# Future of Smart Cities Security Challenges – Proactive Modelling & Identification

Zlatogor Minchev[1,2,*], Luben Boyanov[3]

[1]Institute of ICT, Bulgarian Academy of Sciences, Acad. Georgi Bonchev Str., Bl. 25A, 1113 Sofia, Bulgaria
[2]Institute of Mathematics & Informatics, Bulgarian Academy of Sciences, Acad. Georgi Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria
[3]University of National & World Economy, 8-mi Dekemvri Str. 19, 1700 Sofia, Bulgaria

**Abstract**

Joining technologies & people in future smart cities infrastructure by merging sensors, effectors and intelligence is going to create a rather challenging mixed reality transformation. In this sense, the competition between natural and artificial intelligence is inevitably establishing quite new and interesting society overlaying of humans and technologies with federated domination areas. The results are presently addressing the digital society transformation towards Society 5.0, whilst outreaching the next Society 6.0 expectations. The paper is going to outline a comprehensive analytical intelligence framework (i-framework) for studying the problem, adding a scenario-based proactive analysis, combined with system modelling and results hybrid multicriteria validation. The intelligent part comes from different AI models that are implemented in the process, giving supportive and generative added values. Finally, a concluding discussion on the outlined findings is presented.

**Keywords**

Future smart cities, digital society transformation, security challenges, scenario-based analysis, system modelling, hybrid multicriteria validation

## 1. Introduction

Digital transformation is expected to affect in practice all fields of future society reality, including people and their residence area, adding also biotope dynamics (to note: climate changes, species migration, natural disasters, etc.) [1]. As for the new urban environment of future smart cities, the process is certainly expected to combine new IoTs & AI, providing innovative commodities, services (to mark: transportation, deliveries, education, governance, media, energy supplies, assistance, medicine, economics) and jobs for the citizens, aiming the horizon towards the year 2050 [2]. New smart gadgets' autonomous integration (multifunctional robots, vehicles, etc.) with the vastly interconnected reality (due to broadband wireless meshes & optical network technologies enhanced usage) will additionally advance the new habitual digital landscape [3].

Thus, the digital change towards the post-information age is expected to have both - positive and negative transformational effects on the new Society 5.0 idea [4]. The situation is getting even more complicated with Society 6.0 transcends exploration [5], where AI and machine singularity are expected to appear in practice.

So, new technologies are going to establish a digital divide between citizens in the smart urban reality and the rest of the populated areas. They are going to be considered as a new digital class with advanced capabilities but will be also challenged via joint human-machine threats in the smart habitat [6]. This definitely will affect future jobs and culture transformation, together with deeper smart machines, sensors and algorithms integration in the transformed people's lifestyle and environment smart reshaping. In this context, the security, privacy and ethical issues require an adequate and smart exploration approach that is proactively organized as to be earlier prepared as a civilization for this change.

Further, an exploration methodological approach in this context is going to be outlined, combining both natural and artificial intelligence with expert analytical support.

## 2. Analytical "i-Framework"

Combining human & machine intellect into a joint analytical power is practically extending some of the ideas from [1, 7] into a new "i-framework" (see Figure 1), better applicable to the digital future security dynamics, and comprehensive proactive exploration.

The extension was organized due to the vast dynamics' escalation with AI & IoTs immersion in the post-information age, as stated in the introductory part of the paper that is difficult to be easily handled due to the scale and dynamics with human only intellect.

While aiming proactive identification and comprehensive analysis of digital transformation security in general,

*BISEC'23: 14th International Conference on Business Information Security, November 24, 2023, Niš, Serbia*
*Corresponding author.
zlatogor@bas.bg (Z. Minchev); lboyanov@unwe.bg (L. Boyanov)
0000-0003-2479-5496 (Z. Minchev); 0009-0006-2292-0619 (L. Boyanov)
© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3676/short_02.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

