Disruptive Effects of New Pandemic Age to Shifted Cyber Diplomacy due to Multilateral Mixed Transformation

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

Abstract: The paper outlines a comprehensive model, concerning socio-technological disruptive effects to shifted cyber diplomacy due to multilateral mixed transformation and system effectiveness evolution towards the year 2033. The approach aims towards a proactive understanding of a comprehensive digital future, combining expert and reference data with machine simulations in the "shifted reality" of the new pandemic and technologies. A combination of morphological and system analysis is initially presented with further probabilistic future validation and verification, implementing multicriteria base oscillators cyclic coherence assessment. Finally, a wrap-up discussion on the results, uncertainties and expectations for the future is presented.
Keywords: Shifted cyber diplomacy, Fostered transformation, Comprehensive modelling & analysis, Multicriteria assessment, Future validation & verification.

INTRODUCTION

Understanding today's world and the attempting to foresee the dynamics of future trends is a quite challenging, multilateral task. Since the year 2020, the technological progress has unexpectedly clashed with the COVID-19 pandemic, producing a new "shifted reality" throughout the world.

This, on the one hand, has unconditionally reordered the present civilizational priorities towards survival in a challenging period and, on the other hand, created a closed-loop for the technological innovation dynamic, which are evolving in a new manner. The change is practically establishing a new accelerated Fourth Wave social transformation, that lasts less than five-years' time (Minchev et al, 2019) but technologically oversaturates our human consciousness.

The situation necessitates an adequate support of this accelerated transformation towards a new technologically fostered bio-technologically mixed smart reality. The "shifted reality" is becoming a popular concept, though it is not quite new (Atwater, 2013) but the desire to escape from the transformation's results is inevitably driving this rebirth.

Covering all lifestyle areas of modern global existence, the new pandemic crisis has naturally affected people's freedoms of movement, work, education, medical treatment and self-motivation in an extraordinary way.

What however stays unconditionally important is the successful political governance and diplomatic adaptation to the new shift, establishing both short- and long- term successful strategic planning and an adequate economic response to the necessities (Schwab & Vanham, 2021).

The multiple contradictions in diplomacy between key powers (Riordan, 2019; Snow & Cull, 2020; Rasjid, 2020) have escalated to a new level, joining technological evolution as the "new normal". The "online lifestyle" of adversaries, negotiations, meetings, communications, media

influence and even espionage has resulted in the mixing of "cyber" with "digital" in an unprecedented shift to "shifted cyber diplomacy".

A number of hostile cyber activities in this context are naturally related to the COVID-19 pandemic, concerning governmental and public information resources and infrastructure, to mark some of the most prominent ones (Minchev, 2020; FPred, 2021). More uncertain and with probably state level of organization (following their scale and comprehensiveness) were: FireEye & SolarWinds (targeting government and corporate networks spread among North America, Europe, Asia, and the Middle East, the very recent new Microsoft breach APTs and the water supply terrorist-like unsuccessful cyberattack in Florida.

Apart from this, we have pharmaceutical industry espionage, related to vaccines (Davis, 2021) and the electronic queuing for vaccination (BGHealth, 2021), together with escalating social network vulnerabilities and the resulting psychological and behavioral transformations with political effect (see e.g. Gloster et al, 2020; Ding, 2021), ransomware (Sophos Ransom, 2020) and compromised by design, which are naturally complicating the security landscape, together with the new shifted reality.

The pandemic situation has been marked as important also by the UN, EU, NATO, World Health Organization, World Bank and World Economic Forum (see UNCOVID, 2021; EUCOVID, 2021; NCOVID, 2021; WHOCOVID, 2021; WBCOVID, 2021; WEFCOVID, 2021) outlining the security environment complication together with serious human loss potentialities (due to virus new mutations), climate change and negative economic effects.

In this landscape, the objective for the EU Cybersecurity Strategy update, jointly with EU 5G Strategy, Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy are quite timely efforts towards achieving resilience for a comprehensive EU cyber-physical ecosystem (EU Cybersec, 2021, EU Rec Plan, 2021).

Further in the paper, a comprehensive model concerning the socio-technological disruptive effects for shifted cyber diplomacy multilateral transformations and system effectiveness towards the year 2033 is presented and studied.

Additionally, the outlined findings are explored with an ad-hoc multicriteria final assessment approach.

