Future Cybersecurity Landscape Exploration with CAX in the Age of AI

Zlatogor Minchev[1,2,*]

[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

Provisional understanding of the future cybersecurity landscape in the new age of AI is a quite challenging task due to multiple dynamic socio-technological factors. However, with the progressive development of AI technologies, the task becomes even more complex, joining both human and machine intelligence, while having different evolutionary levels of maturing. The study outlines an almost 10-year effort (since 2015) for a successful cybersecurity landscape predictive outlining with progressive identification of future socio-technological transcendents (threats, challenges, opportunities, etc.), implementing Computer Assisted eXercises (CAX) in the loop. Additionally, some generative AI elements have been recently added, trying to achieve an extended holistic analytical framework with a flexible and futuristic scenario-based exploration context. Both machine and human multimodal feedbacks have been successfully implemented in the study, bringing out a comprehensive enough monitoring & quantitative assessment of the future cyberspace evolution with the new age of AI immersion in our new extended reality of living, joining both humans and machines in a new symbiotic human-machine ecosystem.

Keywords

Cybersecurity, CAX, AI, Socio-technological dynamics, Symbiotic human-machine ecosystem

1. Introduction

Getting provisional knowledge about the future has always been a dream of human civilization. With the fast technological development of the new 21st digital century the AI technologies are already entering our new socio-technological reality, transforming it in an unprecedented manner [1, 2]. The new digitally extended & mixed world is getting more and more smart and this tendency is even expected to take an autonomous character with the not so far future of 15 years ahead with sentient & General AI [3, 4]. We are already living in the "Age of AI" [5] mostly due to deep learning & generative AI solutions presently accessed via (4G/5G mobile, wireless & satellite) with smart wearable IoTs & cloud services. The dreams of a joint human-machine symbiotic existence in the Society 5.0 [6] is already evolving towards Society 6.0 [7]. The last could significantly affect the future socio-technological dynamics due to potential domination of AI or at least dependable need of AI, due to the necessity of multiple data sources huge volume and ultrahigh speed of processing and handling towards knowledge analytical production for both humans and machines.

However, successful exploration of the future digital societies organizational concepts is becoming quite challenging due to multiple unknown issues. Apart of all these facts the future cybersecurity landscape is also evolving, whilst expected to be successfully handled with the AI assistance (though the idea could be somewhat arguable) either completely dominated with the autonomization of machine-to-machine & machine-to-human communications.

Successful identification of these cybersecurity perspectives (threats, challenges, opportunities, divides, etc., called in brief "transcendents") could significantly benefit with the joint human-machine intellect analytical & validation mixing.

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia
*Corresponding author.
†These authors contributed equally.
zlatogor@bas.bg (Z. Minchev)
0000-0003-2479-5496 (Z. Minchev)

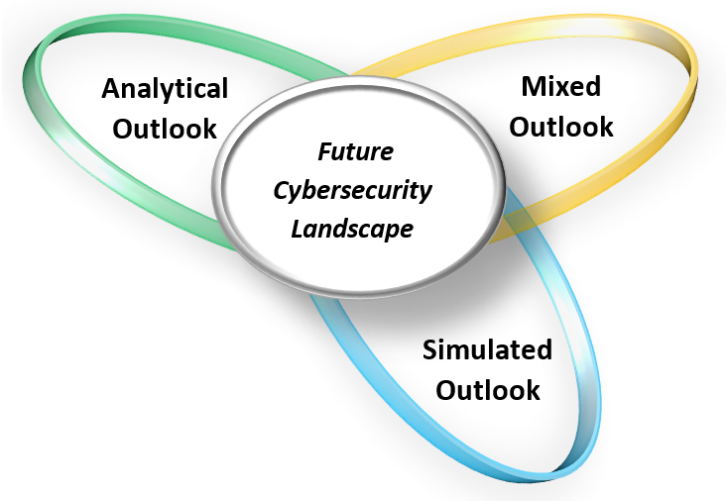


Figure 1: Comprehensive practical framework for future cybersecurity landscape exploration.

Further in the paper, an ad-hoc exploration framework successful implementations within the last 10-15 years will be given, providing also a further comprehensive viewpoint for the near future towards 2037, i.e. giving similar perspective ahead.

