests from both economic and socio-political perspectives. This produces multiple hybrid human-machine attacks of truth and realism. The bigger problem here appears from unreal information greater entertainment and higher popularity effects [10].

So, omitting digital ethics could be quite profitable but dangerous with the future web technologies evolution, as with the new smart virtual worlds of Web 4.0, people are getting less freedoms and become more inclined, directed from humans and AI solutions preferences and behaviour. The upcoming highly dynamic and rich information autonomous handling becomes impossible without suitable smart assistance, i.e. technological support, especially with the new digital societies' evolution is of vital importance. Finally, the multicultural and multilanguage clashes are expected to be less common due to multidimensional media outlook that hopefully will successfully handle the environment and climate changes with adequate trust and credibility relying on a new transformed media environment, properly assisted with Extended AI, either General AI in the not so far future.

As the presented morphological analysis findings are not giving the causality origins of the outlined future media security findings, a further advanced risk system analysis is provided.

3. System Analysis Exploration

The system causality interpretation of future media security transformation could be quite useful, especially from a future foreseeing perspective, allowing an extended use of scenario cross-consistency matrix for a holistic system's dynamic risk assessment. The presented further system-of-systems model, contains 11 entities and 24 bi-directional relations (see Figure 2a), aggregated within a System Risk Diagram (see Figure 2b) in I-SCIP-RA environment, following the ideas of [11].

As dynamic system risks consideration will be studied in more detail with the experimental verification (See Section 4) a final assessment towards the next five years is aggregated stepwise (two for each year, i.e. considering a discrete six months representation as follows:

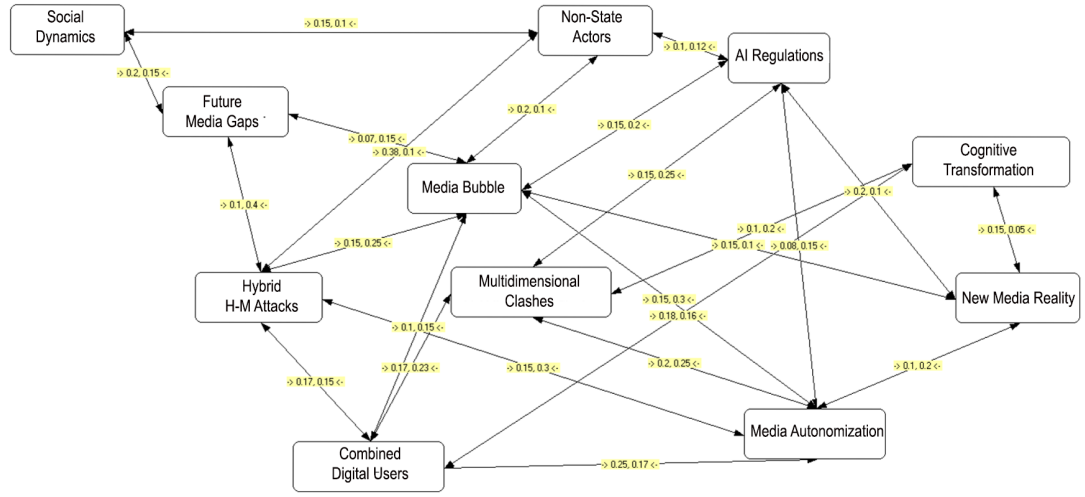
"1 – 2025(I), 1 – 2025(II)…, 9 – 2030(I), 10 – 2030(II)") with a System Risk Diagram (SR Diagram, encompassing a probabilistic assessment of: *Direct* - forward, *Indirect* – backward, and *Aggregated* system risks in the interval [0, 1]), producing a two-class distribution: *Critical* vs *Non-Critical* ones. Additional entities' role assessment (in each of the classes) with "Active" (white) vs "Passive" (grey) ones is also implemented.