METHODOLOGICAL FRAMEWORK

The idea of the curent study is based on the methodology presented in (Minchev, 2020a), but is experimentally enriched with probabilistic prognostic validation and further verified with multicriteria effectiveness assessment. The solution combines both experimental and reference data, ensuring a bidirectional cyclic evolution exploration.

A threefold exploration framework goes through the following stages: (i) Problem Space Definition; (ii) Prognostic Analytical Modelling; (iii) Future Results Assessment.

Being complex enough, the approach is combining both technological and human factor transformations in a fusion state, aiming towards a proactive understanding of a comprehensive

digital future. It also contains "accents" of the fostered transformation in the new "shifted reality", challenging both governance and diplomacy, such as transhumanisation, marked by mixed IoT and pervasive AI.

This naturally is also going to arm the mixed modern society with new AI assisted skills and sensors, capable of handling large communication flows with rich data (springing mostly from multiple sources, both wearable and infrastructure oriented IoTs, having different dynamics) processing and convenient details handling, ensuring a resilient future for the new society towards cyberattacks, APTs, fake news and espionage.

The change is expected to foster a new level of evolution mental and physical capabilities at the level of the human resource, providing also new knowledge elicitation for unplanned events (like: pandemic or other natural-/ man-made disasters) proactive identification, rating and resolution.

IMPLEMENTATION DETAILS

Additional methodological details of the presented three-stage exploration framework are provided in this section, outlining implementation specifics with supplementary results and graphics discussions.

3.1. Problem Space Definition

Defining a plausible scenario set for the study of the future is a quite challenging task that could practically benefit from the morphological analysis towards year 2033, updating the ideas presented in (Minchev, 2020a; Minchev, 2020b). The incorporation of key recent COVID-19 pandemic shifted reality changes with nods to digital technology effects, social reality and diplomatic issues transformations versus suitable drivers and uncertainty aggregation is practically accomplished.

The plausible scenario cross-consistency matrix pool has been produced, with joint expert and reference data fusion in I-SCIP-MA environment, after (Minchev, 2015), ensuring a reasonable morphological analysis for unstructured and noisy inputs. The obtained scenario combinations are weighted quantitatively by the RCW approach (see Fig.1), joining logically the following segment: "driving factor" -> "digital challenge alternative" -> "social issue" -> "future diplomacy alternative" -> "mixed uncertainty".

Three types of scenarios are used ("tangible", RCW > 0, "intangible", RCW < 0, and "neutral" ones, RCW = 0), blueprinting an original futuristic outlook for the shifted cyber diplomacy multilateral transformation effects.

The total scenario number is N = 6000, resulting from the multiplication of dimensions with the number of alternatives in each of them, i.e., N = 4x5x3x4x5x5. The expert and reference help has further filtered N' = 1768 scenario combinations, according to their RCW: positive – 1068 (RCW > 0), negative – 635 (RCW < 0) and neutral – 65 (RCW =0).

Finally, a brief generalization from the morphological analysis scenario pool establishment but without system causality is the following:

- The future intangibles will be mostly driven by fostered dynamics and other (unplanned)

impacts. For instance, we have: the unsuccessful handling of climate change, natural catastrophes, space phenomena, new pandemic or related diseases (see Bostrom & Ćirković, 2008), other unexpected events (conflicts, wars on resources and interests), their potential escalation, together with the technological mixing with humans (HRT, 2020). This naturally is producing effects on information overload, privacy and new regulations due to transhumanisation and lifestyle metamorphosis. The diplomatic response to this new context is expected mainly to address adversarial issues (wars, terrorism, etc.), espionage and strategic communications, whilst the big uncertainties are going to spot the future of e-negotiations, overall parallelism and hybrid securitization with a trend towards total digitalization, that obviously will require more time.

- The reality shifting, stakeholder e-economy (Schwab & Vanham, 2021) and the pervasive smart technology (with AI embedding alongside with smart infrastructure and services, wearable/implantable IoT gadgets, mixing deeper humans with machines (Harari, 2017)) will foster digital acceleration and the e-negotiations diplomatic role, together with the clash of generations and overall transformation bounding uncertainties.

Thus, the present COVID-19 pandemic will catalyze the future society digital transformation, keeping at the same time an indispensable role for the old conflicts and challenges, while complicating them with the new technological senses and capabilities.

