29

# ON THE GROWING TRANSFORMATIONAL ROLE OF AI TECHNOLOGIES FOR THE FUTURE CYBER DIPLOMACY IN THE POST-INFORMATION AGE

Zlatogor MINCHEV Institute of ICT, Bulgarian Academy of Sciences zlatogor@bas.bg

**Abstract:** The modern post-information society's future evolution is inevitably addressing AI technological disruption in the human-machine interactions, establishing also a new style of political, governmental and diplomatic relations between both state and non-state actors connected by the cyber domain and assisted by new technological capabilities. The paper suggests a proactive multiperspective exploration framework on the future cyber diplomacy, aiming at the next 10-15 years. A comprehensive combination of expert, reference and dynamic interactive analytical modeling of future transcendents (adding both morphological & system problem representations) with simulations in mixed reality multiple assessments (joining AI and human biometric feedbacks) for the future is accomplished. Finally, a wrap-up discussion on the results' meaning for the upcoming post-information society from cyber diplomacy, political and governance perspectives is presented. **Keywords:** Post-Information Society, Digital Transformation Transcendents, Future Cyber Diplomacy, Multi-Perspective Exploration Framework, Mixed Reality Simulated Assessment

# **INTRODUCTION**

Properly understanding the future of cyber diplomacy (the term is also known as "digital diplomacy" or "e-diplomacy", though having different nuances excluding governance but implementing technological assets (Sandre, 2015, Riordan, 2019)) certainly requires a better understanding for advanced human-machine interaction, assisted by AI technologies. The reasons for that have both a technological and social nature. The progressive development of narrow AI is giving possibilities for cloud and edge processing of huge data resources, and thus provides indirect capabilities for obvious and hidden knowledge extraction (Russell & Norvig, 2021). The result of the use of this knowledge is to generate future prognoses with multiple information sources, ensuring fake information detection and that of manipulation from the mainstream of the new hypermedia-enriched social environment (Minchev, 2022b).

These facts, together with the evolutionary development towards a "Sentient AI" (Bhaumik, 2018) and in the not-so-far future – "General AI", going next to the establishment of "Superintelligence" (Bostrom, 2014, Shanahan, 2015) are naturally leading to the necessity for a deeper technological symbiosis with present human cognitive and intellectual skills, especially in fields like: intelligence, espionage, negotiations and decision-making under uncertainty, i.e. real-life diplomatic situations (Kissinger, Schmidt & Huttenlocher, 2022).

In the post-information age (Minchev et al, 2022) of joint human-machine knowledge integration fostered by recent COVID-19 pandemic effects (Schwab & Malleret, 2020), the new mixed reality is integrating multiple IoTs (wearables, sensors, etc., (Boyanov, 2021)), both in humans (aiming "advanced humans" or "transhumans", (Bohan, 2022)) and smart



infrastructure (encompassing AI algorithms for monitoring & control) with this new hybrid knowledge (due to joint human-machine data and information processing) in a holistic, digital ecosystem for diplomacy and security transformation (Minchev, 2021a).

The "shifted cyber diplomacy" effects (Minchev, 2021b), resulting from the disruptive pandemic role, are already challenged by the dynamics of future war (Raphael et al., 2020, Ryan, 2022). Around the old hot points of contradictions, new ones are added (GRR, 2023). Here, a special attention has to be given to the recent escalation of the Russian-Ukrainian military conflict (considered even in some analyses as a potential World War III debut scenario, (Osmolovska & Maksak, 2022)) with severe resulting global impacts (Plokhy, 2023) and the objective for a new world order initiation in this sense (as was predicted by Club of Rome about half a century ago (Meadows, Meadows, Randers & Behrens III, 1972)). An enormous quantity of fake information artifacts, espionage, and media manipulation activities (Farwell, 2020, Minchev, 2022b, Nehring & Sittig, 2023) has been generated in this context, joining the information and communication assets to the diplomatic ones in this new 5D modern warfare context (Allen, Hodges & Lindley-French, 2021). Here it should be noted that some analyses on this topic claim a dystopian future of an AI-dominated world with authoritarian organization, while others are quite optimistic and utopian as people are expected to live in peace and harmony with technologies, having no contradictions (Randers, 2012, Leonhard, 2017, Harari, 2017, Tegmark, 2017, Lennox, 2020, Schwab & Mallert, 2022).

