

# **FUTURE DIGITAL SOCIETY RESILIENCE IN THE INFORMATIONAL AGE**

**Edited by  
Zlatogor Minchev**



## **Future Digital Society Resilience in the Informational Age**

Copyright © 2019 Institute of ICT, Bulgarian Academy of Sciences

Copyright © 2019 Softtrade

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the copyrights holders, except in the case of brief quotations embedded in critical articles or reviews.

Editor: Zlatogor Minchev

Content Reviewer: Velizar Shalamanov

Technical Editor: Stayka Angelova

Cover Design: Rositsa Petrova

First published: September 2019

Published by Softtrade

ISBN 978-954-334-221-1

## **Future Digital Society Resilience in the Informational Age**

Foreword	<i>Velizar Shalamanov</i>	5
Chapter 1:	Transcending Digital Transformation: Adversaries, Challenges and Opportunities – <i>Zlatogor Minchev</i>	9
Chapter 2:	Social, Political and International Aspects of Digital Society Formation – <i>Evgeni Krastev</i>	23
Chapter 3:	Economic & Investment Perspectives in the Digital Society – <i>Nedko Tagarev</i>	35
Chapter 4:	“Fake News” Disruption in the Digital Age – <i>Yulian Hristov</i>	53
Chapter 5:	Bitcoin: Present and Future Digital Challenges – <i>Luben Boyanov</i>	67
Chapter 6:	Challenges to Data Protection in Corporate Environment – <i>Ivan Gaydarski &amp; Zlatogor Minchev</i>	82
Chapter 7:	AI Future Progress from Neural Question Generation Perspective – <i>Teodor Toshkov</i>	101
Chapter 8:	Educational Games Future – <i>Elena Paunova-Hubenova</i>	114
Epilogue	Future Social Evolution of the Fourth Wave and Beyond – <i>Zlatogor Minchev</i>	128
Acknowledgements		131
Biographies		132



## Foreword

Modern technologies and especially ICTs are obviously the driver for a new digital society transformation that creates a lot of opportunities, but as well challenges. This naturally is going to establish numerous real threats of different kind, if we the people miss the responsibility for proper handling of their progress and applications. In this situation, having in mind security and safety critical roles, it is fair to say that information security, network security or even cyber security and resilience will stay of vital importance for the near future.

At the same time, digital resilience marked briefly as “digilience” is a new concept, combining digital transformation and cyber resilience towards a future big societal change in the new digital age.

These two research fields, together with high performance computing and artificial intelligence, as well as the development of digital skills are in the very core of the Euro-Atlantic current endeavours that go beyond year 2020, trying to adequately face the future world digital transcending<sup>1,2</sup>.

Being rather innovative, the academic capacity in this area for Bulgaria is still somewhat sparse and there is an obvious necessity for consolidation and creation of a suitable governance and management mechanisms in order to become successful at national level and also to properly harmonize the research efforts at international one.

In this context the initiative for research book preparation of Assoc. Prof. Dr. Zlatogor Minchev towards developing a framework for analysis, prognosis and validation of transcending digital transformation is quite timely and deserves admirations.

Though still fragmented and weakly connected, the gathered community of researchers, lecturers, innovative companies, practitioners and media experts, selected by the editor and inspirator of this book gives a promising prognostic snapshot for the upcoming digital future better understanding.

Formally, the idea for this research has been started in year 2017 as “Secure Digital Future 21” initiative<sup>3</sup> for expert and user professionals ideas and knowledge web exchange for the future digital society securing, receiving support both from the budget and through additional competitive projects participation, jointly with private sector sponsorships. The community nowadays covers about 50 countries around the world with above 100 participants from the five continents.

The present book is aiming to explore current challenges, adversaries and opportunities for the digital transformation, noting digilience necessity for the future digital society.

The ideas are spread in eight chapters based on promising research results in selected

---

<sup>1</sup> Digital Europe program: Funding digital transformation beyond 2020, [Online]. Available: [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2018\)628231](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)628231). [Accessed: 30-August-2019].

<sup>2</sup> The effort to modernize NATO’s infrastructure is known in the NATO Communication and Information Agency as the Digital Endeavor, [Online]. Available: <https://www.ncia.nato.int/NewsRoom/Pages/2019.03.019.aspx>. [Accessed: 30-August-2019].

<sup>3</sup> Secure Digital Future 21 Web Portal [Online]. Available: <http://securefuture21.org>, <https://www.facebook.com/groups/sdf21/>. [Accessed: 30-August-2019].

key areas, and we have to congratulate Assoc. Prof. Dr. Zlatogor Minchev as a new head of “IT for Security Department” at Institute of ICT, Bulgarian Academy of Sciences for the brave leadership and sustainable desire to continue and advanced the tradition started 10 years ago for reviewing and consolidating objectives for the known national security research results<sup>4</sup>, trying to go beyond with establishing a vision for the next 10 years.

The analytical framework is an original and rather extended development, partially derived from the methodology, assembled for defense planning and crisis management in the fields of scenario generation, analysis and multicriteria assessment about 15 years now<sup>5</sup>.