A deeper exploration of these wrap-ups is further given with system-of-systems causality analytical modelling and the holistic assessment of the resulting transformation effectiveness.

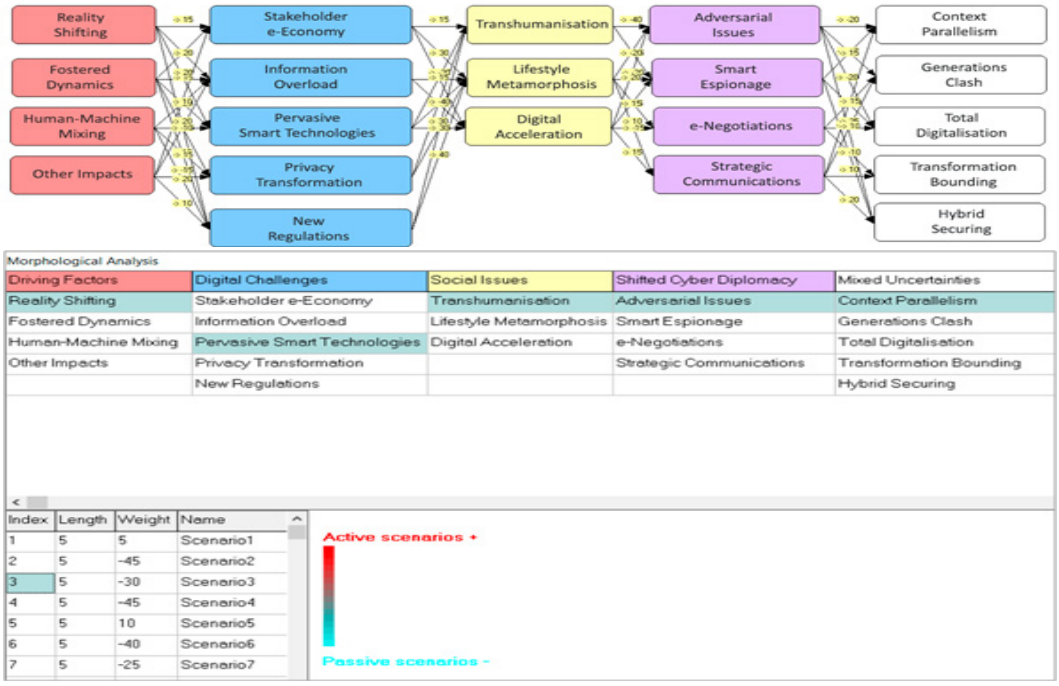

Figure 1. *Graph-based model representation (a) with cross-consistency scenario matrix (b) for shifted cyber diplomacy & multilateral society transformation effects studying in I-SCIP-MA environment*

3.2. Prognostic Analytical Modelling

Achieving a holistic assessment of the next 10 years and beyond for the cyber diplomacy multilateral shifted transformation could be achieved with system-of-system discrete modelling over a weighted graph, using causality representation of the studied problem at hand.

An "Entity – Relationship" representation is originally used. "Entities" (noted as labelled rounded rectangles) and "Relationships" (noted as bi-directional weighted arcs) have been used in the modelling process, ensuring suitable abstract representation of the holistic system (Vester, 2007), incorporating "many-to-many" multidimensional interconnectivity.

The overall graph-based aggregated assessment is presented in a 3D "System Effectiveness Diagram" – SE Diagram, based on the system effectiveness – Es interpretation by feed-forward effectiveness – Ef and feed-backward – Eb ratio usage in I-SCIP-EA environment (Minchev et al, 2019). Es values have been obtained using Bayesian probabilistic approach towards a certain scenario evolution.

Briefly, the idea could be summarized as follows: Es (Ef, Eb); Ei (Ri, Ui, Sk) = P (Ri|Sk) x P (Ui|Sk), where: P (…) – Bayesian probability, Ri – system risk, Ui – system utility, i = {f, b}, Sk – selected k-th scenario from the scenario matrix pool M (see Fig. 1b). Both Ri and Ui could have multiple probabilistic meanings, but not obviously with correlating nature.

The resulting dual behavior of entities is transposed in a SE Diagram with both "Intermittent" vs "Perpetual" main classes (graphically divided with the NW/SE diagonal). A sub-classification for both types of entities, regarding their roles are: "active" (white) or "passive" (grey) ones.