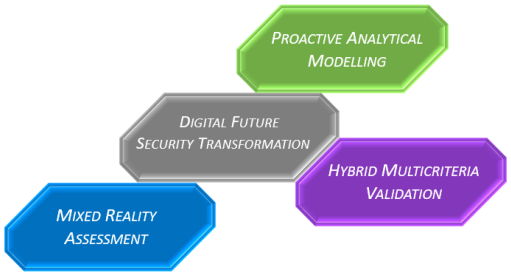


**Figure 1:** Analytical "i-framework" for digital future security proactive exploration.

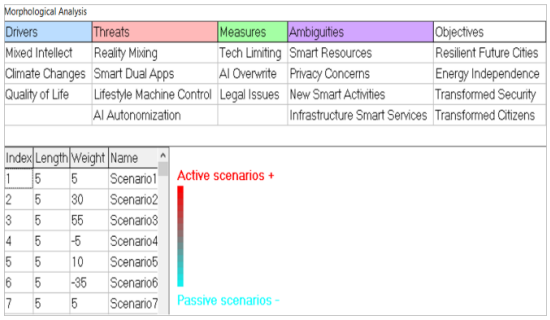


**Figure 2:** Future smart cities security transcendents towards year 2037.

the current "i-framework" implementation is addressing the future smart cities in particular. Being a broad landscape example for security dynamics studying with people & technologies digital transformation, the outlined findings could be further used with the broader digital society evolution deeper exploration.

Further in the paper a detailed illustration of the trilateral "i-framework", concerning (2.1) Proactive Analytical Modelling, (2.2) Hybrid Multicriteria Validation & (2.3) Mixed Reality Assessment will be given for the future smart cities' comprehensive security challenges context exploration.

## 2.1. Proactive Analytical Modelling

Achieving proactive analytical modelling is combining both morphological and system analysis approaches. A starting implementation of the scenario method, with expert and reference data, towards the establishment of plausible and implausible scenario combinations is accomplished. The result is a cross-consistency matrix $M$, containing three types of scenarios, in accordance with their Relative Common Weight – $RCW$: Active (tangible), Passive (intangible) & Neutral (probably most uncertain) [8]. With the present study on future smart cities, the particular matrix context towards year 2037 and post-information society of 136080 scenarios [1] has been zoomed for smart cities security topic, with a total scenario number $N* = 2880 (N* = 5 \times 3 \times 4 \times 3 \times 4 \times 4$; plausible – $N1* = 86$ & implausible ones – $N2* = 2794$; from $N1*$ are additionally selected: Active, i.e. – "tangible" $(76, RCW > 0)$ & Passive, i.e. – "intangible" $(10, RCW < 0)$.

As this landscape shows quite an uncertain future with mostly implausible scenarios, a deeper analytical causality exploration has been performed toward smart city system sensitivity analysis.

A "system-of-systems" modelling paradigm over an i-fuzzy weighted graph-based "Entity – Relationship" representation in I–SCIP-SA environment [9] has been performed.

Taking an aggregated analytical representation into a "3D Sensitivity Diagram" – "3D SD" with Influence – x, Dependence – y & Sensitivity – z, due to relations i-fuzzy weights, concerning future smart cities security towards year 2037 (simulated in 10 steps) is finally achieved with 16 entities (addressing social – yellow, technical – blue & mixed – white aspects) & 41 bi-directional relations model (see Figures 3 and 4).

The resulting classification gives four classes for the model entities distribution (with two subclasses for each: Active – white & Passive – grey) in the 3D SD diagram as follows:

*Buffering* (in green): "Social Credits Score" – 16, being at the same time Passive.

*Active* (in red): "Smart Infrastructure" – 5, "Transformed Life" – 8, "Mixed Intelligence" – 11, all being Active.

*Critical* (in yellow): "Super Humans" – 3, "Human Preservation" – 15, both being Passive & "Autonomous AI" – 2, "Data Leakages" – 6, "New Jobs" – 7, "Smart Communication" – 9, "Criminal Activities" – 13 all being Active.

*Passive* (in blue): "Privacy Concerns" – 1, "World i-Domination" – 4, "AI Regulations" – 10, "Hardware Compromising" – 12, "Law Enforcement" – 14 all being Passive.