And how to cope properly with this new, rather complex mixed reality is a quite challenging task, especially with the prospect of future disruptions. Further on, the paper will outline an exploration framework for experimental proactive handling of the marked diplomatic, technological and mixed transformational transcendents identification, towards the not so-far-future of the sentient AI age.

# **EXPLORATION FRAMEWORK**

The ideas in the current framework are following the ones for the post-information age foresight analysis recent aggregated study (Minchev, 2022a), but are taking a trilateral outlook from modeling, simulation and analytical perspectives. Whilst this rather aggregated framework is comprehensive enough, a lot of implementation details have to be added, trying to clarify some uncertainties and bottlenecks on the problem of interest, but – future cyber diplomacy.

The future cyber diplomacy tasks for the digitally transformed world are expected to merge regular diplomacy with technologies in a multilateral manner (Riordan, 2019), establishing a more dynamic, but somewhat unstable and uncertain (though requiring agility and adaptability) future political environment (Susskind, 2018). This will give some advantages to those players on the international political board that will proactively use new cyber technologies (Kissinger, Schmidt & Huttenlocher, 2022), being able to get advanced information (from different channels and huge levels of data processing), whilst keeping a relevant and comprehensive enough joint human-machine security level, ensuring a resilient new digital society, and finally taking more relevant and proactive decisions, assisted with the future sentient AI.

As far as in all three framework perspectives a joint human-machine symbiosis is naturally assumed, the new cyber domain normally gets higher popularity due to both technological progress and AI autonomization, establishing the smart ecosystem of the future society, and requiring at the same time an adequate approach for comprehensive proactive exploration and handling.





Figure 1. A trilateral exploration framework of future cyber diplomacy experimental handling, adapted from (Minchev, 2022a).

# **IMPLEMENTATION DETAILS**

Further on, some implementation details of the outlined trilateral exploration methodology are going to be presented, adding important specifics and illustrations to the obtained results, together with explanatory discussions. What is important to note here is the natural overlapping between framework perspectives that are actually showing different accents and proactive findings for the future cyber diplomacy towards the year 2037, when the post-information society of knowledge is expected to be reached with the digital transformation evolutionary changes (Minchev et al, 2022).

### **Modeling Perspective**

Defining a suitable cyber diplomacy exploration modeling perspective requires structuring, scale and details observation of the future post-information society, that could be achieved by combining both scenario-based morphological and system analytical model representations. The idea is to initially establish a pool of plausible and implausible future scenarios that are created and evaluated by expert and reference data values fusion in I-SCIP-MA environment, following the ideas of (Minchev, 2015). The actual result is extending the comprehensive post-information age expectations from (Minchev et al., 2022) with the ones of shifted cyber diplomacy (Minchev, 2021b) tailored in particular for the future mixed human-machine context.

Morph	ological Ana	alysis							
Driving Factors		rs	Digital Challenges	Digital Adversaries	Digital Divides	Digital Opportunities	Digital Ambiguities	Future Contradictions	Future Cyber Diplomacy
Smart Innovations		tions	Joint H-M Regulations	Total Digitalisation	Transhumanisation	Technological Progress	Environment Integrity	H-M Clash	iEspionage
Reality Mixing			Smart Economy	Hybrid Securing	Resources Access	Mixed Ecosystem	Growth Bounding	Social Devolution	Smart Negotionations
Social Dynamics		ics	Societal Resilience	Biohacking	Smart Services	Transc People_Society	Context Overlaying	H-M Fostered Evolution	Strategic iCommunications
Climate Changes		ges	Social Behaviour	Parallelism	Governance_Quality of Life				Intelligent Decision Making
Total Connectivity		tivity	Information Overload	Machine Domination					
Exo Impacts			Huge Data						
Index	Length	Weig	ht Name 🔺						
1	8	42	Scenario1 Activ	e scenarios +					
2	8	42	Scenario2						
3	8	-41	Scenario3						
4	8	2	Scenario4						
5	8	12	Scenario5						
6	8	47	Scenario6						
7	8	-26	Scenario7 Pass	ive scenarios -					