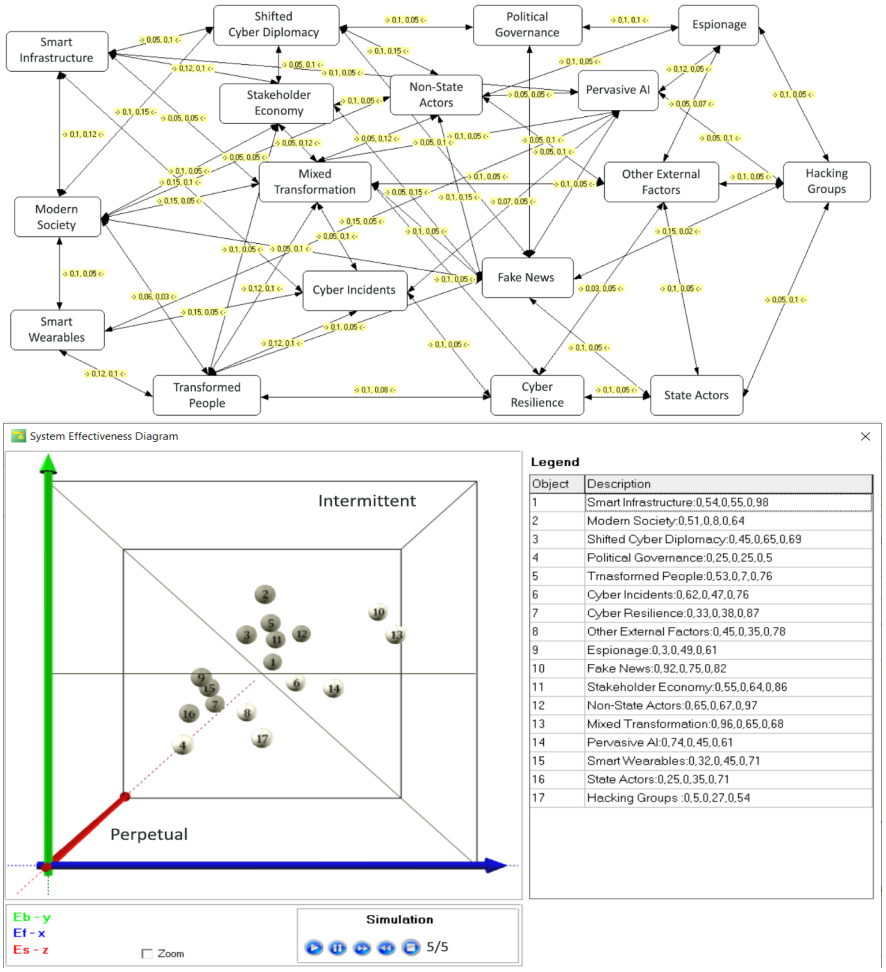

Figure 2. *System modelling (a) of socio-technological disruptions for shifted cyber diplomacy and (b) of multilateral society transformation effects, with SE Diagram joint assessment, towards the year 2033, in I-SCIP-EA environment*

The results from the system analytical modelling with effectiveness assessment could be summarized as:

- Perpetual: "Political Governance" – 4, "Other External Factors" – 8, "Hacking Groups" – 17, all expected to be active; "Cyber Resilience" – 7, "Espionage" – 9, "Smart Wearables" – 15, "State Actors" – 16, all four expected to be passive;

- Intermittent: "Cyber Incidents" – 6, "Fake News" – 10, "Mixed Transformation" – 13, "Pervasive AI"– 14, all four expected to be active; "Smart Infrastructure" – 1, "Modern Society" – 2, "Shifted Cyber Diplomacy" – 3, "Transformed People" – 5, "Stakeholder Economy" – 11, "Non-State Actors" – 12, all six expected to be passive.

Obviously, in the next 10 years towards 2033 and beyond, the role of the fake news and pervasive AI is expected to grow, fostering the mixed human-machine transformation and producing, at the same time, new types of cyber incidents. This naturally will affect the modern society, people and smart infrastructure digital transformation. An establishment of a shifted role for the cyber diplomacy with both state and non-state actors, aiming towards a sustainable political governance and societal resilience, is going to take place.