Further, the presented quantitative classification results could be aggregated in more detail, around several key findings:

(i) That future smart cities will create numerous threats and challenges from their critical infrastructure perspective [10], that could be attacked with different vectors: communicational, data & hardware ones. Apart of this, the future superhumans will have a somewhat ambiguous role with new technologically extended capabilities. So, insider security threats are neither to be completely excluded or added by default due to potential technological

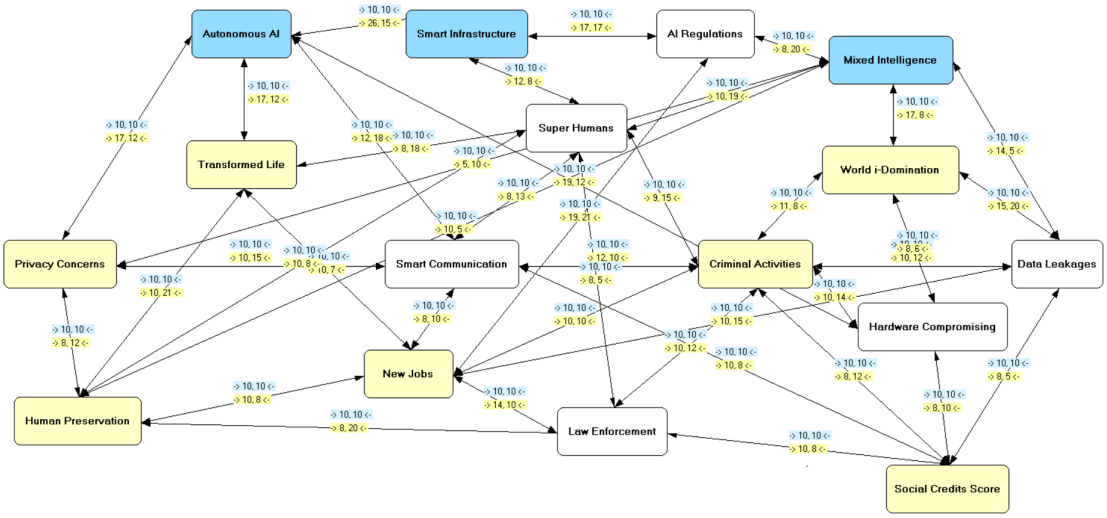


**Figure 3:** Future smart cities security transcendents of a discrete system-of systems model.

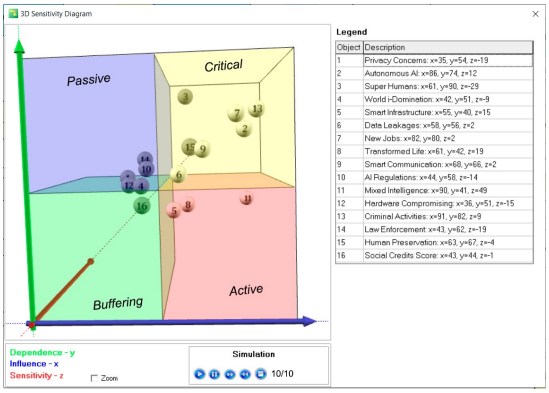


**Figure 4:** Resulting 3D SD analytical assessment towards year 2037.

influence.

(ii) New jobs and ambitions for intelligent world domination will certainly appear and progress both from positive and negative (criminal, manipulative) perspectives, adding AI & IoT with new capabilities and challenges;

(iii) Mixing artificial and natural intelligence for future smart cities' security could be quite beneficial except if a superintelligence with negative objectives manages to compromise the system due to emergency external influences (natural or man-made disasters).

(iv) Keeping privacy and humanity present understandings will be quite different for the future as the role of AI & IoT transformation will also demand new ethical and social boundaries.

All these findings will hopefully omit the dystopian scenarios with machine-controlled social credits and behaviour that normally are a question of culture and social system respect, whilst trying to keep a non-authoritarian but secured future urban reality.

As the presented expert findings are mostly based on expert analytical beliefs, further AI-assisted validation and assessment will also be given, trying to achieve a comprehensive urban security landscape exploration.

An overall evaluation of the exercise has been performed by the participants (with Positive either Indefinite judgment marks) via a q-based survey, giving feedback for: reality, scenario & interawaring complexity, AI & human factor roles, training satisfaction (see Figure 6).

Being somewhat subjective the obtained results could be also enriched with biometric & simulation assessments (see [1, 9]) and finally combined within the system model. More details on these ideas will be given further.

## 2.2. Mixed Reality Assessment

The mixed reality assessment of the accomplished analytical findings (see Section 2.1) was further conducted, using a transformed reality interactive simulation, organized in the framework of CYREX 2023 [11]. Assuming a fictitious scenario events script (generated with human intellect guiding & tailoring Open AI ChatGPT results), interactively played (for about 180 minutes) from the trainees in several multirole teams, an exploration of future smart cities security transendents was performed.

