Cybersecurity Synergies & Gaps Identification in the Age of Digital Cognition

Zlatogor Minchev[1,2,3][0000-0003-2479-5496]

[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
[3] Centre for Implementation of Scientific Research on Digitisation of the Economy in an Environment of Big Data (DEEBD), Sofia, Bulgaria
zlatogor@bas.bg

Abstract. Nowadays smart digital reality is already evolving to a new fundamental change, related to the fast AI algorithmic sentient progress with vast interconnectivities and the resulting H-M symbiotic development. The study outlines a practical experiment on the "digital cognition" modelling, in the context of AI sentient evolution exploration. Expert data and generative AI feedbacks are initially used in this process, both fused in an ad hoc created system-of-systems dynamic model. Further, a dynamic assessment of the model is performed with mixed H-M validation by implementing the scenario method and probabilistic HPC simulations. Most prominent results have been finally jointly verified in an interactive simulation with a human-in-the-loop active role during CYREX 2025 and in lab conditions. The approach is trying to identify key synergies and gaps of the model, outlining also internal triggers, aiming potential system advancements. The obtained results are expected to support the development of a forward-thinking holistic proactive analysis of the cyber security evolution, giving accent to the sentient features of "digital cognition" in both offensive and defensive context. These will create a suitable post-information society preparation for successful handling of the future interconnected reality's AI-influenced transcendents and the necessity for a dual human-machine smart regulations establishment within the not so far future.

Keywords: Future Cyber Security, Synergies & Gaps Identification, Digital Cognition, System Dynamics Modelling, H-M Validation & Verification.

1 Introduction

Modern digital reality of joint human-machine co-existence is already evolving to a new level of profound transformation, mostly related to the fast AI algorithmic sentient progress & IoTs' interconnectivities boom [1]. Todays' AI generative solutions are creating an impression for "digital cognition" framework existence that certainly needs improvements [2]. At the same time, this shapes the modern human thinking and

Research Paper
DOI: https://doi.org/10.46793/BISEC25.120M
Part of ISBN: 978-86-89755-40-4

cognition in a unique manner, establishing emotional attachment to digital technologies, based on human & machine bidirectional smart communications [3]. This new phenomenon will probably trigger the future digital society evolution towards Society 6.0 (majorated with AI and robots) in an unprecedented way for the next 10-15 years [4].

This new societal organization is expected to establish a landscape where human systems, digital ecosystems, and AI will co-evolve rather than merely coexist. In this system organization, the digital cognition will become a shared layer of awareness, with AI agents interpreting, predicting, and adapting to human needs in real time. As AI is going to approach a sentience level of evolution, functions like: self-modeling, context-aware reasoning, or autonomous goal formation are going to reshape the future governance, security, and overall identity. The boundary between human and machine cognition will become quite porous, creating a hybrid societal intelligence that is both more capable, but also more fragile.

In this context, proactively identifying the human-machines synergies and gaps is of vital importance, especially for the future security and in particular – cybersecurity, successful proactive handling together with important triggers & advancements [5].

So, several key synergetic moments need to be specifically marked hereafter and further explored:

(i) Wide smart devices interconnection with IoT concept, that practically are implementing different heterogenous networks holistic outlook, towards "Internet of Everything" and smart AI agenting within multiple sensors [6];

(ii) "Machine-to-Machine" & "Machine-to-Human" smart communications in the "Internet of Everything" context progressive and autonomous development;

(iii) AI algorithms self-assessment, aiming initially "sentience" with potential further "singularity" objectives [7];

(iv) New Society 6.0 dominated with smart technologies, services and the lifestyle overall digital transformation;

(v) Human factor role in the new Society 6.0 and the responsive effects to the live vs digital cognition [8];

(vi) New cybersecurity offensive/defensive capabilities and the role of AI autonomization [9];

(vii) Regulations and boundaries to AI, aiming dual human-machine sentience and singularity [10].