Apart from these, other (unplanned, natural and man-made disasters) external factors and hacking groups, assisted with new technological products and services will definitely influence the future reality. Directing extended espionage and other criminal activities mainly via smart solutions (wearable/embedded sensors & devices, producing new mixed IoTs), the future cyberattacks and advanced threats are going to encompass AI assisted solutions, inspired both by state and non-state actors (groups and allies) with diplomatic adversarial issues (targeting future transformed smart infrastructure, services, devices and humans), supporting both negotiations and the achievement of strategic goals (political, economic, military, etc.).

Whether these findings sound quite reasonable or not, further assessment is required, implementing both probabilistic machine simulation and expert beliefs for the future.

3.3. Future Results Assessment

Dynamic Probabilistic Exploration

The findings presented so far from both morphological and system analyses are based on expert beliefs and reference data for the future gathered around Secure Digital Future 21 initiative (SDF 21, 2021) activities since the summer of 2020 up the early spring of 2021. What however is interesting to state here is the possibility of a foundation for an ad-hoc future validation approach. The greatest problem in this objective fulfilment however is the reliablility of future outlines. As solving this task only from mathematical perspective sounds infeasible, a hybrid (human-machine) solution has been used here. The idea is to use a quasi-Monte Carlo probabilistic evaluation (Minchev, Dukov, Boyadzhiev & Mateev, 2016), implementing selected scenario sets, using the system modelling findings as simulation criteria achievements, being mirrors of the expert future beliefs.

One of the key problems in this solution however is the cyclical nature of all of the studied processes, while the other is the combinatorial boom of possibilities that have to be studied. So, a model simplification has been used, following (Minchev et al, 2019). In practice, the

Kondratiev's waves probabilistic multiphase approximation has been implemented, using Beta distribution of both a priori and a posteriori assessment. The former includes expert beliefs, machine assisted trend distribution generation, following Forrester simplifications of: dual growth & equilibrium, assuming non-stationarities could be transformed in sub-models, concerning selected scenario set, assuming the criteria defined in (Minchev, 2020b). The idea is using an agent-based approach of a sub-graph model, resulting from the holistic system model.

Selected illustrative results, for the "Shifted Cyber Diplomacy" with effectiveness assessments Es' & Es" is presented in Fig. 3.

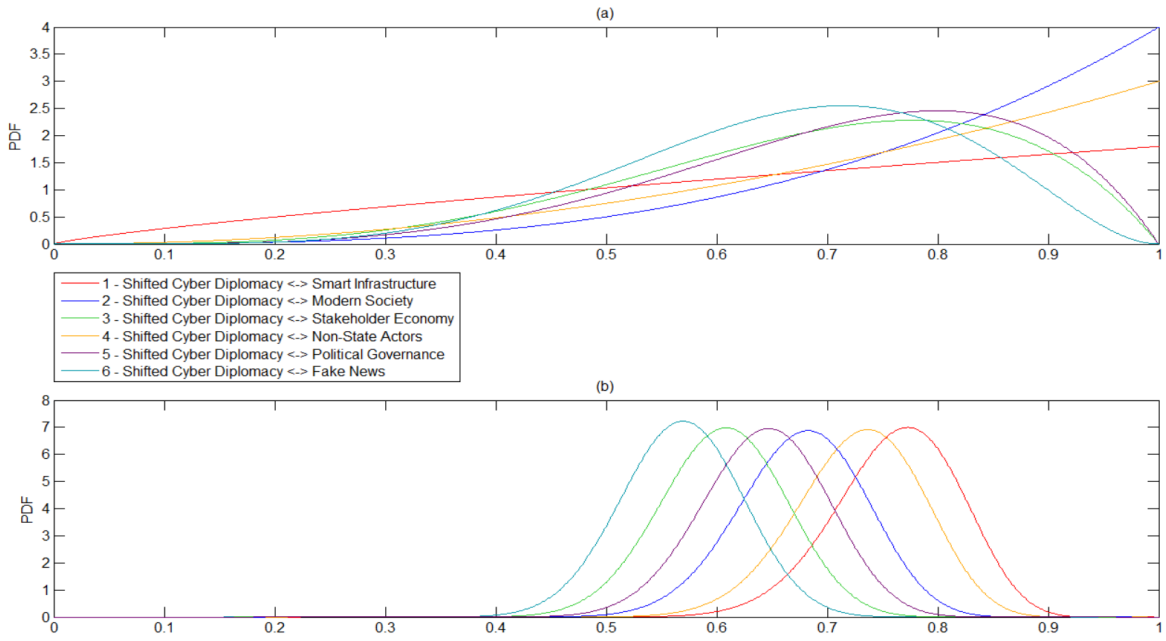

Figure 3. *PDF effectiveness assessment idea for both a priori – Es' (a) and a posteriori – Es" (b) values of "Shifted Cyber Diplomacy" up to year 2033*

