Information & Security
Published since 1998

G. Sharkov, Ch. Todorova & P. Varbanov
vol. 50, no. 1 (2021): 11-22
https://doi.org/10.11610/isij.5030
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Strategies, Policies, and Standards in the EU Towards a Roadmap for Robust and Trustworthy AI Certification

George Sharkov [1,2] (✉), ***Christina Todorova*** [1, 2], ***Pavel Varbanov*** [1, 3]

[1] *European Software Institute – Center Eastern Europe, Sofia, Bulgaria https://esicenter.bg/*

[2] *Cybersecurity Laboratory at Sofia Tech Park, Bulgaria, https://sofiatech.bg/*

[3] *Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences, Sofia, Bulgaria, https://iict.bas.bg/*

Abstract:

Within recent years, governments in the EU member states have put increasing efforts into managing the scope and speed of socio-technical transformations due to rapid advances in Artificial Intelligence (AI). With the expanding deployment of AI in autonomous transportation, healthcare, defense, and surveillance, the topic of ethical and secure AI is coming to the forefront. However, even against the backdrop of a growing body of technical advancement and knowledge, the governance of AI-intensive technologies is still a work in progress facing numerous challenges in balancing between the ethical, legal and societal aspects of AI technologies on the one hand and investment, financial and technological on the other. Guaranteeing and providing access to reliable AI is a necessary prerequisite for the proper development of the sector. One way to approach this challenge is through governance and certification. This article discusses initiatives supporting a better understanding of the magnitude and depth of adoption of AI. Given the numerous ethical concerns posed by unstandardized AI, it further explains why certification and governance of AI are a milestone for the reliability and competitiveness of technological solutions.

Article Info:

Received: 01 Sep 2021
Revised: 16 Sep 2021
Online: 19 Sep 2021

Keywords:

artificial intelligence, governance, certification, ethics, lawfulness, security, trustworthy AI, robust AI

✉ Corresponding Author: George Sharkov; E-mail: gesha@esicenter.bg

Introduction

In recent years, ethical issues in all research areas have risen to the forefront, particularly in light of the COVID-19 epidemic, and artificial intelligence is no exception. The European Data Strategy recognized the development of the European Union as a role model for a society empowered by data as a crucial goal even before the outbreak of the epidemic.

Thanks to measures such as the General Data Protection Regulation and the European High-Level Expert Group on AI (AI-HLEG), ensuring and providing access to trustworthy AI is no longer only a competitive advantage but a basic necessity for the sector's healthy growth. The European Commission recently issued a proposal for a European Act on Artificial Intelligence (AIA) in April 2021.

Regulating Artificial Intelligence and ensuring the development of ethical AI solutions has become a fundamental approach towards the evolution of the potential of AI solutions. Moving towards lawful, ethical, and technologically robust AI, however, is not a recent initiative.

Making the initial steps toward regulating AI has been a topic of interest in Europe, especially within recent years. While AI systems have many benefits, they also carry many risks that need to be addressed carefully and appropriately. Topics, such as compliance, have been developed to support an ethical approach to Artificial Intelligence and promote a sense of responsibility among organizations, governments, institutions, and companies of all sizes.

To achieve the goal of reaching a common baseline of responsibility on such a large scale, definitions, and guidelines of human-centric artificial intelligence, do not suffice to promote human welfare and liberty through the creation of ethical artificial intelligence solutions. Governance and certification of artificial intelligence need to be implemented to serve as guidelines for the process.

Certifying artificial intelligence systems based on their lawfulness, reliability, and human-centricity, however, is not a task easy to achieve. The high degree of uncertainty and complexity based on the diverse applications of artificial intelligence has brought many challenges for the government to design and implement effective artificial intelligence governance policies.