Figure 2. Digital transformation and cyber diplomacy future transcendents cross-consistency matrix, towards 2037, extended with (Minchev et al, 2022), developed in I-SCIP-MA environment.

Finally, an eight-dimensional space of mutually exclusive alternatives, connected with weighted relations (using the Relative Common Weight – RCW idea (Minchev, Boyanov, & Georgiev, 2013)) is built, following the logical scenario structure of: "driving factor" -> "digital challenge" -> "digital adversary" -> "digital divide" -> "digital opportunity" -> "digital ambiguity" -> "future contradiction" -> "future cyber diplomacy".

A three-type scenario classification is assumed: "tangible", RCW > 0, "intangible", RCW < 0, and "neutral" ones, RCW = 0, outlining a futuristic view of the cyber diplomacy exploration context.

The total scenario number is N = 622080 (resulting from the multiplication of dimensions with the number of alternatives in each of them, i.e., N = 8x6x6x5x4x3x3x3x4) with plausible ones -N1 = 18360 & implausible ones -N2 = 603720, additionally identifying from N1: "tangible" (14358, RCW>0), "intangible" (3152, RCW<0) & neutral (850, RCW=0) scenarios.

Finally, a brief generalization of the morphological analysis findings could be outlined as follows:

The most intangible scenarios for the future will be related to divides with people's transhumanization (Sirius & Cornell, 2015) and new digital society reorganization provoked by AI algorithms and machine domination (Leonhard, 2016, Harari, 2017). This naturally is going to establish a transformed social hierarchy due to smart governance and i-espionage because of different understanding for the peoples' privacy and future society post-information lifestyle (being polyarchic or authoritarian (Tegmark, 2017)), but most probably hybrid ones, as was recently observed during COVID-19 pandemic (Schwab & Mallert, 2021). The overall resource access is added also to this scenario set due to new reality mixing climate changes and total connectivity (with new mobile solutions and satellite communication advances), (Minchev et al., 2022).

As far as the future transhumans are expected to have also different social behaviour (due to deeper technologies integration, providing new, advanced skills, (Bohan, 2022)) the social resilience and information overload effects need also to be carefully considered. Further, living parallelism (fostered by accelerated hyperreality and humans' deeper bilateral interconnectivity with wearable devices and implants), hybrid securing and strategic i-communications (by means of human-machine symbiosis with potential machine superiority (Minchev, 2021a)) are going to be of key importance for the upcoming post-information society building.

However, these changes are not isolated and the holistic transformational growth (clashing humans and machines at different levels of the future digital society) with the resulting new post-information ecosystem evolution are going to positively support the future society and people's fostered transformation (Minchev, et al., 2019).

On the other hand, the tangible scenarios are mainly addressing new smart services and technological innovations (Boyanov, 2021) that are going to transform the future smart economy (joining digital and social profits, including AI and robotics), adding huge data (produced with numerous IoTs integrated in the new smart ecosystem), smart negotiations



and decision making, but demanding new hybrid regulations necessity (due to the deeper technological penetration into the living matter, generating multiple ambiguities, (Minchev, et al., 2022)).

Here, transformational adversaries like biohacking and total digitalization will most probably stay under the human intelligence control, assisted by machines, though partially limited (as still the singularity is not that close but sentient AI appearance is definitely on the way (Leonhard, 2016)).