2. Exploration Framework

The presented framework hereafter is generalizing some of the methodological approaches, outlined in [4, 8, 9], but accentuate on three different outlooks to the problem at hand – future cybersecurity landscape multiaspect exploration via Computer Assisted eXercises – CAX [10]. As far as this incorporates live, virtual & constructive simulations, together with some computational and analytical efforts the three different outlooks (Analytical, Simulated & Mixed) have been chosen as a comprehensive enough combination with practically proven results for proactive exploration studies.

More details on the presented framework, regarding different outlooks for cybersecurity future landscape exploration will be given within the next section of the present work.

3. Implementation Details

In this section the triplet of analytical, simulated & mixed outlooks (see Fig. 1) to the future cybersecurity landscape exploration will be given in detail with selected illustrative practical examples.

3.1. Analytical Outlook

This exploration outlook combines both morphological & system analysis, while mostly relying on expert support, thus having a somewhat subjective nature in general. In brief, the analytical part relies on well-known techniques for unstructured data processing like "morphological analysis" that are modified with the idea to tailor future uncertainties and establish a scenario pool of plausible and implausible combinations in a discrete software environment, while handling uncertainty [4]. Further, the results are used for deeper system-of-systems modelling and assessment towards the future, adding causality and achieving a holistic system overview. Selected examples with this section could be outlined with CYREX 2018 & CYREX 2023, considering the future smart homes & smart cities with further system sensitivity analysis and prognostic findings.

Both studies clearly outline aggregated future trends for AI autonomization and mixing with infrastructure, producing numerous smart services. Apart of this, future people are also transforming with AI-assisted capabilities, concerning future homes and cities. This however has a dual nature establishing

Morphological Analysis

Devices	Activities	Communication Medium	Environment Characteristics	Human Factor Characteristics
Mobile Smart Devices	Entertainment	Cable Networks	Physical	Bioelecrics
Home Entertainment Systems	Communication	Wireless Networks	Structural	Spacial
Home Automation Systems	Everyday Work	Social Networks	Functional	Sensual
	Household Support			

Index	Length	Weight	Name
1	5	170	Scenario1
2	5	125	Scenario2
3	5	265	Scenario3
4	5	145	Scenario3
5	5	195	Scenario4
6	5	195	Scenario5
7	5	140	Scenario6
8	5	160	Scenario7
9	5	210	Scenario8

Active scenarios +

Passive scenarios -

(a)

Morphological Analysis

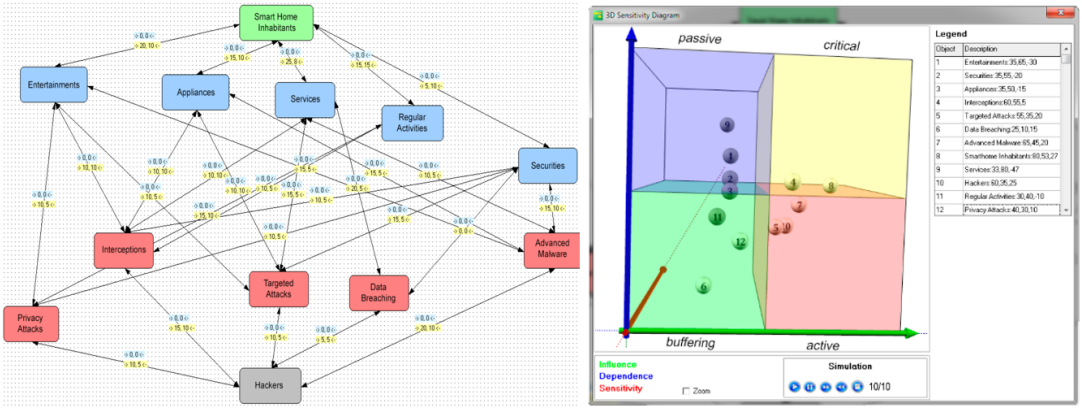
Drivers	Threats	Measures	Ambiguities	Objectives
Mixed Intellect	Reality Mixing	Tech Limiting	Smart Resources	Resilient Future Cities
Climate Changes	Smart Dual Apps	AI Overwrite	Privacy Concerns	Energy Independence
Quality of Life	Lifestyle Machine Control	Legal Issues	New Smart Activities	Transformed Security
	AI Autonomization		Infrastructure Smart Services	Transformed Citizens

Index	Length	Weight	Name
1	5	5	Scenario1
2	5	30	Scenario2
3	5	55	Scenario3
4	5	-5	Scenario4
5	5	10	Scenario5
6	5	-35	Scenario6
7	5	5	Scenario7