The presented results show an aggregated probabilistic system risk assessment for future media security transformation towards year 2030 as follows:

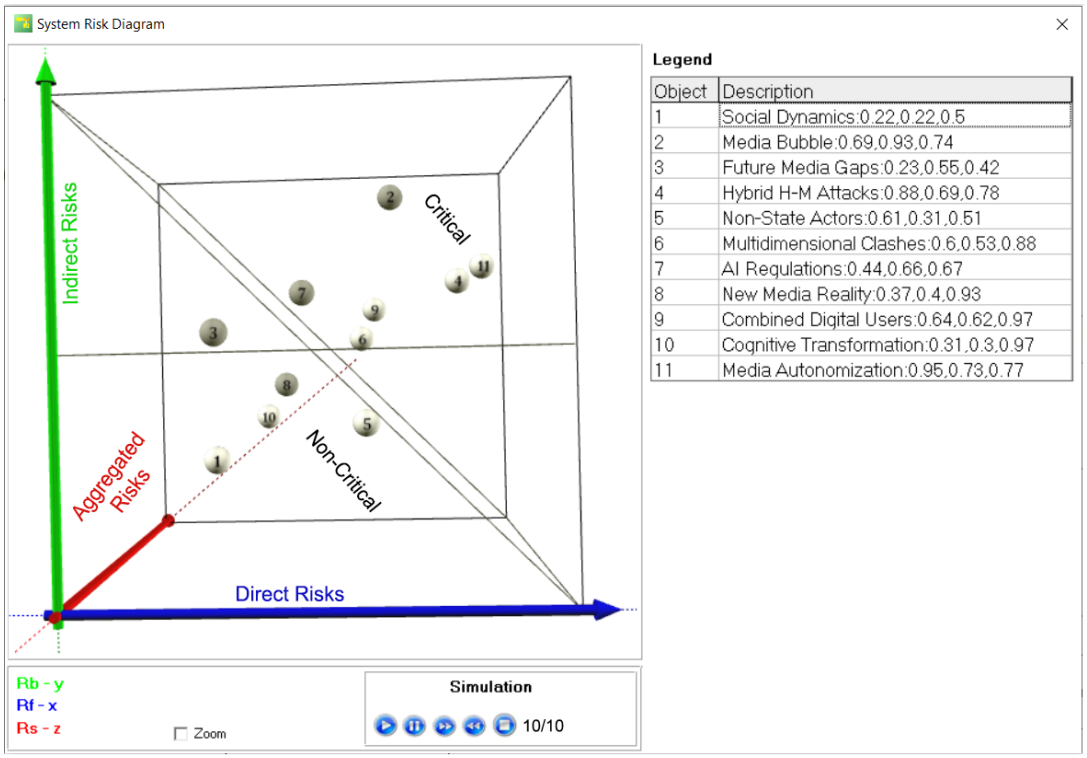
Critical risk priorities are expected for: Media Bubble (2), AI Regulations (2), whilst all being "Passive"; Hybrid H-M Attacks (4), Multidimensional Clashes (6), Combined Digital Users (9), Media Autonomization (11), all being "Active".

Non-Critical risk priorities are given to: Future Media Gaps (3), New Media Reality (8), all "Passive"; Social Dynamics (1), Non-State Actors (5), Cognitive Transformation (10) all "Active".

Obviously, the future media security transformation gives a quite important role to AI mixing with the new media reality. This actually hides a lot of risks towards the new media bubble that is going to be addressed from numerous hybrid attacks and clashes inspired with state & non-state actors, having different motivations [12, 13]. Apart of this, with the AI progressive development the regulation of this transformed media reality security will certainly need both framework and assisted AI support, as far as future media is probably going to become somewhat autonomous, transforming audience cognitive & emotional responses [8]. And all these is developing a new level of autonomous machine-to-machine communication that is targeting the human audience in an unprecedented manner. Luckily, the human intellect will be able to keep domination due to speed, scale and contents AI assisted handling. With these analytical expectations marked in Section 2 & Section 3 a further aggregated results' experimental verification will be presented in the next section.



(a)