The main objective of CYREX 2023 exercise was to test the human-machine inter-awareness in an imaginary context, concerning the future smart cities mixed reality from different aspects (both utopian and dystopian


**Figure 5:** Selected moments (a, b) & organizational architecture (c) of CYREX 2023 [11].

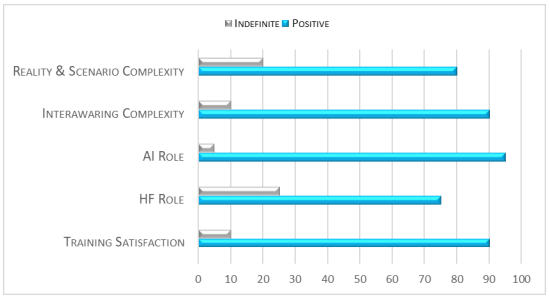


**Figure 6:** Aggregated participants' q-based assessment of CYREX 2023.

ones), concerning the cyber security area different aspects: technological, social, infrastructural, security, political, governance, diplomatic. The idea was to develop and test a set of morphological and system models for the not-so-far future (10-15 years from now), among young

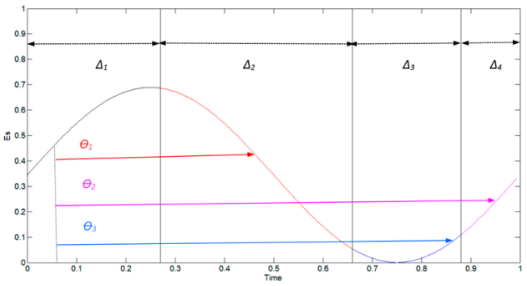


**Figure 7:** Socio-technological S-shaped curve quantum representation, after [1].

people (Y- & Z- generations), joining both human and machine intelligence in the process of decision-making and scenario development, while using a role-based organization, multiple smart gadgets (smartphones, laptops, advanced PCs, smart TVs & interactive screens) and platforms (Windows, Android, iOS). The training was illustrated, combining results of artificially generated images, videos, sounds and popular multimedia clips (assisted with Gencraft, beatovenAI & invideoAI). The approach allows studying of complex security transcendents dynamics in a futuristic mixed reality smart ecosystem, giving excellent training feedback results, especially at organizational and operational levels.

## 2.3. Hybrid Multicriteria Validation

The main idea for this section is to combine both human and AI expectations for the future of smart cities' security, taking as a base the presented in 2.1. Analytical i-Framework findings in the dynamic context. So, a joint smart approach has been further accomplished, adding human beliefs vs machine-adaptable smart multicriteria optimization [10]. In this manner, it is possible to get a feasible evaluation of potential future expectations, taking into account trends S-shaped dynamics, but with unplanned jumps (see Figure 7) that could be best explained with quantum tunnelling effect stochastic socio-technological modelling of system model relations dynamics [1].

Selected multicriteria near future illustrative critical entities (towards the year 2037, see Figure 8), concerning the system-of-systems discrete model of smart cities security transcendents (see Figure 3) are further presented, taking the risk-assessment approach from [12], but using a percentage-based measuring scale.

So, taking society the system-of-systems model ideas is quite intriguing as normally the model is both subjective to the expert beliefs and at the same time – limited due to the preliminary analytical assessment. In this sense, the validation process has been extended with