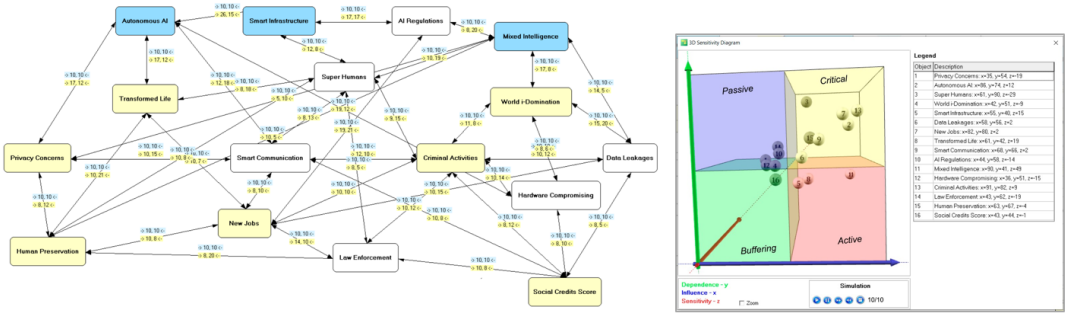
Active scenarios +

Passive scenarios -

(b)



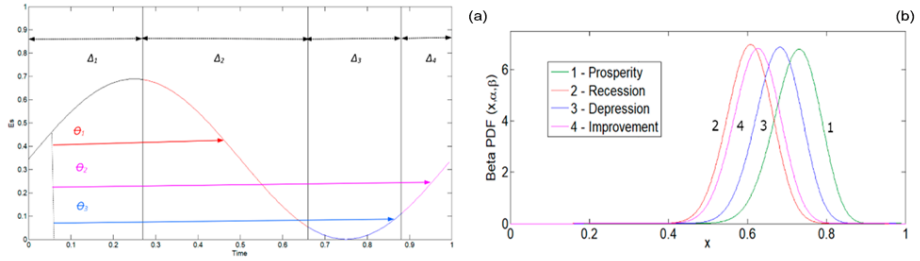
(c)



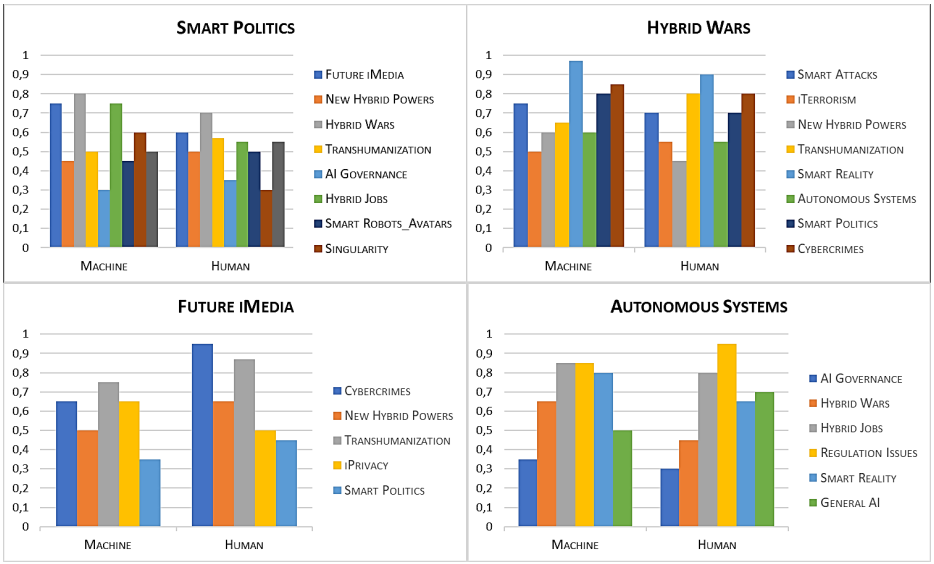
(d)

Figure 2: Future smart homes (a) & smart cities (b) coss-consistency matrices (with respectfully N1= 1620 & N2 = 2880 scenarios) and resulting system models with sensitivity analysis diagrams (c), verified with CYREX 2018 & CYREX 2023 events [11, 12].

at the same time a smart cyber security landscape with dual offensive and defensive roles for both humans & machines. Though sounding quite sci-fi-oriented these findings are already getting visibility with AI progressive implementations. So, some further results' dynamic assessments, adding machine algorithms intelligence together with the human ones will be presented next.