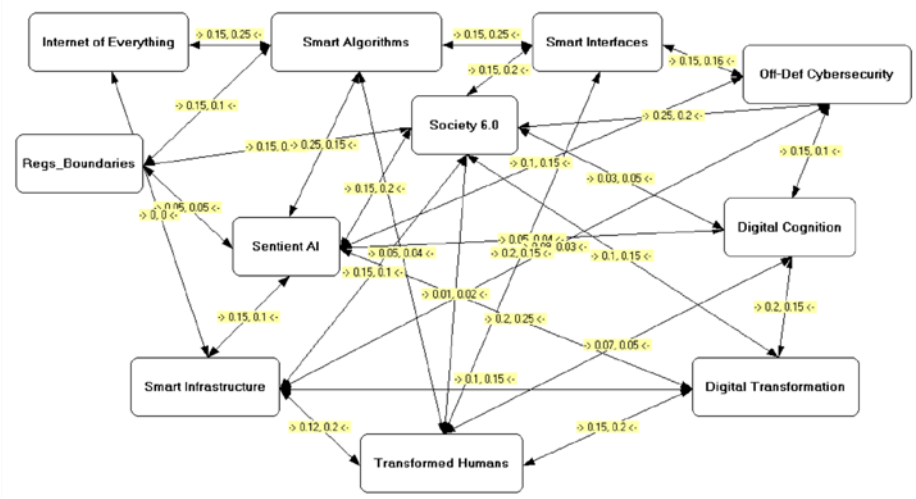
As this list is not completely exhaustive but quite comprehensive, the uncertainties and gaps need also to be added for completeness, aiming transformation to a new cognitive level of quantum computing and communicating between humans and machines.

Further in the paper a more comprehensive, systematized exploration of these synergetic moments and gaps of H-M joint symbiosis in the new smart cybersecurity context of the transformed digital future will be given via a three-fold approach, advancing the ideas from [1], [11] but seeking for deeper H-M symbiosis: dynamic system model development (Section 2), followed by multiple cybersecurity scenarios matrix establishing (Section 3), further validated with H-M mixed efforts (Section 4) and verified with the most prominent results with a human-in-the-loop active role (Section 5), concludingly wrap-up with a brief discussion on the obtained results (Section 6).

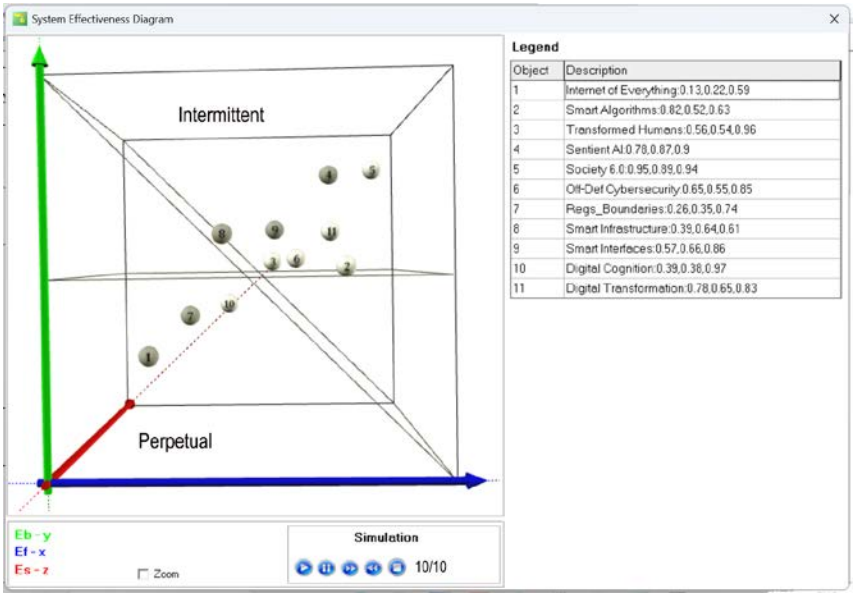
2 Dynamic System Model

The system-of-systems modelling, proposed by famous Generalized System Theory [12], has been simplified in the discrete case by Vester [13], whilst keeping causality model for entities interconnectivities interpretation of Entity-Relationship (E-R) modelling [14]. This gives quite useful approach for exploring the future digital cognition age cybersecurity issues, especially from a future foreseeing perspective, providing a holistic system's dynamic effectiveness assessment.

The presented further system-of-systems model, contains 11 entities and 28 bi-directional relations (see Fig. 1a), aggregated within a System Effectiveness Diagram (see Fig. 1b) in I-SCIP-EA environment, following the ideas of [11].



(a)



(b)

Fig. 1. System modelling of future cybersecurity issues in the age of digital cognition (a) & resulting SE Diagram (b), towards year 2040 in I-SCIP-EA environment.