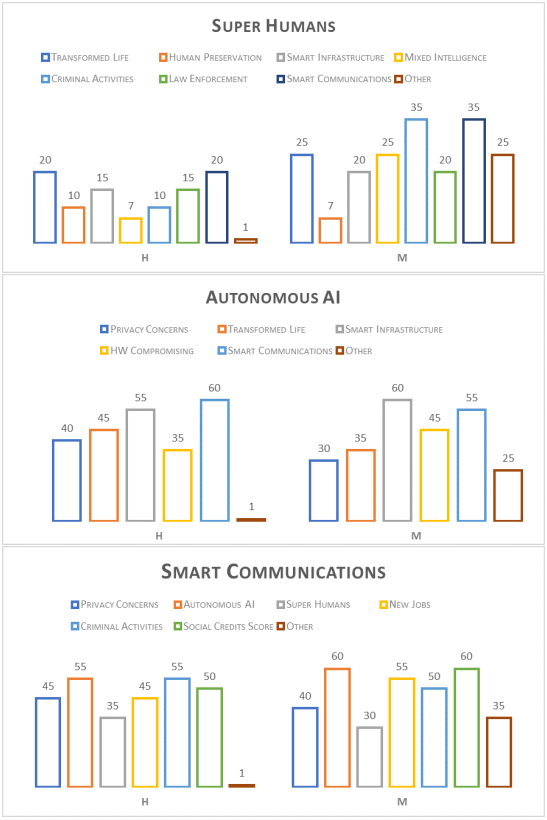


**Figure 8:** Selected multicriteria smart cities security future entities illustrative assessment (after Figure 3) from human – H & machine – M perspectives towards 2037.

"Other" additional relations and entities. This additional extension could be produced from both human and generative AI hints and supplementary human discussions. With the presented illustrative examples an added human opinions value has been taken from SRS'2023 young international participants in the context of Society 6.0 [13]. The machine-generated added value was produced by taking Open AI ChatGPT feedback with the human responses' extension, towards machine domination, concerning smart cities' security near future evolution.

## 3. Conclusion

Proactively identifying the future smart cities' security challenges is a quite complex task that could benefit from both human and machine intelligence joint efforts. Going deeper in the problem normally requires a suitable framework as has been already shown in the present study. Whilst human intelligence is always subjective by nature responsive biometric feedback could be quite helpful with the analytical models' more detailed assessments. As for the role of AI, it is still at an early stage of development and the dream for a "General AI" is still quite limited. However, it should be honestly marked that the generative AI on the other hand, is quite supportive in the analytical assessment and experimental issues. Thus, providing both a neutral opinion advisor and a rapid prototyping tool that facilitates the exploration efforts' proactive nature a lot. This clearly shows a positive technological trend for the not so far digital future new social evolution.

## Acknowledgment

The results presented in this study are due to the technological, industrial and expert support obtained in the framework of the international forum initiative "Securing Digital Future 21" with more than sixty countries now, spread around the world, https://securedfuture21.org/

## References

[1] Z. Minchev, et al., Digital Transformation in the Post-Information Age, 1st Edition, SoftTrade & Institute of ICT, Bulgarian Academy of Sciences, Sofia, 2022.

[2] United Nations, Envisaging the Future of Cities, World Cities Report 2022, UN Human Settlements Programme, https://unhabitat.org/, 2022.

[3] L. Boyanov, igital World – The Change, 1st. ed., Avangard Prima, Sofia, 2021.

[4] G. Wahlers (Ed), The Digital Future, International Reports, Konrad Adenauer Stiftung, No. 1, https://goo.gl/8CLcvn, 2018.

[5] S. Bousri, Embracing Society 6.0: A Technological Renaissance for Human Living and Economies, Elit Web3 Solutions, https://www.linkedin.com/pulse/embracing-society-60-technological-renaissance-human-living-bousri-1f/, 2023.

[6] United Nations, Addressing the Digital Divide Taking Action towards Digital Inclusion, United Nations Human Settlements Programme (UN-Habitat), https://unhabitat.org/programme/legacy/people-centered-smart-cities/addressing-the-digital-divide, 2021.

[7] Z. Minchev, Proactive identification of future cyber threats, in: Proceedings of the 13th BISEC Conference, 2022, pp. 42–49.

[8] Z. MINCHEV, Future transformational outlook for the digital society and economy, Romanian Cyber Security Journal. Fall 2 (2021) 25–37.

[9] Z. B. Minchev, Human factor role for cyber threats resilience, in: Handbook of Research on Civil So-

ciety and National Security in the Era of Cyber Warfare, IGI global, 2016, pp. 377–402.
[10] Z. Minchev, Security challenges to critical infrastructure of future smart cities, in: Proceedings of the 9th BISEC Conference, 2019.
[11] CYREX 2023 Multimedia Clip, https://youtu.be/m7mTfvtmtFc, 2023.
[12] Z. Minchev, Malicious Future of AI: Transcendents in the Digital Age, in: Proceedings of the 12th BISEC Conference, 2019, pp. 18–22.
[13] International Research Summer School on Mathematics & Informatics - SRS'23, Multimedia Report, https://www.globaldiplomatic.eu/post/international-research-summer-school-on-mathematics-informatics-srs-23, 2023.