In this paper, we discuss some challenges related to AI governance and certification as an important opportunity to shape the future and well-being of Europe. The paper is structured as follows:

The Introduction chapter provides a background for the topic of governance and certification in AI. The second section of the paper, "Lawful, Ethical and Technically Robust Artificial Intelligence," provides an overview of the necessity of these three pillars, as defined in the Ethics Guidelines for Trustworthy AI by the High-Level Expert Group on Artificial Intelligence (AI-HLEG). The third chapter provides a discussion on the topic of AI Governance and Certification, including some challenges to AI Governance, as well as the next steps to initiate AI Governance and Certification of AI, based on the currently existing standards on AI. The last chapter provides a summary of the conclusions from this study and subsequent actions and recommendations.

Lawful, Ethical and Technically Robust Artificial Intelligence

The reliability of artificial intelligence is a prerequisite for individuals and society to develop, implement and use artificial intelligence systems in a way it preserves their dignity, fundamental human rights, and freedoms. Without trust, the artificial intelligence system could endanger people, unintended with the possibility of a variety of unfavorable consequences occurring, thereby hindering the realization of the huge social and economic benefits that artificial intelligence can bring to the European digital market.

Confidence in the development, deployment and use of artificial intelligence systems not only refers to the inherent properties of the technology but also refers to the quality of the socio-technical systems involved in artificial intelligence applications.[1]

With AI being increasingly integrated into sectors, such as aviation, nuclear energy, and defense, the trustworthiness of artificial intelligence systems is no more just a feature but a necessary prerequisite to market. Therefore, striving to achieve reliable artificial intelligence not only refers to the reliability of the artificial intelligence system itself but also requires a holistic and systematic approach, including the reliability of all participants and processes that are part of the social-technical background of the system.

The AI-HLEG defines three main components of trustworthy AI, which should be met throughout the system's entire life cycle:

1. *lawful*, complying with all applicable laws and regulations;
2. *ethical*, ensuring adherence to ethical principles and values;
3. *robust and secure*, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm.

Each of the above-mentioned components is necessary but not self-sufficient on its own to guarantee the trustworthiness of AI. Ideally, these three are coordinated and overlapping in operation.

As a society, our individual and collective responsibility are to work hard to ensure that all three components contribute to the security of reliable artificial intelligence. A reliable method is a key to achieving "responsible competitiveness." It provides a basis for all those affected by artificial intelligence systems to ensure that their design, development, and use are legally and ethically sound.

The High-Level Expert Group on AI has further proposed a set of seven key requirements that an artificial intelligence system must meet to be considered reliable. Specific evaluation checklists are designed to help verify the application of each key requirement.

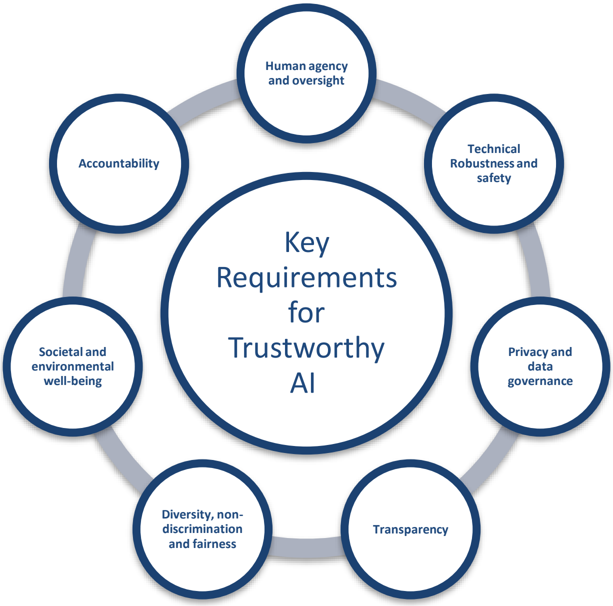
Human agency and oversight
Technical Robustness and safety
Privacy and data governance
Transparency
Diversity, non-discrimination and fairness
Societal and environmental well-being
Accountability
Key Requirements for Trustworthy AI

Figure 1 Key Requirements for Trustworthy AI by the Ethics Guidelines for Trustworthy AI by the High-Level Expert Group on Artificial Intelligence

These requirements aim to promote responsible and sustainable artificial intelligence innovation in Europe, seeking to use ethics as the central pillar of the development of unique methods of artificial intelligence, aimed at benefiting, empowering, and protecting the prosperity of individual human beings and the common interests of society.