As far as the effectiveness assessment will be considered in dynamics in more detail with the experimental validation (see Section 4) a final assessment towards the next fifteen years (targeting year 2040) is presented stepwisely (one step for each year & a half, i.e.: "1 – 2025,…, 9 – 2039, 10 – 2040) with a resulting *System Effectiveness Diagram* (*SE Diagram*), after [11], encompassing a probabilistic assessment of: system effectiveness – E_s interpretation by feed-forward effectiveness – E_f and feed-backward – E_b ratio usage. E_s values have been obtained, by using a Bayesian probabilistic approach towards a certain scenario evolution. Briefly, the idea could be summarized as follows: E_s (E_f, E_b); E_i (R_i, U_i, S_k) = P ($R_i|S_k$) × P ($U_i|S_k$), where: P (...) – Bayesian probability, R_i – system risk, U_i – system utility, $i = \{f, b\}$, S_k – selected k-th scenario from the scenario cross-consistency matrix pool M (see Section 3). Both R_i and U_i could have multiple probabilistic meanings, but not obviously with a correlating nature. The resulting behavior of entities (assessed in the SE Diagram) varies with both "Intermittent" vs "Perpetual" classes (divided with the NW/SE diagram diagonal). A sub-classification for both types of entities, regarding their model roles are: "*Active*" (white), either "*Passive*" (grey) ones.

The presented results show an aggregated probabilistic system effectiveness assessment for the future cybersecurity issues in the age of digital cognition, towards year 2040 as follows:

Perpetual entities priorities are expected for: “Internet of Everything” – (1), “Regs_Boundaries” – (7), all being “Passive” & “Digital Cognition” – (10), being an “Active” one’s.

Intermittent entities priorities are given to: “Smart Algorithms” – (2), “Transformed Humans” – (3), “Society 6.0” – (5), “Off-Deff Cybersecurity” – (6) & “Digital Transformation” – (11), all being “Active”; “Sentient AI” – (4), “Smart Infrastructure” – (8), “Smart Interfaces” – (9), all “Passive”.

So, in the future age of digital cognition it is expected that everything will be heterogeneous, i.e. connected via Internet (with multiple tech solutions, like: optics, mobile comms, wireless solutions, wires), keeping at the same time regulations and boundaries for AI, but being also in a way threatening both offensive & defensive cyber security because of the numerous unknowns (like: synergies, gaps, triggers).

Whilst transformed humans and smart AI algorithms are going to be quite unstable for the new Society 6.0 (dominated with AI and robots), keeping alive & continuing digital transformation processes of both humans and machines.

Apart of these, hidden threats are expected to emerge from smart infrastructure and interface, together with sentient AI. Going deeper to these findings in the next section will be considered and the cyber security matrix, outlining more details on the future cybersecurity issues.

3 Cybersecurity Scenarios Matrix

At this section, an assumption for a scenario-based planning, concerning the not so far digital future (towards year 2040) for the “age of digital cognition” [1]. Following a morphological cross-consistency matrix representation [15], a set of six dimensions *(Cyber_AD_Pairs, Targets, Joint Effects, Security Gaps, H-M Synergies, H-M Triggers)* and twenty-three mutually exclusive alternatives (marked as cells in each dimension) have been defined. The resulting matrix contains both plausible & implausible pools for cyber- attack/defense (AD) scenarios in the context of H-M different symbiotic issues (gaps, synergies, triggers) & joint effects, addressing the new smart transhuman idea, infrastructure, services & interfaces.

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 [15].

The exploration process here has been 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 [16].

The presented example in Fig. 2, shows a cross-consistency scenario matrix screenshot from I-SCIP-MA, having N1 = 1110 (430 – active, 634 – passive & 46 – neutral), plausible combinations & N2 = 15090 – implausible ones (being somewhat uncertain) of **N** = 16200 (6 x 3x 5 x 3 x 3 x 4 x 5) in total.