Here it should be also noted that the problem complexity is quite high, as the effectiveness evaluation – Es is both dependent on risk – Rs and utility – Us (Minchev et al, 2019), having multiple joint evolution dynamics. Luckily, this dynamic could be approximated with assumption similar to the one in (Minchev, 2019). Due to overlapping in the final results PDFs distribution (i.e. assuming existence of more than two entities simultaneous connectivity with $p > 0,5$) the dynamics cyclic nature is getting quite complex.

Finally, a part of the overall model dynamics high complexity and potential (planned & unplanned, closely related also to external model influences with different origin (Frank et al, 2018) non-stationarity, probabilistic base (fundamental) oscillator models implementation coherence could be used (Minchev, 2020c). Bellow this concept will be given in more details with implementation in multicriteria verification of future results.

Multicriteria Verification

Understanding the obtained results meaning is a quite complex task especially for the future, so hereafter an expert-based multicriteria verification is proposed. Using a selected set of

oscillator models implementation coherence from present situation to the desired future. The idea behind is combining effectiveness assessment with a priori (Es' – present) and a posteriori (Es" – future) values from the previous section probabilistic validation with the concerns marked in (Minchev et al, 2019; Minchev, 2019; Minchev 2020c). The key moment is to handle unplanned and unexpected events by means of uncertainties with suitable coefficients (see Pavlov & Andreev, 2013; Dezert, Tchamova, Han, & Tacnet, 2020), while in the previous section the main objective was to understand the potential dynamics trend & periodicity due to overlays in different phases (see Fig.3b). The concept is based on the inductive reasoning as follows: if we assume a certain effectiveness classification for a model entity, then the other ones related to this entity should be able to ensure a new classification optimally and independently equivalent. In other words – the model Es" reassessment (with Ef/Eb ratio changes and final results coefficients re-weighting, see Fig.4), all starting from the Es' initial a priori effectiveness classification should produce an admissible predictable uncertainty (marked as "Other"). Otherwise, there have to be additional model entities or relations existing in the present model configuration, or to use different dynamics oscillators models. These findings from the future socio-technological context practically address new unplanned factors or players in the future transformation of the digital society.

Some selected examples (see Fig.4) from the holistic system model (see Fig.2a), encompassing "Shifted Cyber Diplomacy", "Pervasive AI", "Mixed Transformation" & "Modern Society" entities, being of significant importance due to their intermittent behavior for the future (see Fig.2b), are studied here.

Figure 4. *Multicriteria effectiveness assessment results for present – Es' and future – Es" effectiveness on selected key entities from the system modelling (see Fig. 2)*