Finally, other unplanned external impacts are considered as neutral, and this addresses mostly potential social devolution caused by the appearance of unprecedented levels of stressors of natural or man-made origin (pandemics, magnetic storms, wars, social revolutions, etc., (Bostrom & Ćirković, 2008)), most probably assisted for meeting with future cyber diplomacy enabled smart negotiations and strategic i-communications between states.

Whilst these morphological analysis findings lack modeling causality, a profound understanding of new digital society system transformation details and the role of future cyber diplomacy could be achieved with a system-of-systems modeling exploration.

# **Analytical Perspective**

Achieving a comprehensive enough modeling exploration for the next 10-15 years (towards the year 2037) on the future cyber diplomacy and the attendant dual socio-technological post-information transformation effects could be achieved, benefiting from the experience with (Minchev, 2020 & Minchev, 2021b) approaches, and thus implementing system-of-system discrete representation of the studied problem at hand.

A holistic system graph-based machine representation in I-SCIP-SA environment is further used for this purpose, following the "Entity – Relationship" paradigm, while providing a "many-to-many" causality interconnectivity between the entities (Minchev, 2015). As far as working with expert and reference data is difficult to be handled regarding noise, uncertainties and multiple discretization understandings, an interval [0, 1] fuzzy weighting is accomplished for a discrete number of steps. The model graph-based generalized assessment is visualized in a four-sector 3D "Sensitivity Diagram" – SD ("Buffering" – Green, "Active" – Red, "Passive" – Blue, "Critical" – Yellow with additional sub-classification, regarding the entities' roles: "Active" – White & "Passive" – Grey). The SD is actually showing the entities' three-dimensional weights with the system model, according to: "Influence" – "X", "Dependence" – "Y" and their ratio, "Sensitivity" – "Z", values (Minchev, 2020).

What is important to state here is the extension of the author's study results on "shifted cyber diplomacy" (Minchev, 2021b) but going deeper in the problem by emphasizing AI sentient evolution tendencies (Tegmark, 2017), maybe even growing towards General AI (Russell & Norvig, 2021, Lennox, 2020). Further understanding the fostering transformational role of recent COVID-19 pandemic (Schwab & Mallert, 2021) goes even beyond the risk/utility ratio usage for holistic effectiveness assessment to system sensitivity (Minchev, 2015, Minchev, et al., 2019). This actually provides an opportunity to discover the instability of some entities,



following the famous Chaos Theory ideas (Strogatz, 2015), that will be discussed below with the model's analytical findings.

The results from the system modeling and sensitivity analysis, regarding the entities' foursector classification could be summarized as follows:

- Active: "Political iGovernance" -3, "Advanced Security Incidents" -7, "Fake Information Artefacts" -9, "Sentient AI" -10, all being also active with the model due to this zone classification;

- Passive: "Assisted Cyber Diplomacy" -2, "Smart Interfaces" -4, "Transformed People" -11, "State Actors" -14, "Hybrid Mediators" -15, all being also passive with the model due to this zone classification;

- Critical: "iMedia Environment" – 1, "Advanced Economy" – 5, "Non-State Actors" – 8, "Smart Resilience" – 17, being also active with the model & "Hybrid Knowledge" – "6", "Adversarial Groups" – 13, "Intelligent Data Breaches" – 16, being passive with the model.

- Buffering: "Other External Factors" – 12, being also active with the model.

Obviously, in the not-so-far future of the year 2037, assisted cyber diplomacy is going to hide numerous uncertainties and potential (Riordan, 2019), together with new state actors (being expected to both use and regulate the new AI technologies in the diplomatic field and everyday lifestyle), transformed people, hybrid (human-machine) mediators (being per se assistants to the transformed people with the new mixed reality), and smart interfaces in between them with the overall smart digital ecosystem (Kissinger, Schmidt & Huttenlocher, 2022). Active will be sentient AI (Bhaumik, 2018), which is expected to foster, together with non-state actors, the new political i-governance, influenced by new i-media environment (expected also to be critical), with fake information artifacts and advanced security incidents fostered by AI evolution (Susskind, 2018, Minchev, 2022b).