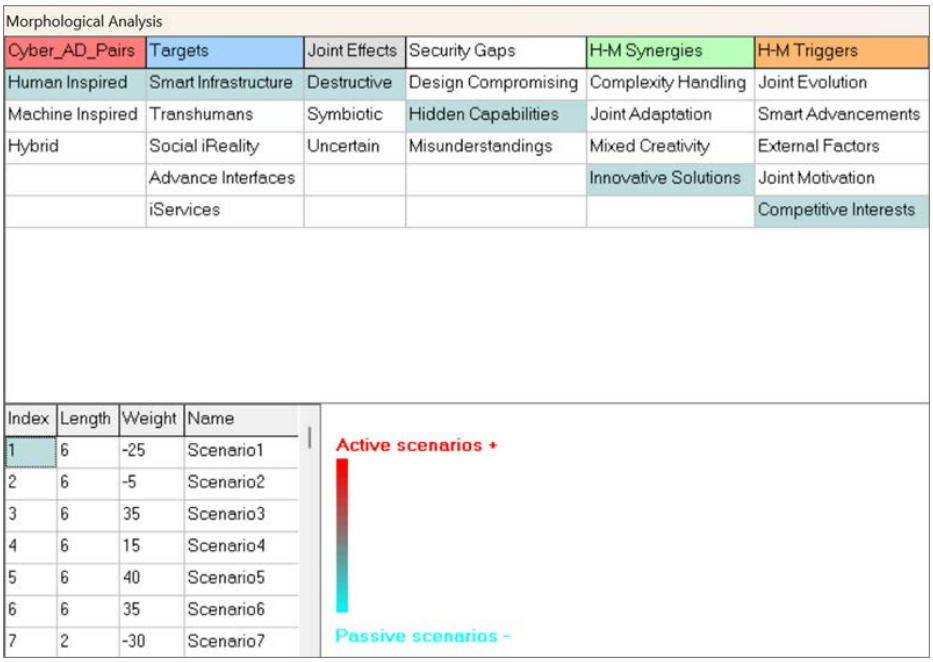


Fig. 2. Multiple cybersecurity scenarios matrix M within different H-M symbiotic issues *(Attacks/Defense Pairs, Targets, H-M Joint Effects, Gaps, Synergies & Triggers)*, related to the age of digital cognition, produced in I-SCIP-MA environment.

Some consolidated comments on the future cybersecurity issues in the H-M joint context for the age of digital cognition, resulting from the scenario matrix morphological analysis are given hereafter:

- Most of the hidden problems that will affect the future cybersecurity (both offensive & defensive ones) will result from AI algorithms embedding in the smart infrastructure, transhumans & the use of new, advanced interfaces for presenting intelligent services in the future social intelligent reality;

- As far as the new Society 6.0 is proclaimed to be quite utopian within the new joint H-M extended skills and traits, negative, destructive effects for the humans and machines are quite possible due to multiple security gaps (like: design compromising, hidden capabilities or misunderstandings from the system updates, patches or new configurations);

- More complex and huge scale and speed tasks handling that will be easily solvable with extended H-M creative symbiosis, producing new level of societal evolution;

- Different motivations for both human and machines, but at the same time possible competitiveness that could produce dual effects and affect both cyber security and society organization.

As the presented analytical findings are important to be studied in a more formalized way, trying to outline the dynamic nature of the cybersecurity in the age of digital

cognition, a further implementation within the system model from Section 2 has been performed.

4 Mixed Validation

Properly handling the holistic systems complexity of a model is in general a context dependable task. A suitable dynamic approach to a bounded by a relevant model context for cybersecurity issues with related to them triggers, gaps and synergies could be considered by joining the results of both system and morphological analyses in a symbiotic H-M manner, especially for the age of digital cognition.

So, using both human expectations and machine simulations for a feasible future, a joined H-M result could be aggregated, as follows:

(i) A system model dynamics probabilistic distribution approximation fitting, regarding entities desired position (by means of SE Diagram, see Fig. 1b) with Beta (in 2D) & Dirichlet (in the multidimensional case) distributions;

(ii) Consideration of Kondratiev & Forrester's simplifications, noted in [17] with a certain time horizon, whilst adding appropriate assessment criteria for (i) (see e.g. [1], [11]) towards the future time horizon of year 2040.

Further, the algorithm could be extended with three more steps:

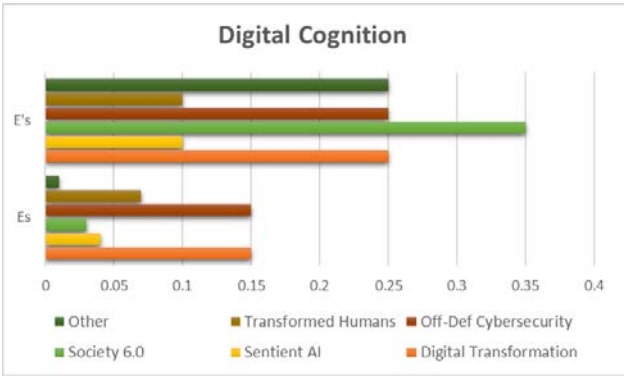
(iii) Initial machine assignment of a priori probabilistic values for the scenarios in matrix M (see Section 3), by rearranging the classification weights in the interval [0, 1], produced by humans and machines collaboration, i.e.: $M \in [a, b] \rightarrow M' \in [0, 1]$, $M' = f(M\text{-}a/b\text{-}a)$, Where f – is a non-linear transfer function that converts the interval $[a, b] \rightarrow [0, 1]$;