Following the establishment of the High-Level Group on AI, it seemed like a logical translation of those guidelines and recommendations into a legal framework,[2,3] however, the entire work conducted under this High-Level Group, showed us the complexity of the realization of such next steps.

Two years later, following a series of other initiatives in the field of Artificial Intelligence governance and standardization on a global, European, and national levels alike, the European Commission published the proposal of the new EU Artificial Intelligence Act (AIA), which is among the first initiatives worldwide, aiming to provide a legal framework for AI. It follows the *risk-based approach to AI* development, implementation and use, introduced earlier in 2020 with the White paper on AI [4] by the Commission, and also referring widely to the outcomes and recommendations by the AI-HLEG on the trustworthy AI. As part of AIA, the idea to appoint national bodies responsible for the standardization and supervision of AI development has risen to the forefront, with the hope to put the EU in a position of "leadership by example" on the global stage, as one of the pioneers in reliable artificial intelligence worldwide.

Therefore, encouraging the governance and certification for achieving trusted artificial intelligence solutions is considered fundamental for promoting and maintaining basic human rights-based across Europe. And only by ensuring credibility can European citizens, as well as citizens worldwide by consequence, will be able to fully reap the benefits of artificial intelligence systems and be sure that steps have been taken to prevent potential risks.

AI Governance and Certification

With the development and complexity of artificial intelligence systems, their risks and interconnectivity with other complex Systems-of-Systems will also increase, requiring the creation of specific governance mechanisms, including for particular industrial sectors, due to the diversity of the applications of AI.

Challenges to AI Governance

The high degree of uncertainty and complexity in the field of artificial intelligence has brought many challenges for governments to design and implement effective artificial intelligence governance policies.

Many of the challenges posed by artificial intelligence stem from the unpredictability and the non-homogenous nature of AI applications, making it difficult for governments to set specific goals in their policies [5] and legal frameworks. Thus, the inherent opacity and unpredictability of machine learning systems pose technical challenges for the compliance assessment of artificial intelligence against established standards, strategies, and policies.

Among the core challenges, related to ensuring compliance against existing standards, explainability and non-discrimination take center stage. As also expressed in article 22 of the GDPR,[6] this concerns the right of the users to request an explanation of an algorithmic decision that was made about them and avoiding discrimination in that decision. Consequently, more questions arise in connection to this topic, including how can transparency and fairness be ensured when decisions are being made by artificial intelligence, and especially in cases where human intervention is required. Nevertheless, the GDPR states that "properly applied algorithms" can outweigh human accuracy in terms of output. However, the design, development, and implementation of such artificial intelligence solutions, requires strict compliance with standards, policies, and regulations for ethical artificial intelligence development, which further requires additional resources, such as ethical backbones, including certification and standardization bodies, to ensure compliance. This leads us to the starting point of this discussion.

The lack of human controllability over the behavior of AI systems further suggests a difficulty of assigning liability and accountability for harms resulting from software defects, as manufacturers and programmers often cannot predict the inputs and design rules that could yield unsafe or discriminatory outcomes.[7]

In this regard, the European Union has already enforced quite strict standards, as compared to the US, for example, which are likely to adopt an antitrust approach,[8] conversely to the EU approach for ethical compliance.

Furthermore, data fragmentation and lack of interoperability between systems limit the organization's control over the entire life cycle of data flow. The shared role between different parties in data exchange covers AI-driven decisions/events and the parties involved in the promotion.[9]

Conversely, information mismatch between technology companies and regulators exacerbates the latter's difficulties in understanding and applying new or existing legislation to artificial intelligence applications.[10]

Regulators are putting in intense efforts to fill these information gaps and are falling behind due to the rapid development of technology, which in turn leads to laws that are "too general" or "vague" and lack the specificity of effective regulatory technology.[11]

In particular, legislators may not be able to outline the specific rules and responsibilities of algorithm programmers to allow for future experiments and code modifications to improve software, but in doing so, programmers have room to evade responsibility and accountability of accounts by the resulting behavior of the system.