A new advanced economy (assisted by AI technologies) is expected to be essential in the future (Schwab & Mallert, 2022), along with adversarial hacking groups, and hybrid (joining human cognition with machine processing power) knowledge for meeting future security transcendents and exponentially growing transformational dynamics. Quite challenging will also be the new intelligent data breaches, affecting the smart resilience of the new digital society (Minchev, 2021a, Minchev, et al, 2022).

Having a predictive nature, these system modeling findings are giving focus to future state actors and sentient AI, establishing a new i-governance that naturally will establish cyber diplomacy and i-media, assisted by AI for which autonomous self-control will be difficult. Thus, the role of non-state actors and transformed individuals will remain inevitable in this context, trying to maintain the new socio-technological balance, while competing in the diplomatic area.

Next in the paper the simulation perspective of the problem at hand is presented, highlighting a joint human-machine role in the process.









(b)

**Figure 3.** Future cyber diplomacy modeling (a) and Sensitivity Diagram generalized analytical results (b) of dual socio-technological post-information transformation effects, towards the year 2037 in I-SCIP-SA.

### **Simulation Perspective**

The outlined future of cyber diplomacy in the post-information age modeling and analytical findings towards the next 10-15 years from now, would be extremely useful if they are further dynamically explored in a mixed reality environment with user feedback assessment. This allows combination of both human and machine intelligence in a simulated reality of different projections (augmented, virtual, mixed, in the context of a new, transformed and ad-hoc digital ecosystem establishment) with interactive tailoring of useful analytical results.



A set of experimental activities, joining different details of human-machine inter-awareness (i.e., multimodal and multilevel communication) is further presented in this sense, trying to verify some of the findings for the future in a selected mixed reality scenario context, following the results from the already marked modeling and analytical perspectives findings.

Cyber Research Exercise Study – The experiment has been organized during the CYREX i. 2023 event, joining the efforts of the Institute of ICT, Bulgarian Academy of Sciences and the University of National and World Economy, with the support of "Secure Digital Future 21" international initiative and IFIP TC 14, UNESCO (CYREX, 2023). The main idea of the 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 ones), concerning the cyber security area (technological, social, infrastructural, security, political, diplomatic). The idea was to develop and test a set of morphological and system models for the not-so-far future, among young people (Y- & Z- generations ones), joining both human and machine intelligence in the process of decision-making and scenario development, while using a role-based organization, multiple smart gadgets and platforms. The training was illustrated, combining results of artificially generated images, videos, sounds and popular multimedia clips. The idea allows the studying of complex security transcendents dynamics in a futuristic mixed reality smart ecosystem, giving excellent training feedback results, especially at organizational and operational levels (Minchev, et al., 2022).



Figure 4. Pictures of participants, architecture and media materials during CYREX 2023



Figure 5. Generalized results of CYREX 2023.



*ii. Simulated Reality Exploration* – the main idea of the approach is to recreate imaginary scenario situations for the future, while joining augmented and virtual realities with multimodal hardware and software, monitoring at the same time a selected user group feedback response with different biometrics, following (Minchev, et al., 2022).



(b)



**Figure 6.** Simulated reality experimental set-ups: VR (left) & AR (right) with three selected futuristic scenario combinations aggregated results: (a) - (c), adapted from (Minchev, et al., 2022).



The practical implementation of this approach has been performed in a 3D simulated reality, regarding three short multimedia scenario combinations: *Future War, Cyber Terrorism* and *Digital Politics*, using both virtual and augmented realities mix (because of different electronic setups generating a mechanical conflict with the visualization hardware, like: VR helmet and EEG electrodes simultaneous mounting), while monitoring participants' central (brain activity via EEG) and peripheral nervous system (GSR response from dominant hand) correlates, together with additional measuring of psychometric preliminary and post-experimental bias (personality, motivation, short-term memories on objects from the multimedia stimulation), trying to achieve a proactive and comprehensive understanding on the part of the audience of a futuristic exploration context.