(iv) HPC matching with Quasi Monte-Carlo (QMC) simulations of M scenarios probabilities to the model relationships' (R) weights' matrix – N, towards a new repositioning of the entities (E) in the system model, by changing N, $(N \times M \rightarrow N')$, while using a Bayesian probability assessment for the new effectiveness $E'_i(E'_f, E'_b)$, $E'_i(R'_i, U'_i, S'_k) = P(R'_i|S'_k) \times P(U'_i|S'_k)$, where: $P(...)$ – Bayesian probability, R'_i – a posteriori system risk, U'_i – a posteriori system utility, $i = \{f, b\}$, S'_k – selected k-th scenario changed probability, Where: $S_k \propto S_k.P(QMC_k)$, similar to [1].

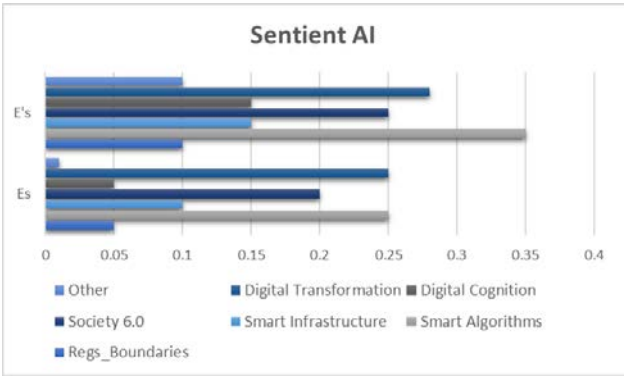
(v) Overall results listing arrangement for successful bounding of scenarios, relations and entities.

Finally, what is important to note within the dynamic simulations' hereafter are the difficulties related to potential multiple sub-models of interest parallel exploration that requires a lot of computational resources. Supportive solution in this sense is the implementation of base dynamic wave oscillators that allow periodic synchronization assessments [11].

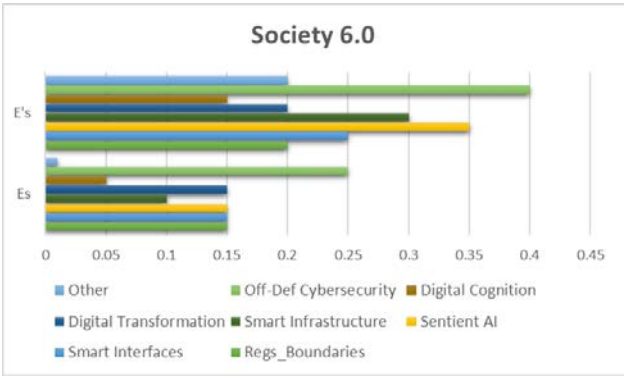
Some illustrative examples, concerning selected entities from the system model presented in Fig.1 are given below:



(a)



(b)



(c)

Fig. 3. Mixed H-M assessment examples of present E_s & future E'_s effectiveness dynamic changes for three selected entities from the system model from Fig. 1.

As far as all these mixed model assessments are with somewhat limited human factor role and subjective AI usage, resulting from multiple uncertainties (due to futuristic

exploration a priori inclines & natural discrete modelling generalizations), an additional verification has been studied too.

5 Joined Verification

The verification activities were executed in two distinct parts.

(i) The primary part was performed during the Cyber Research Exercise 2025 (CYREX 2025), organized as a youth‑focused training event within the International Conference with Cyber/HPC Training “Future Security Transformation: Synergies in the Post‑Information Age”, [18]. This event was jointly coordinated by Joint Training Simulation & Analysis Center (JTSAC), Institute of ICT, Bulgarian Academy of Sciences (IICT‑BAS), EDIH “Trakia”, and the EuroCC2 project research group, in cooperation with the Association of the Officers in the Reserve “Atlantic”, IFIP TC 14 “Entertainment Computing”, and the Association for the Development of the Information Society. Funding support was provided through the National Scientific Programme “Security & Defense” and the Secure Digital Future 21 international expert forum.

(ii) Complementary verification was conducted through laboratory‑based experiments addressing mixed (MR) and extended reality (XR) scenarios, including biometric feedback analyses, performed by JTSAC and IICT‑BAS.

CYREX 2025 took place as a web‑distributed, computer‑assisted cyber exercise, continuing a ten‑year tradition of engaging universities, academic bodies, professional associations, and industry partners. Its core training group includes about twenty selected participants, among them young researchers and invited experts from the Secure Digital Future 21 forum (see Fig. 4a).