(a)



(b)

(c)

Figure 3: Socio-technological S-shaped curve quantum representation & resulting four-stages probabilistic assessment idea (a), after [4]; multicriteria malicious use of AI [15] & future smart cities security issues system models (b) [16] (c) from human – H & machine – M perspectives, towards year 2037.

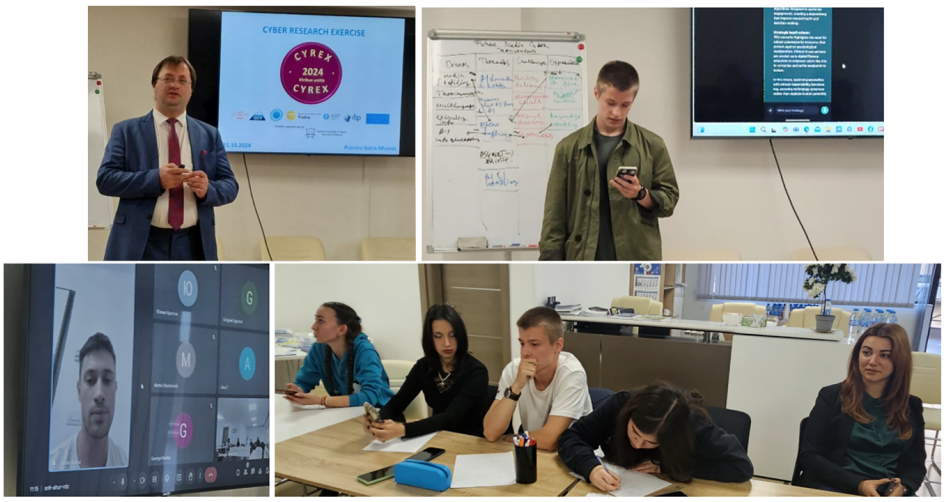
3.2. Simulated Outlook

Being somehow static the outlined analytical findings in Section 3.1 are explored also dynamically taking in to account the ideas from [13, 14]. In brief, the accomplished ideas could be aggregated on each of the system model relations with an S-shaped probabilistic exploration. The last is approximated using Quasi-Monte Carlo scenario-based integration within the four stages (assuming the Kondratiev's society dynamics assumptions) of evolution [4]. Whilst this approach is quite useful, some unexpected events as transitional jumps (to mark COVID-19 or other unexpected man-made either natural cataclysms) have been recently added, taking the quantum tunneling ideas practical use, assuring simulation of interstages jumps [4].

3.3. Mixed Outlook

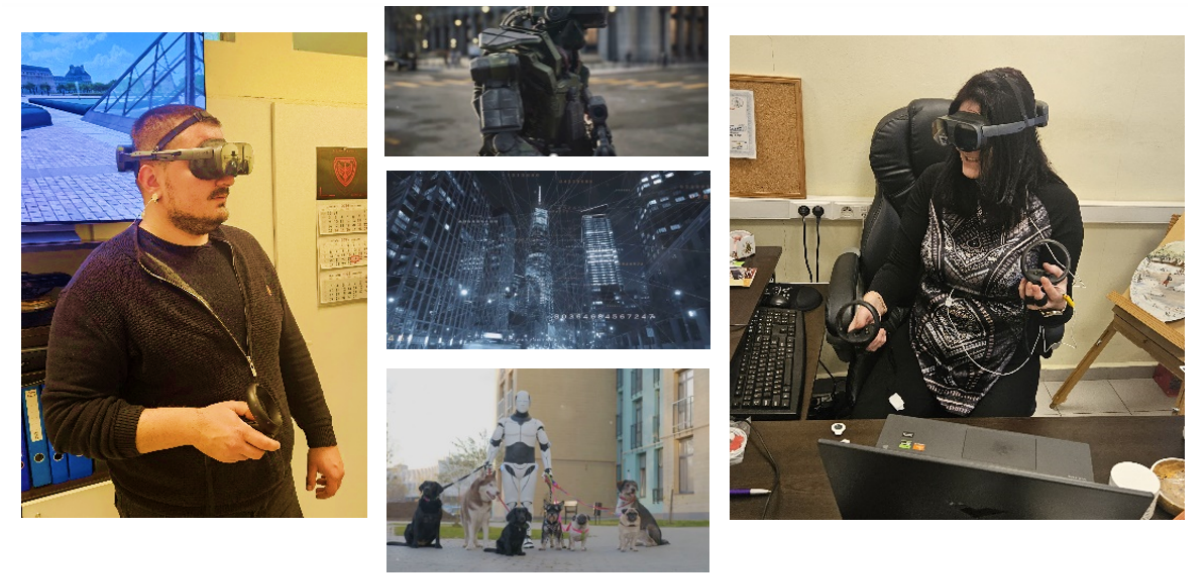
The organization of this stage is quite complex as it combines both (i) messages exchanged amongst the CAX participants (following an agent-based multirole architecture), together with their (ii) engagement & response assessment within the training process (measured by a battery of psycho & biometrics). Additionally, with the progressive development of AI, (iii) generative & indexing smart tools have been also recently implemented from a machine perspective. Social verification (because of the prognostic nature of the task) is also applicable via different events like workshops, summer schools, conferences, etc. (see e.g. [17]) Some recent illustrations of the above-mentioned mixed outlook, taking the CYREX 2024 organization [18], extended reality verification mini-lab (with heart rate, respiration, GSR set dynamics with HTC VIVE XR Elite & Bitalino/Plux wearable biomonitoring box, i.e. and IoT device) and joint human-machine multicriteria assessment, following the experience with [16], but adding also ChatGPT generative AI feedback are given below.