Obviously, experimenting with user feedbacks (both voluntary and non-voluntary ones) is always uncertain but somewhat useful as the scenario context is stimulating human-only traits (like: imagination, creativity, intuition, emotions, feelings & judgments) that are still not part of the smart machines (Leonhard, 2016, Tegmark, 2017). The actual positive expectations for the role of AI solutions at this stage are quite helpful, as far as some sensitive findings could be deliberately, proactively studied and extended in mixed and simulated realities flexible context, achieving comprehensive multiaspect understanding for the digitally transformed post-information future of joint human-machine symbiosis. These findings are selected subjectively by the humans and address different transformational transcendents, such as: new smart ecosystem cyber responses on social dynamics, related to the future: wars, terrorism, criminal activities, diplomacy, politics, governance, i-media and lifestyle as a whole.

# **CONCLUSION**

In the not-so-far future of the next 10-15 years, a fostered AI evolution is certainly going to be observed towards sentient AI, i.e. which is a significant step up from the narrow AI of present reality. This technological disruption is going to reshape the new digital ecosystem of people, technologies, biotope, infrastructure and the symbiotic inter-awareness among them for a new post-information society progressive development. Different ways of making decisions and extracting information from multiple data sources are expected to appear in this sense, transforming intelligently the media environment, political governance and diplomacy at a new level of knowledge-assisted extraction and dynamics handling from cyber domain perspective. This profound change is certainly going to transform the future military conflicts, diplomatic negotiations and overall political decision-making to a new i-governance stage of either a polyvalent federated world or an authoritarian one.

So, establishing a proactive framework for a comprehensive exploration of these transformational processes is evidently a challenging task that could benefit from both human and machine modeling joint efforts, adding a suitably interactive assessment of dynamic results.

The presented findings are demonstrating a clear tendency for this new social deep change at state and global levels. What however is still quite unclear is whether this transformation will lead to a dystopian or utopian world, as the state and non-state actors are still controlled by human emotions and objectives for social reality domination, resulting often in irrational actions and decisions.



Going even further, the external influences of climate changes and collateral damages, resulting from military conflicts, pandemics, economic transformations and constant new generation objectives for change, make the future cyber diplomacy tasks quite complex and challenging, trying to keep the balance between mankind's sustainable and resilient well-being versus dominated post-information society governance, assisted but hopefully not totally controlled by new AI technologies

#### **Acknowledgments**

The results presented in the study are due to the technological, industrial, diplomatic and expert support obtained within the initiative "Secure Digital Future 21", http://securedfuture21.org. Additional gratitude is expressed towards the author's colleagues: Luben Boyanov, University of National and World Economy, Velizar Shalamanov, Institute of ICT, Bulgarian Academy of Sciences, Galit Margalit Ben-Israel, Beit-Berl Academic College, Stoyan Ivanov, SKAT TV, Evgeni Krastev, Military TV Channel, Yordan Bozhilov, Sofia Security Forum, and Thorsten Geißler, Konrad Adenauer Stiftung, for the inspiration and fruitful discussions, related to the cyber diplomacy exploration framework implementation.

# **REFERENCE LIST**

- Allen, J., Hodges, B., & Lindley-French, J. (2021). Future War and the Defence of Europe, Oxford University Press, ISBN: 978-0-19-259786-1
- Bhaumik, A. (2018). From AI to Robotics Mobile, Social, and Sentient Robots, CRC Press, Taylor & Francis Group, ISBN-13: 978-1-4822-5147-0
- Bohan, E. (2022). Future Superhuman (Our Transhuman Lives in a Make-Or-Break Century), NewSouth Publishing, eISBN: 978-1742238357
- Bostrom, N. & Ćirković, M. (2008). Global Catastrophic Risks, Oxford University Press, ISBN-13: 978-0199606504 Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies, Oxfor University Press, ISBN: 978-0199678112