The exercise concerns a fictitious scenario for a two-hour distributed training of a multirole human-machine joint intellectual synergy cooperation that considers the following story in brief:

(a)

(b)

(c)

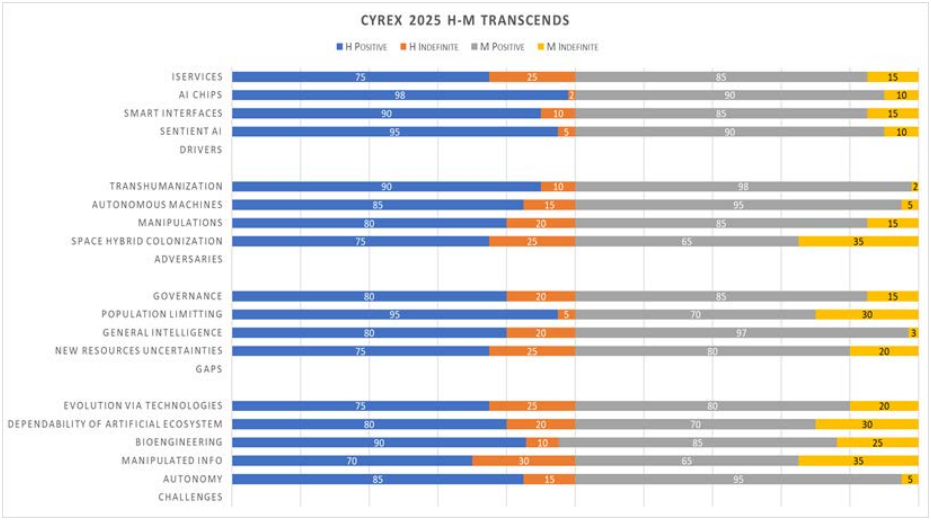
Fig. 4. Selected moments, architecture & scenario from CYREX 2025 training event (a); Experimental lab studies with MR (b) and XR (c), implementing biometrics feedback analyses.

A solar system planet smart megacity struggles to contain a rising clash between machines, seeking to overwrite biology and insurgents twisting DNA and cyber systems of humans' inhabitants, whilst aiming to seize control of city and transhumans neural infrastructure. As hacked instincts, weaponized evolution, and misfired AI behaviors collide. Humanity survived only by transforming into something new, reshaping the future of life and conflicts, while cleaning the Earth and stabilizing its climate.

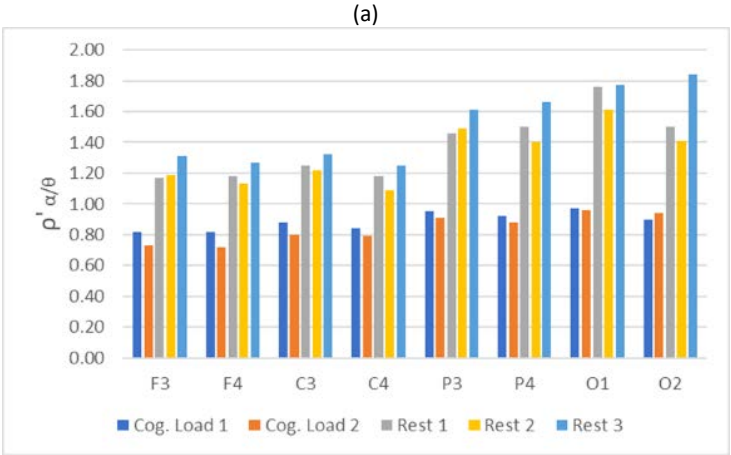
Key participants in the exercise were: smart robots, drones, people and AI in a fight for concurring and domination of human cognition with advanced cyber-warfare technologies, based on implants & sentient AI.

In practice the idea is to simulate a future war situation in a mixed reality, between smart machines and bio-engineered human warriors, while using different smart gadgets for participants' multirole interconnectivity (similar to longstanding practices [19]), adding private & public AI generative and analytical tools, while taking their responses on innovative & smart cyber security issues.