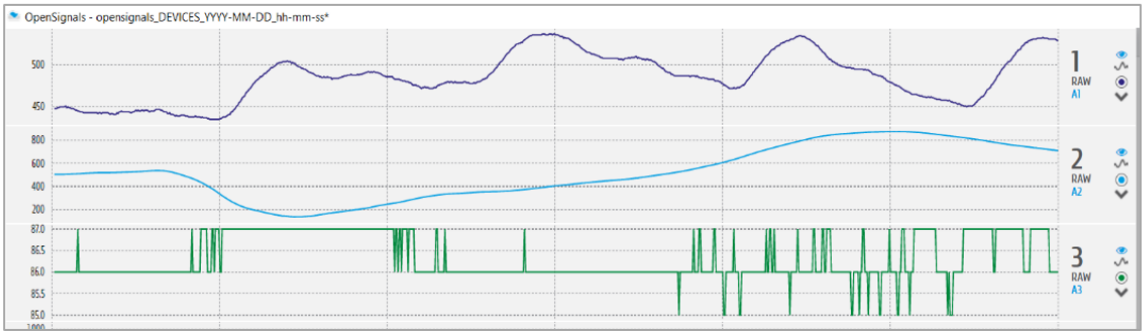
(a)



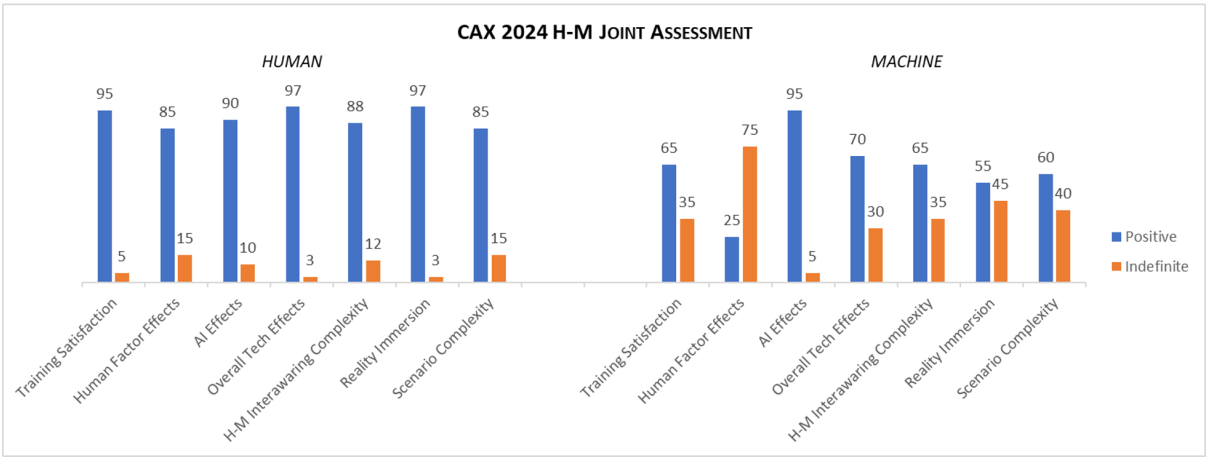
(b)

Figure 4: Selected moments from CYREX 2024 organizational architecture (a) & training process (b).