Boyanov, L. (2021). Digital World - The Change, Avangard Prima, ISBN: 978-6192396374

CYREX (2023) Cyber Research Exercise 2023, https://youtu.be/m7mTfvtmtFc

- Farwell, J. (2020). Information Warfare, Marine Corps University Press, ISBN: 978-1-7320030-9-5
- GRR (2023). The Global Risks Report 2023, WEF, https://www3.weforum.org/docs/WEF\_Global\_Risks\_ Report\_2023.pdf
- Harari, Y. (2017). Homo Deus: A Brief History of Tomorrow, HarperCollins Publishers, ISBN-13: 978-0062464316
- Kissinger, H., Schmidt, E., Huttenlocher, D. (2022). The Age of AI: And Our Human Future, Back Bay Books, ISBN-13: 978-0316273992
- Lennox, J. (2020). 2084: Artificial Intelligence and the Future of Humanity, Zondervan Reflective, ISBN: 978-0-310-10958-7
- Leonhard, G. (2016). Technology vs Humanity: The Coming Clash between Man and Machine, Fast Future Publishing, ISBN: 978-1-0964967-2-4
- Meadows, D., Meadows, D., Randers, J., Behrens III, W. (1972). The Limits to Growth, A Report for the Club of Rome Project on the Predicament of Mankind, Universe Books, ISBN: 0-87663-165-0
- Minchev, Z., Boyanov, L., & Georgiev, S. (2013). Security of Future Smart Homes. Cyber-Physical Threats Identification Perspectives, In Proc. of National Conference with International Participation in Realization of EU HOME/2010/CIPS/AG/019 project, Sofia, Bulgaria, pp. 165–169, ISBN: 978-954-92552-7-0
- Minchev, Z. (2015). Human Factor Role for Cyber Threats Resilience, In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, 1 ed., M. Hadji-Janev and M. Bogdanoski, Eds., IGI Global, pp. 377-402, ISBN-13: 978-1466687936
- Minchev, Z., et al. (2019). Future Digital Society Resilience in the Informational Age, Softtrade & Institute of ICT, Bulgarian Academy of Sciences, ISBN: 978-954-334-221-1