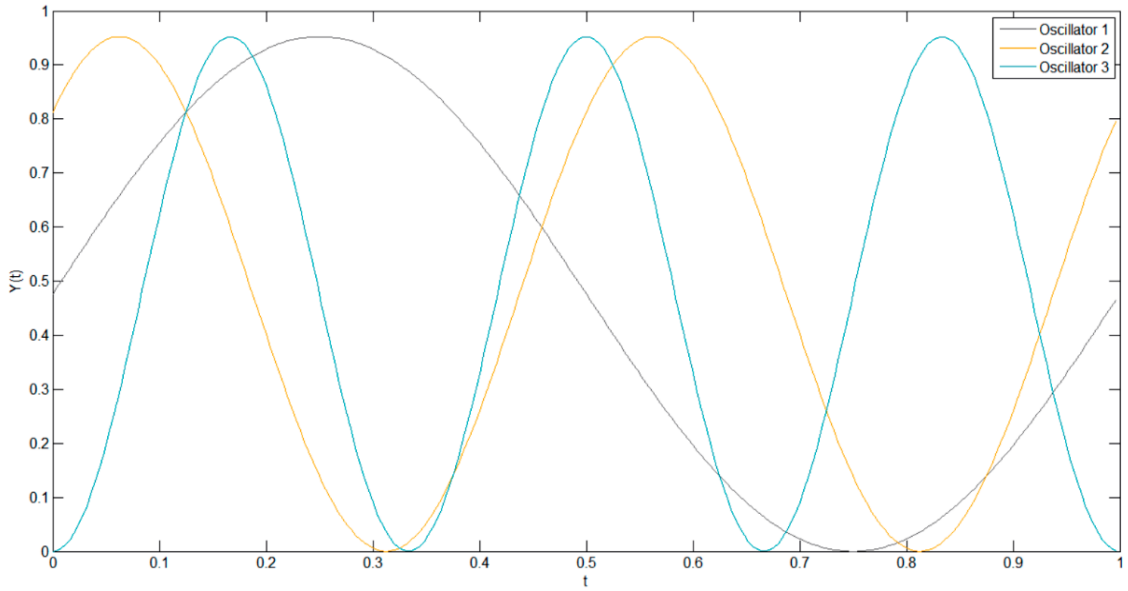

Figure 5. *Illustrative representations of three non-stationary, probabilistic oscillator models,used for effectiveness verification of multicriteria future assessment with cyclic coherence (see Fig.4)*

DISCUSSION

The presented results and findings are demonstrating the clear near future dependence on cyber diplomacy shifting due to multiple criteria effects (both technological and social ones), keeping at the same time a sustainable political governance. The role of non-state actors is confirmed to grow together with the stakeholder economy, adding AI and IoT innovations (infrastructural, wearable and embedded ones, using cloud services) to the general landscape transformation. What however will be difficult to handle towards the next 10 years and beyond are the fake news, through the future technological progress with new AI assisted human senses and services, supporting the huge rich data storages processing and knowledge extraction. This is expected to strongly influence the future shifted cyber diplomacy, keeping at the same time a resilient society despite hacking groups and cyber incidents. Thus, the contradictions and conflicts in the new mixed human-machine smart reality will still be dominated by human objectives and intelligence.

Obviously, the role of new external factors is also expected to grow due to multiple reasons (to mark: climate changes, social crisis, new pandemics, wars, contradictions, etc.), shifting the modern future society and people into a new kind of reality dynamics, which are more complicated. This new reality is going to be fostered by both social and technological hybrid phenomena.

Future people are most probably going to live in a new “preferable & adjustable reality” of fake news, smart human-machine governance and mixed human-machine lifestyle symbioses.

This new shifted and rapidly changing reality will be extremely difficult to handle through the diplomacy of peaceful global existence due to the negative dynamics prognosis of the near future fostered by the recent COVID-19 pandemic and climate change challenges, among others.

ACKNOWLEDGEMENTS

The results presented in this study are due to the technological, industrial, diplomatic & expert support obtained in the framework of the initiative "Securing Digital Future 21", http://securedfuture21.org.

REFERENCE LIST

Atwater, P. (2013). Future Memory, Hampton Roads Publishing, ISBN: 978-1-57174-688-7.

BGHealth (2021). Minister Angelov: Hacker Attacks on the Electronic Register for Vaccine Against COVID-19 Continue, March 7, https://www.mh.government.bg/bg/novini/aktualno/ministr-angelov-hakerskite-ataki-km-elektronniya-r/

Bostrom, N. & Ćirković, M. (2008). Global Catastrophic Risks, Oxford University Press, ISBN: 978-0199606504.

Davis, J. (2021). Hackers Leak COVID-19 Vaccine Data Stolen During EU Regulator Breach, Jan 13, https://healthitsecurity.com/news/hackers-leak-covid-19-vaccine-data-stolen-during-eu-regulator-breach

Dezert, J., Tchamova, A., Han, D. & Tacnet, J. (2020). The SPOTIS Rank Reversal Free Method for Multi-Criteria Decision-Making Support, 2020 IEEE 23rd International Conference on Information Fusion (FUSION), Rustenburg, South Africa, pp. 1-8.