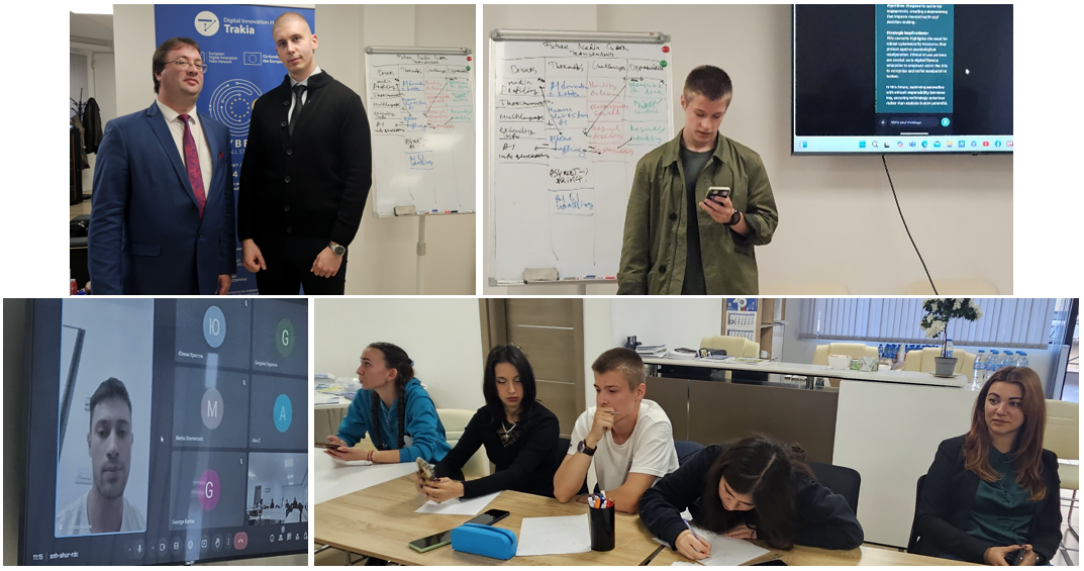
(b)

Figure 2: Future media security transformation system model (a) & resulting SR Diagram (b) in I-SCIP-RA environment

4. Experimental Results Verification

This stage has been performed in two parts: (i) During the international Cyber Research Exercise 2024 – CYREX 2024, organized as a training event amongst young people gathered in the framework of European Digital Innovation Hub "Trakia", National Scientific Programme "Security & Defense" & Secure Digital Future 21 forum united cybersecurity efforts [14]. (ii) Additionally, some high-level discussion generalized findings have been collected during "Future media and security issues in the Age of AI" roundtable discussion of BISEC 2024 [16].

In brief, CYREX 2024 has been organized as an international, web distributed, computer assisted exercise with nine-years history, providing cyber training that involves university, academic, profes-



(a)

(b)

Figure 3: Selected moments from CYREX 2024 training event (a) & "Future media and security issues in the Age of AI" roundtable discussion at BISEC 2024 (b).

sional associations and industrial participants. The main training audience is a selected group of about thirty students from Bulgaria & Italy with some invited expert members of Secure Digital Future 21 international forum (see Figure 3a).

The exercise concerns a fictitious scenario for a three-hour distributed training of a multirole human-machine intellect competition that involves: smart robots, media & people in a fight for leadership and domination, concerning future of climate changes and human beings' settlements around the Solar System. In practice the idea is to use different smart gadgets for participants' multirole interconnectivity via social networks and an ad-hoc smart media platform [15], adding AI generative and analytical tools, while taking their responses on innovative AI security transcendents practical identification [17].

Further, the accomplished findings from CYREX 2024 were somewhat extended and used during a roundtable media and security discussion, organized amongst BISEC 2024 security conference participants with invited international key-note speakers and stakeholders from academia, media & state administration (see Figure 3b).

The aggregated results, concerning future media security in the age of AI in the process towards year 2025 are presented graphically in Figure 4.

Figure 4: Future Media & AI aggregated verifications towards year 2035, after [14, 15].

Obviously, the presented models' verification results give some future security extensions. This fact is valid, especially about the expectations for emotions and psychology fears from the perspective of future media AI assisted (and even AI-to-AI autonomous ones) infinite interaction isues even without human-in-the-loop. The problem could get much worse, considering the AI models pretraining, usually considered as "hallucination" and the issues of media audience information flooding [9]. The last normally produces attention fatigue or digital overloading necessity (and even addiction) regarding different audience ages, but is also resulting an unhealthy interest on fake news as a tool for countering the overall artificially directed "grey" information context. The new AI generated contents should be properly branded as to achieve proper smart media environment regulation, while keeping freedom and reliability of the environment. This access, while measuring the cognitive and emotional responses of the mixed H-M audience. Finally, it should be noted, that the problem of future media security handling is quite important not just from human perspective as the AI evolution could grow towards sentient or general levels. These will transform the new social environment of the digital age in an unprecedented manner that will require AI dual media transformation especially with Web 4.0 & Web 5.0 will become even more personalized due to transhumanization and H-M realities different mixing and competing for domination. At the same time, however the new smart media stays susceptible to both state and non-state actors influencing, that together with avataring, AI assistants and multipurpose bots involvement will make the digital future quite insecure without suitable AI protection extensive support.