Naturally, several new key elements are added, providing a broader understanding towards the established models effectiveness assessment, cyclic behaviour exploration, combined with high-performance computational probabilistic validation and biometric response monitoring.

As far as the scope of any book is not able to cover the complete set of adversaries, challenges and opportunities to the digital transformation and digilience successful accomplishing an outline for the key ones is proposed. The approach is presenting an ambitious and successful attempt to review known current research in a network of experts and to feed it as a multi-institutional endeavor, targeting the definition of the research agenda for the next fifteen years towards year 2033.

In Chapter 1 “Transcending Digital Transformation: Adversaries, Challenges and Opportunities”, Zlatogor Minchev is setting up the reader security landscape with a comprehensive methodology for future foreseeing of digital transformation trends. It is actually presenting a framework for future research, established under his leadership during the last 10 years now, involving more and more key players and competencies in order to obtain both successful expert plausible beliefs extraction and a reliable future validation approach.

The other chapters, provide invited authors’ views on different implications of the digital transformation, noting socio-political, economic, security, computer science and education dimensions spread amongst three major blocks.

The first block of the book is about socio-political aspects of the digital transformation and is covered in Chapter 2 and Chapter 4 by professional journalists.

In Chapter 2 “Social, Political and International Aspects of Digital Society Formation”, provided by Evgeni Krastev an exploration of the evolution of the societal models is outlined. Further the study focuses on the transition processes in the “Third Wave”, giving accents to social, political an international relations assets. Additional notes on the post-information era of the future “Fourth Wave” with recognition of the complexity, increased speed of change and uncertainties to cope with it are also marked.

Very specific and challenging social and political phenomenon is covered in Chapter 4 ““Fake News” Disruption in the Digital Age” by Yulian Hristov. The author analyses the phenomenon of “fake news” and their influence on society with respective challenges – for the citizens, but for the journalists, as well – their professionalism and ethics, together

---

<sup>4</sup> Shalamanov, V. Minchev, Z., Tagarev, T. et al, SEcurity RESearch and Change Management in the Security Sector. The Bulgarian Experience 1999-2008, Sofia, Demetra Ltd, 2008, (in Bulgarian).

<sup>5</sup> Niemayer K., Shalamanov V., Tagatev T., Rademaker M. Operations Research Support to Force and Operations Planning in the New Security Environment: SfP981149, Sofia, Artgraf Ltd, 2009.

with technological discoveries like “deep fakes” and tries to warn us for the future of media information reliability.

The second block is bounded with Chapter 3 and Chapter 5, giving examples of the role of ITs in economic development, noting opportunities and challenges created by technologies. The two chapters are contributed by researchers from the University of National and World Economy.

Chapter 3 is prepared by Nedko Tagarev and is addressing the economic dimensions of the digital change “Economic & Investment Perspectives in the Digital Society”. His study is in the area of investments in the new technologies and the disruptive effects of these developments.

Another specific aspect of digital transformation is presented in Chapter 5 “Bitcoin: Present and Future Digital Challenges”, provided by Luben Boyanov, who is a computer science professional moved from the academy to the university, supporting the research and educational network idea progress. His study is focussed on digital currencies and their disruptive nature for the future economy, in case the mankind is not able to establish a resilient model of operation with the present bank system for the future.

The third block is focusing on human aspects of technology influence and is covered in Chapters 6, Chapter 7 & Chapter 8. The result is prepared by an analyst, who is also an entrepreneur from the private IT sector, jointly with the book editor and two young researchers from the academia community.

The cyber resilience and security of the organizations is covered in Chapter 6 “Challenges to Data Protection in Corporate Environment”, presenting results of a study, performed by Ivan Gaydarski and Zlatogor Minchev. In order to exploit the opportunities and to get the benefits of ICT and digital transformation in particular, it is evident that cyber security aspects need to be addressed properly on the organizational and personal level. The chapter explores the challenges and defines the necessary measures for assuring a sustainable corporate security and in the broader context – organizational ones, focusing on multiple data segments handling.

In Chapter 7 “AI Future Progress from Neural Question Generation Perspective”, Teodor Toshkov explores the problem of text comprehension as an important aspect of human-machine interaction in the modern web search engines and multiple teaching systems, noting also the possible effect on AI future progress. The paper is focussed on live models and algorithms for generating questions about facts in a text in order to test the level of understanding of the content by the machines. It is a powerful approach for learning, supported by machine reasoning and could bring changes in the future process of education and training, but not only.

Last but not least, Elena Paunova-Hubenova presents results from a research on using ICT in educational process even for children in Chapter 8 “Educational Games Future”. The study provides interesting results about the usage of ICT in the educational processes throughout the country, noting taught subjects and categories of students. The games are considered as the most effective ICT educational tool with specific requirements to be met by participants in order to exploit their potential.

The presented in this book chapters, prepared as an initiative of Assoc. Prof. Zlatogor Minchev for gathering researchers and professionals and discussing ideas towards successful

transcending of the digital future, together with the additional Epilogue for the post-informational age, accentuating on the upcoming quantum technologies disruptive effect are of high value and we have to congratulate him for this successful effort.