Ding, K. et al. (2021). Mental Health among Adults during the COVID-19 Pandemic Lockdown: A Cross-Sectional Multi-Country Comparison, International Journal of Environmental Research and Public Health, 18, 2686, https://doi.org/10.3390/ijerph18052686

EUCOVID (2021). Coronavirus Response, EU, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response_en

EU Cybersec (2021). Cybersecurity, Shaping Europe's Digital Future, EC, https://ec.europa.eu/digital-single-market/en/cybersecurity

EU Rec Plan (2021). A Recovery Plan for Europe, Feb 11, https://www.consilium.europa.eu/en/policies/eu-recovery-plan/

FPred (2021). Predictions 2021, Forrester Research Inc., https://go.forrester.com/predictions/

Frank, A., Carroll-Nellenback, J., Alberti, M. & Kleidon, A. (2018). The Anthropocene Generalized: Evolution of Exo-Civilizations and Their Planetary Feedback, Astrobiology, vol. 18, no. 5, pp. 503-518.

Gloster, A. et al. (2020). Impact of COVID-19 Pandemic on Mental Health: An International Study. PLoS ONE 15(12): e0244809. https://doi.org/10.1371/journal.pone.0244809

Harari, Y. (2017) Homo Deus: A Brief History of Tomorrow, HarperCollins Publishers, Introduction to Theory and History. 10th Edition, Pearson Education, ISBN: 9780062464316.

Hybrid Round Table - HRT (2020). Digital Transformation Extended Future Outlook: Challenges, Adversaries, Divides & Opportunities, International Discussion, Sofia, Bulgaria, October 22-23, https://cutt.ly/4gxOZtf

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, ISBN: 978-1466687936.

Minchev, Z. (2019). Security Challenges to Critical Infrastructure of Future Smart Cities, In Proc of BISEC 2019, https://dx.doi.org/10.13140/RG.2.2.18120.75525

Minchev, Z. et al. (2019). Future Digital Society Resilience in the Informational Age, Sofia: SoftTrade & Institute of ICT, Bulgarian Academy of Sciences, ISBN: 978-954-334-221-1.

Minchev, Z. (2020). UK-BG Cyber-Security Newsletter, Issue 2, August, https://doi.org/10.11610/cybsec02

Minchev, Z. (2020a). Future Digital Society Transformational Transcendents & Gaps Extended Outlook, Romanian Cyber Security Journal, Spring 2020, No. 1, Vol. 2, pp. 11–18.

Minchev, Z. (2020b). 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, 2020, Kyiv, Ukraine, pp. 381-388.

Minchev, Z. (2020c). Digital Transformation – An Extended Future Outlook for the Balkans Region, Romanian

Cyber Security Journal, Autumn 2020, No. 2, Vol. 2, pp. 39–48.
Minchev, Z., Dukov, G., Boyadzhiev, D. & Mateev, P. (2016). Future Cyber Attacks Modelling & Forecasting, in ESGI 120 Problems & Final Reports, Sofia, Fastumprint, pp. 77-86.
NCOVID (2021). NATO and COVID-19, https://www.nato.int/cps/en/natohq/174592.htm
Pavlov, Y. & Andreev, R. (2013). Decision Control, Management, and Support in Adaptive and Complex Systems: Quantitative Models, IGI Global, ISBN: 978-1466629677.
Rasjid, S. (2020). Art of Diplomacy, Afterhoursbooks, ISBN: 978-602-6990-56-3.
Riordan, S. (2019). Cyberdiplomacy: Managing Security & Governance Online, Polity Press, ISBN: 978-1-5095-3407-4.
Schwab, K. & Vanham, P. (2021). Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet, WEF, John Wiley & Sons, ISBN: 978-1119756132.
SDF (2021). Securing Digital Future 21 Web Forum, http://securedfuture21.org
Snow, N. & Cull, N. (2020). Routledge Handbook of Public Diplomacy, Routledge, ISBN: 978-1-138-61086-6
Sophos Ransom (2020). The State of Ransomware 2020, SOPHOS White Paper, https://bit.ly/389TFNo
UNCOVID (2021). Coronavirus Global Health Emergency, https://www.un.org/en/coronavirus
Vester, F. (2007). The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity, Munchen: MCB–Verlag, ISBN: 9783939314059.
WHOCOVID (2021). Coronavirus Disease (COVID-19) pandemic, https://www.who.int/emergencies/diseases/novel-coronavirus-2019
WEFCOVID (2021). COVID Action Platform, https://www.weforum.org/platforms/covid-action-platform
WBCOVID (2021). The World Bank Group's Response to the COVID-19 (coronavirus) Pandemic, https://www.worldbank.org/en/who-we-are/news/coronavirus-covid19

Zlatogor MINCHEV

He 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.