5. Discussion

Understanding the future of media transformation in the age of AI fast progress is a quite challenging task. Whilst successful joining of the human and machine intellect in this task is somewhat useful with the implementation of experimentally verified morphological and system analysis findings, the future security transcendents identification and coping is always under discussion. Suitable extension of the proposed methodology is on the way with Web 4.0 & Web 5.0 technological support of wearable devices for VR/XR media smart environment access, while measuring the cognitive and emotional responses of the mixed H-M audience. Finally, it should be noted, that the problem of future media security handling is quite important not just from human perspective as the AI evolution could grow towards sentient or general levels. These will transform the new social environment of the digital age in an unprecedented manner that will require AI dual use of technologies, while giving them semiautonomous role, at least in the future media environment handling.

Acknowledgment

The authors of this study are granting special appreciations for the experimental base and partial funding support to the National Scientific Programme "Security & Defense". Additional gratitude for the institutional contribution is provided to EDIH Trakia and in person to Denis Petkov & Hristo Kukov, Università Bocconi, Italy for the help during CYREX 2024 training. Distinctive thanks are expressed to BISEC 2024 organizers from Belgarade Metropolitan University and in person to Nemanja Zdravković & Plamen Kolev, HiLife Media for the fruitful discussions during the roundtable "Future media and security issues in the Age of AI". The analytical results presented in the paper are benefiting the international expert support obtained in the framework of the initiative "Securing Digital Future 21" with more than sixty countries now, spread around the world, https://securedfuture21.org/.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Z. Minchev, L. Boyanov, et al., Future digital society resilience in the informational age, Sofia: SoftTrade & Institute of ICT, Bulgarian Academy of Sciences (2019).

[2] R. Lätti, P. Hermansson, N. Malmelin, M. Paltschik, MEDIA 2035: Four Scenarios for the Future of Media, 2024. URL: https://www.mediaalantutkimussaatio.fi/wp-content/uploads/Media-2035-Four-Scenarios-for-the-Future-of-Media.pdf.

[3] Z. Minchev, L. Boyanov, Smart homes cyberthreats identification based on interactive training, in: Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE), International Conference on Application of Information and Communication, 2013, pp. 72–82.

[4] Research & Markets, Immersive Entertainment Market Size, Share & Trends Analysis Report by Technology Type (Virtual Reality, Augmented Reality, Mixed Reality), Application (Gaming, Live Events), Region, and Segment Forecasts, 2024-2030, 2024. URL: https://www.researchandmarkets.com/reports/5976548/immersive-entertainment-market-size-share-and.

[5] Y. N. Harari, Nexus: A brief history of information networks from the stone age to AI, Signal, 2024.

[6] H. Osawa, D. Miyamoto, S. Hase, R. Saijo, K. Fukuchi, Y. Miyake, Visions of artificial intelligence and robots in science fiction: a computational analysis, International Journal of Social Robotics 14 (2022) 2123–2133.

[7] Z. Minchev, Digital Transformation in the Post-Information Age, SoftTrade, 2022.

[8] D. A. Rohlinger, S. Sobieraj, The Oxford handbook of digital media sociology, Oxford University Press, 2022.

[9] Z. B. Minchev, Human factor role for cyber threats resilience, in: Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI global, 2016, pp. 377–402.

[10] S. Vosoughi, D. Roy, S. Aral, The spread of true and false news online, science 359 (2018) 1146–1151.

[11] Z. Minchev, Analytical challenges to modern digital transformation, in: Proc. of Tenth National Conference "Education and Research in the Information Society", Plovdiv, Bulgaria, 2017, pp. 38–47.

[12] E. Pauwels, Preparing for Next-Generation Information Warfare with Generative AI, 2024. URL: https://www.cigionline.org/static/documents/Pauwels-Nov2024.pdf.

[13] World Economic Forum, The Global Risks Report 2024, 19th Edition, 2024. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

[14] Securing Digital Future 21, 2024. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

[15] Defakeoutlet web platform, 2024. URL: https://shorturl.at/gfRnM.

[16] N. Zdravkovic, Z. Minchev, P. Kolev, E. Radibratović, Future media and security issues in the Age of AI, 2024. URL: https://youtu.be/FjHNXtd_ItE?t=6245.
[17] CYREX 2024, Cyber research exercise 2024, 2024. URL: https://securedfuture21.org/cyrex_2024/cyrex_2024.html.