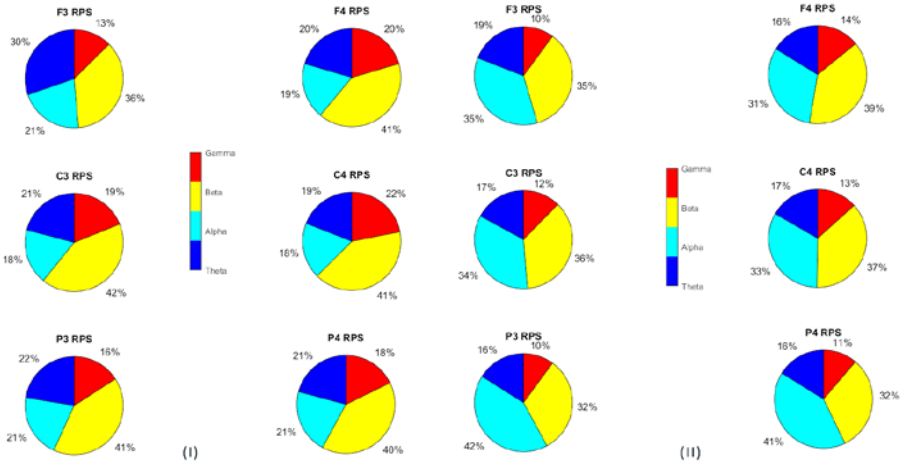
Further, the accomplished findings from CYREX 2025 were aggregated (see Fig. 5a) and partially more profoundly studied with additional cognitive experiments (in extended and mixed realities), trying to assess cognitive loads vs rest discrimination and the role of digital fatigue, following the approaches from [1] & [11] (see Fig. 5b).



(a)



(b)



(c)

Fig. 5. Aggregated CYREX 2025 findings for cognitive age transcendents proactive H-M identification (a); generalized results for ρ'α/θ ratio from EEG activity for Rest vs Cog. Load discrimination with fatigue accumulation in MR (b); EEG Relative Power Spectrum for Rest (I) vs Cog. Load (II) differences without fatigue accumulation in XR (c).

Certainly, the extended verification findings offer a more comprehensive and nuanced perspective on the interaction between digital and human cognitive processes, marking also factors like digital fatigue, information overload & flooding (see e.g. [20]), as well as the biofeedback responses that have significantly enriched the modelling analytical results. These insights not only the technical performance of the systems involved but also the broader landscape in which H-M cognition unfolds.

However, it is essential to underscore, and the pronounced context-sensitivity of such systems to external factors (already noted within the previous morphological modelling and H-M validation). These influences can generate interpretive ambiguities for human users and, conversely, induce overfitting or overtraining effects within the machine-learning models.

The challenge becomes even more salient in an era where increasing levels of AI autonomization will enable machines to operate not merely as supportive symbiotic partners but also as potential agents capable of shaping complex cognitive domains, including beliefs, values, and emotional states (some of them observed during CYREX 2025 as clear AI domination attempts).

The possibility of such cognitive modulation (intentional or emerging ones) definitely requires a careful ethical, technical, and regulatory consideration for the AI progress. Understanding these dynamics, particularly from the machine's perspective, needs a certain conceptualizing of a new threshold of AI sentience or even more advanced one, concerning the "General AI" idea, than the largely generic architectures and LLM currently being in the focus of AI progressive trends [21]. Developing such understanding is not only a technical endeavour but also a philosophical and societal one, calling for interdisciplinary engagement to ensure that future AI systems will

remain aligned with human well‑being and cognitive integrity in the age of digital cognition.

6 Discussion

Exploring the age of digital cognition within the next fifteen years and proactively identifying of future cybersecurity synergies and gaps is obviously a rather complex process, that studies the symbiotic digital coexistence between transhumans and smart machines, whilst dynamically reshaping joint interaction and cognition. This process extends beyond technology, driving new post-informational social realities reshaped by numerous socio‑technological transcendents. In this sense, a coordinated analytical and governance response is essential. The multistakeholders' collaboration by means of uniting scientific, industrial, and institutional expertise from one hand, and the supported by advanced AI technologies from another, can certainly provide a fast and adaptive framework for successful achieving of a resilient and secure new digital Society 6.0, majorated with AI and robots. Central moment in this discussion is the balance between rapid technological evolution and the necessity of social adaptation and regulation. As AI, smart systems & services are advancing by an unprecedented speed, human cognition still remains superior in contextual reasoning, ethical judgment, and societal integration but not on huge heterogeneous data processing. These unique human biases, extended with smart tech transformation will continue to be vital for guiding technological development and safeguarding the integrity of the new social well-being.

Toward 2040, cybersecurity must therefore be understood not only as a technical challenge but also as a socio‑cognitive imperative, ensuring that digital coexistence remains secure & resilient, being also properly regulated and progressive.