The future in itself could be bright, but definitely brings to us many challenges, that could turn into real threats, especially if the following scenarios become reality:

1. Group of people decide to use the new technologies in highly connected digital world against other human beings;
2. Technologies themselves become “independent” from the people, reaching singularity and turn into ones with adversary behavior for “their own” reasons out of human control;
3. Complexity, uncertainty and speed of processes in the digital world become too difficult and comprehensive for human control, so mistakes bring unintentional disasters that we are not be able to cope with.

Thus, in order to be able to deal successfully with the three main scenario threats outlined above, the following measures are necessary to be taken:

1. Maintain technological superiority to any potential adversaries, that will require very intensive research and innovation with younger and younger people involved;
2. Establish proper controls over the development of the technologies, keeping the “democratic human control” over and preventing the ability for turning against people intentionally;
3. Maintain “human-in-the-loop” with guarantees for safety and security of the technologies in the more complex, uncertain and fast changing digital environment.

Successfully addressing the identified adversaries, challenges and opportunities is not possible only with isolated work of even the most talented researchers, so consolidation is required with the adequate governance and management on academic, university and industrial national and international levels.

The specific nature of the digital transformation and the transcending digital future requires to involve in the research, experimentation and training young people with new bright and ingenious ideas – especially the new generations to come, being now still students at schools and universities. This is a field, where Dr. Minchev has also done and achieved a lot with young talents on mathematics and informatics, jointly with his invited classes on cybersecurity for university students during the last 15 years, bringing additional value and generation enrichment of the current research.

The book is a first comprehensive attempt to consolidate most of the available knowledge in a research framework for analysis, assessment and future trends prognosis. So, a lot of further efforts for maturing and cooperation extending will be supportive towards the successful meeting of the complex problems of governance, management and diligence in the digital transformation process, keeping the exploits and opportunities for the benefit of the society and people, while securing and preparing them for the transcending digital future.

*Assoc. Prof. Dr. Velizar Shalamanov*  
Deputy Director on e-Infrastructure & Security Issues  
Institute of ICT, Bulgarian Academy of Sciences

## Acknowledgments

The editor and co-author of the book Zlatogor Minchev would like to express his personal deepest gratitude to his family and colleagues for their patience, help and stimulation during the manuscript preparation.

Additional thanks for the technological and expert support is also given to the initiative “Secure Digital Future 21”<sup>1</sup>.

Explicit appreciation to the editor’s long-standing mentor in the security area – Velizar Shalamanov for the encouragement, positive attitude towards the idea and challenge acceptance for preparing the book review message to the readers.

Special acknowledgment for the financial support is also granted from the authors as follows:

Chapter 3 “Economic & Investment Perspectives in the Digital Society” to project “Economic Analysis of the Security of Smart Settlements”, University of National and World Economy, Sofia, NID NI-15/2018, 2018-2019.

Chapter 6 “Challenges to Data Protection in Corporate Environment” to: project “Modelling the Architecture of Information Security Systems in Organizations”, Ref. No: 72-00-40-230/10.05.2017, ICT Sciences & Technologies Panel, Program for Young Scientists and PhD Students Support – 2017, Bulgarian Academy of Sciences; National Scientific Program “Information and Communication Technologies for a Single Digital Market in Science, Education and Security – ICTinSES”, 2018-2020, financed by the Ministry of Education and Science, Republic of Bulgaria.

Chapter 8 “Educational Games Future” to projects: “Learning Data Analytics for ICT Resource Integration in Bulgarian Schools”, M02/1, contract DM 02/1, 13.12.2016; APOGEE – smArt adaPtive videO GamEs for Education, DN12/7/2017. Both funded by the Bulgarian National Science Fund.

Supplementary recognition is also provided to the editor’s friend and book co-author – Evgeni Krastev and Voennite Reporteri team of Military TV Channel for the preparation of the documentary film “Cybersecurity – The Challenge to the Young Generation”<sup>2</sup>, outlining the future Society 5.0 live experiment, during Research Summer School on Mathematics & Informatics 2018 – SRS’2018 marked in Chapter 1 “Transcending Digital Transformation: Adversaries, Challenges and Opportunities”.

Finally, a priviliged appreciation for the Epilogue “Future Social Evolution of the Fourth Wave and Beyond” exclusive consultancies and fruitful discussions is also given by the book editor to his colleagues: Galit Ben-Israel, Beit-Berl Academic College, Israel, Pier Luigi Capucci, Noema, Italy, Luben Boyanov, University of National & World Economy, Bulgaria, Albena Tchamova & Velizar Shalamanov, Institute of ICT, Bulgaria.

---

<sup>1</sup> Secure Digital Future 21 Web Portal [Online]. Available: <http://securefuture21.org>, <https://www.facebook.com/groups/sdf21/> [Accessed: 30-August-2019].

<sup>2</sup> E. Krastev, Cybersecurity – The Challenge to the Young Generation, Documentary Film, “Voennite Reporteri” Broadcast, Military TV Channel, November 4, 2018, [Online]. Available: <https://www.youtube.com/watch?v=1aO4j-VQSGU>. [Accessed: 30-August-2019].