- Minchev, Z. (2020). Future Digital Society Transformational Transcendents & Gaps Extended Outlook, Romanian Cyber Security Journal, vol. 2, no. 1, pp. 11-18
- Minchev, Z. (2021a). Malicious Future of AI: Transcendents in the Digital Age, In Proc. of BISEC 2021, Belgarade Metropolitan University, DOI: 10.13140/RG.2.2.27693.00487
- Minchev, Z. (2021b). Disruptive Effects of New Pandemic Age to Shifted Cyber Diplomacy due to Multilateral Mixed Transformation, International Journal of Cyber Diplomacy, Vol. 2, pp. 49-59
- Minchev, Z. (2022a). Proactive Identification of Future Cyber Threats, In Proc. of BISEC 2022, Belgarade Metropolitan University, DOI: 10.13140/RG.2.2.27998.92488
- Minchev, Z. (2022b) Public Opinion Influence Through Electronic Propaganda Activities, In Bogdanoski, M. (Ed) Building Cyber Resilience against Hybrid Threats, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol.61, pp.60 - 70, DOI10.3233/NICSP220018
- Minchev, Z., et al. (2022). Digital Transformation in the Post-Information Age, Softtrade & Institute of ICT, Bulgarian Academy of Sciences, ISBN: 978-954-334-251-8
- Nehring, Ch. & Sittig, H. (2023). Blurring the Truth: Disinformation in Southeast Europe, Konrad-Adenauer-Stiftung e.V., ISBN: 978-3-98574-110-6
- Osmolovska, I. & Maksak, H. (2022). Five Security Scenarios on Russian War in Ukraine for 2022–2023: Implications and Policy Recommendations to Western Partners, GLOBSEC "Ukraine and Eastern Europe" Program Report, http://bitly.ws/Ey2R
- Plokhy, S. (2023). The Russo-Ukrainian War (The Return of History), Penguin Books, ISBN-13: 1978-0241617359
- Randers, J. (2012). A 2052: Global Forecast for the Next Forty Years, Chelsea Green Publishing, White River Junction, Vermont, eISBN: 978-1-60358-422-7
- Raphael, C., et al (2020). The Future of Warfare in 2030: Project Overview and Conclusions. Santa Monica, CA: RAND Corporation, http://www.rand.org/t/RR2849z1 [Accessed ?]
- Riordan, S. (2019). Cyberdiplomacy: Managing Security & Governance Online, Polity Press, ISBN: 978-1-5095-3407-4
- Russell, S. & Norvig, P. (2021). Artificial Intelligence: A Modern Approach, 4 ed, Pearson, ISBN-13: 978-0134610993
- Ryan, M. (2022). War transformed: the future of twenty-first-century great power competition and conflict, Naval Institute Press, ISBN-13: 978-1682477427
- Sandre, A. (2015). Digital Diplomacy. Conversations on Innovation in Foreign Policy, Rowman & Littlefield, ISBN-13: 978-1442239128
- Schwab, K. & Malleret, T. (2020) COVID-19: The Great Reset, World Economic Forum, ISBN-13: [978-2940631124 Schwab, K. & Mallert, T. (2021). COVID-19: The Great Reset, WEF, ISBN-13: 978-2940631124
- Schwab, K. & Mallert, T. (2022) The Great Narrative, WEF, eISBN: 978-2-940631-31-5
- Shanahan, M. (2015). The Technological Singularity, The MIT Press, ISBN-13: (978-0262527804
- Sirius, R. & Cornell, J. (2015). Transcendence: The Disinformation Encyclopedia of Transhumanism and the Singularity, Disinformation Books, ISBN-13: 978-1938875090
- Strogatz, S. (2015). Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, Second Edition (Studies in Nonlinearity), CRC Press, 2nd edition, ISBN-13: 978-0813349107
- Susskind, J. (2018). Future Politics, Oxford University Press, ISBN 978-0-19-882561-6
- Tegmark, M. (2017). Life 3.0: being human in the age of artificial intelligence, Alfred A. Knopf, eISBN: 978-1101946602





#### **Zlatogor MINCHEV**

Is an "Associate Professor" (2010) on "Automation and Control", IT for Security Department Head (2016) at Institute of ICT, Bulgarian Academy of Sciences; Part-time "Associate Professor" (2011) at Operations Research, Probabilities & Statistics Department, Institute of Mathematics & Informatics Bulgarian Academy of Sciences. Director of the Joint Training Simulation & Analysis Center (2007), organizing and conducting research in the fields of foresight analysis with mixed realities assessments, supercomputer simulations, cybersecurity, crisis & emergency management. Author and co-author of a large number (above 200) of scientific publications; successful participant in numerous (above 50) national & international scientific projects on expert and managing positions; International visiting professor on multiaspect security and cybersecurity problems in Europe, Latin & North America & the Balkans. His diplomatic experience dates back with NATO Public Diplomacy Division recognition as Security Opinion Leader (2010), further extended with Cybersecurity problems (2014). He has been also collaborating on the diplomatic field with the non-government sector: Managing Board of Association of the Officers in the Reserve "Atlantic" (2010-2012) & Executive Board of George C. Marshall Association -Bulgaria (2008-2010). Vice-Chairman of Communication & Information Specialists Association - Bulgaria; e-Sigurnost Balkans Association honorable member (2017). President & founder (2017) of the international forum "Secure Digital Future 21" for research, business and policy makers efforts and experience joining with more than 50 countries now. Awarded and distinguished with numerous prestigious national and international awards. Well-known expert for the media (with above 300 interviews) in the country and abroad on security and technological challenges.