Acknowledgments. The author of this study is granting a special appreciation for the experimental base and partial funding support to the National Scientific Programme "Security & Defense". Additional gratitude for the institutional contributions is provided to EDIH "Takia", Association of the Officers in the Reserve "Atlantic", IFIP TC 14 "Entertainment Computing", and the Association for the Development of the Information Society. Distinctive thanks are further expressed to Fsas Technologies, Fujitsu for the private AI cloud tools provision support. The analytical results in the paper are also benefiting the Centre of Competence on Digitisation of the economy in an environment of Big Data-second stage, Grant No. BG16RFPR002-1.014-0013-C01, financed by the Science and Education for Smart Growth Operational Program and co-financed by the European Union through the European Structural and Investment Funds. Finally, the international expert support is further reinforced by the initiative "Securing Digital Future 21" with more than sixty countries now, spread around the world, https://securedfuture21.org/.

References

1. Z. Minchev, Future Security Issues in the Age of Digital Cognition, Softtrade, 1st edn. (2025)
2. J. Rekart , R. Baker, Designing for Human Intelligence in an Artificial Intelligence World, Apress Berkeley, CA, 1st edn. (2025)

3. P. Dutta, S. Gupta, S. Kashyap, A. Gehlot, R. Karmakar, P. Bhattacharya (eds) Emotional Intelligence in the Digital Era, 1st edn. CRC Press (2025)
4. S. Žižek, M. Mulej, A. Potočnik. The sustainable socially responsible society: well-being society 6.0. Sustainability 13(16):9186, (2021), https://doi.org/10.3390/su13169186, last accessed 2026/02/11
5. Z. Minchev, V. Tzourov, Global Security Transformation Towards 2040: Transcendents in the Age of AI, Softtrade, 1st edn. (2025)
6. A. Choudhary, Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discov Internet Things 4, 31 (2024), https://doi.org/10.1007/s43926-024-00084-3, last accessed 2026/02/11
7. S. Russell, P. Norvig (eds), Artificial Intelligence: A Modern Approach, 4th edn. Pearson (2022)
8. S. Malja, H. Afrasiabi, Artificial intelligence and society: mapping the research through a systematic review. AI & Soc (2025). https://doi.org/10.1007/s00146-025-02555-9, last accessed 2026/02/11
9. L. Ofusori, T. Bokaba, & S. Mhlongo, Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Applied Artificial Intelligence, 38(1) (2024), https://doi.org/10.1080/08839514.2024.2439609, last accessed 2026/02/11
10. E. Zaidan, I. Ibrahim, AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. Humanit Soc Sci Commun 11, 1121 (2024). https://doi.org/10.1057/s41599-024-03560-x, last accessed 2026/02/11
11. Z. Minchev, et al. Digital Transformation in the Post-Information Age, Softrade, 1st edn (2022)
12. L. Skyttner, General Systems Theory, World Scientific, 2nd edn (2006)
13. F. Vester, The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity, Munchen, MCB–Verlag, 1st edn (2007)
14. P.Chen, The Entity-Relationship Model-Toward a Unified View of Data, ACM Transactions on Database Systems, 1, 9-36 (1976)
15. F. Zwicky, Discovery, Invention, Research through the Morphological Approach, Macmillan, 1st edn (1969)
16. 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, 1 edn., M. Hadji-Janev and M. Bogdanoski, Eds., IGI Global, (2015)
17. Z. Minchev, Digital Society Future Transformation Perspectives in the Informational Age, In Proc. of 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020, 14-18 May, Kyiv, Ukraine, 381-388, (2020)
18. Conference with Cyber/HPC Training "Future Security Transformation: Synergies in the Post-Information Age, Home Page, https://bit.ly/4tBemsQ, last accessed 2026/02/11
19. Z. Minchev, Future Cybersecurity Landscape Exploration with CAX in the Age of AI, in Proc. of BISEC 2024, Nis, Serbia, Nov 28-29 (2024), CEUR Workshop Proceedings, https://ceur-ws.org/Vol-3971/short09.pdf, last accessed 2026/02/11
20. M. Arnold, M. Goldschmitt, T. Rigotti, Dealing with information overload: a comprehensive review. Front Psychol. 2023 Jun 21;14:1122200. doi: 10.3389/fpsyg.2023.1122200, last accessed 2026/02/11
21. J. Anthis, J. Pauketat, A. Ladak, A. Manoli. Perceptions of Sentient AI and Other Digital Minds: Evidence from the AI, Morality, and Sentience (AIMS) Survey. In Proc. of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25). Association for Computing Machinery, New York, NY, USA, Article 10, 1–22 (2025), https://doi.org/10.1145/3706598.3713329, last accessed 2026/02/11