(a)



(b)

Figure 5: User-based verification in XR of the futuristic training scenario with biometric battery assessment (a); Joint H-M multicriteria aggregated assessment results of the exercise.

What is important to note here is the presence of AI within this mixed outlook stage. This actually should be taken with the assumption for human extensive control. In any case, it is important to note that both AI-generated scenarios (for CYREX 2024 & the Society 6.0 context, by Invideo AI) demonstrate constant striving algorithmic subjectiveness towards machine domination. It should be noted that the AI-observed data was taken completely from human recent discussions during "Digital Transformation in the Age of AI" training at SRS'2024 [19]. Apart of these, the event assessment amongst the participants and via AI was also somewhat challenging as the machine-generated responses have a

different, autonomous viewpoint, even with exclusive human interests' context requesting.

4. Discussion

Properly understanding the future cybersecurity landscape certainly requires a complex outlook from both static and dynamic analytical perspectives. In this sense however, it is extremely important to note the role of AI that if it becomes out of control could find a dominant position, especially with the generation of completely unknown, or very uncommon new cyber threats, either inclined feedback results. Luckily, the process is still dominated by the human intellect and could be significantly supported with AI assistance that has no-dominative behavior, i.e. semiautonomous AI, and completely takes the human beings leading decision-making & responsibility position. Whether this position is right or wrong is a really philosophical moment that from a technical perspective has no particular meaning, at least for the present technological level of our new digital society aiming for joint symbiotic human-machine co-existence.

Acknowledgements

The study is granting special appreciation for the extended reality mini-lab establishment and further exploration funding support to the National Scientific Programme "Security & Defense". Additional gratitude for the international expert support is given to EDIH Trakia & the initiative "Securing Digital Future 21" with more than sixty countries now, spread around the world, https://securedfuture21.org/.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] G. Leonhard, Technology vs. Humanity: The coming clash between man and machine, FutureScapes Lodge, UK, 2016.
[2] Y. N. Harari, Nexus: A brief history of information networks from the stone age to AI, Signal, 2024.
[3] R. Kurzweil, The singularity is nearer: When we merge with AI, Penguin, 2024.
[4] Z. Minchev, et al., Digital transformation in the post-information age, Institute of ICT, Bulgarian Academy of Sciences & Softtrade (2022).
[5] H. A. Kissinger, E. Schmidt, D. Huttenlocher, The age of AI: and our human future, Hachette UK, 2021.
[6] G. Wahlers, The Digital Future, 1, International Reports, Konrad Adenauer Stiftung, 2018. URL: https://goo.gl/8CLcvn.
[7] S. Bousri, Embracing society 6.0: A technological renaissance for human living and economies, 2023. URL: https://www.linkedin.com/pulse/embracing-society-60-technological-renaissance-human-living-bousri-1f/.
[8] Z. Minchev, L. Boyanov, et al., Future digital society resilience in the informational age, Sofia: SoftTrade & Institute of ICT, Bulgarian Academy of Sciences (2019).
[9] Z. Minchev, Proactive identification of future cyber threats., in: BISEC, 2022, pp. 42–49.
[10] 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.
[11] CYREX 2018, Cyber research exercise 2018, 2018. URL: https://securedfuture21.org/cyrex_2018/cyrex_2018.html.
[12] CYREX 2023, Cyber research exercise 2023 - clip, 2023. URL: https://youtu.be/m7mTfvtmtFc.

[13] K. R. Dark, The waves of time: long-term change and international relations, Bloomsbury Publishing, 2016.
[14] D. Meadows, J. Randers, D. Meadows, A synopsis: Limits to growth: The 30-year update, Estados Unidos: Chelsea Green Publishing Company 381 (2004).
[15] Z. Minchev, Malicious future of ai: transcendents in the digital age, in: The 12th International Conference on Business Information Security (BISEC-2021), 2021, pp. 18–22.
[16] Z. M. Minchev, L. Boyanov, Future of smart cities security challenges – proactive modelling & identification, in: The 14th International Conference on Business Information Security (BISEC-2023), 2024, pp. 12–17.
[17] Web Forum Initiative, Secure digital future 21, 2024. URL: https://securedfuture21.org/.
[18] CYREX 2024, Cyber research exercise 2024, 2024. URL: https://securedfuture21.org/cyrex_2024/cyrex_2024.html.
[19] Digital Transformation in the Age of AI, Video Report, SRS'2024, Varna, Bulgaria, 2024. URL: https://youtu.be/xnXkrPkgrDQ.