Steering Governance

The issues raised in the preceding section lead to a whole other subset of problems related to the level of government involvement in AI research, development, deployment, and application.

Without a doubt, the key to steering the governance of AI lies in promoting proper mechanisms and instruments for government support and encouragement of AI-related capacity development, including structured methodologies and sector-based guidelines to support organizations in overseeing the compliance of AI-based goods.

One approach to achieving this balance between fostering technological progress while still ensuring compliance with applicable standards for AI is proposed in the AIA from April 2021. The method proposed by the EC in this document follows a process of prolonged research and assessment phases injuring the laboratory and market testing processes while overseeing the proper insurance of mechanisms, supporting organizations in this development phase.

In its impetus to encompass as many application areas as possible, to overcome uncertainty, and steer singularity, the European Commission's proposal mentions in specific contexts or lists risky components, technologies, products, processes, and concepts. One such example concerns the biometric identification and categorization of natural persons, which is high ranking in the High-Risk AI Systems list. However, biometrics-based AI technologies hold tremendous potential to enhance the e-government processes and facilitate citizens in their interactions with the authorities.

In general, due to erroneous interpretation, the vast majority of the aforementioned AI concepts, technology, and applications could be taken out of context and barred from further research and development by national governments.

The implementation of such regulations should be thoroughly examined, and related dangers should be taken into account while steering governance for AI solutions.

An approach to mitigate this danger, discussed, once again in AIA, is to granulate the regulatory bodies on a national level, however ensuring their centralization into a European Artificial Intelligence Board. Said Board will consist of representatives from every Member state to assist national supervisory authorities in the decision-making regarding high-risk AI systems and ensure a body of competence regarding AI risk assessment and management.

Audit, Certification, and Compliance of AI

The use of artificial intelligence (AI) is one of the most important technological contributions that will penetrate the life of Western society in the next few years, not only providing important benefits but also highlighting risks that need to be assessed and minimized.

A widely recognized practice for the provision of such a guarantee is the standardization cycle. The development process for AI-related standards, as well as relevant methodologies for conformity assessment, maintenance procedures, and accreditation bodies, is still in progress. No specific all-encompassing approach towards the standardization of AI can be identified at this point at the European level.

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) have established a new Joint Technical Committee 21 "Artificial Intelligence," as a part of the response of both associations to the EC White Paper on AI and the German Standardization Roadmap for Artificial Intelligence.

The new JTC 21 is responsible for the development and adoption of standards for AI and related data. In particular, CEN-CLC/JTC 21 identifies and adopts international standards already available or under development from other organizations like ISO/IEC JTC 1 and its subcommittees. CEN-CLC/JTC 21 claims to focus on addressing the European market and societal needs, as well as underpinning EU legislation, policies, principles, and values.

The European Telecommunications Standards Institute (ETSI) describes its intentions to the AI in a white paper issued in June 2020. The focus and related *objectives of ETSI on the subject of AI* could be summarized as follows:

- *to ensure interoperability, and harmonized terminology*, including concepts, and semantics;
- *to provide horizontal space for the interchange of formats* for machine learning data models and algorithms interchange that ensures adaptive governance;

- *to foster piloting and testing of AI solutions*;
- *to provide a framework for the certification of trustworthy AI.*

Among the thematical areas where ETSI intends to develop standardization activities are 5G, IoT, data acquisition and management, security and privacy, testing, societal applications of AI and health.

Significant progress is achieved by the Technical Committee (TC) CYBER (Cybersecurity) [12] in the domain of Internet of Things (Conformance Assessment of Baseline Requirements issued in 2021), the establishment of the ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI), whose main task is to *develop technical specifications and reports to address three aspects of artificial intelligence in standards*, namely:

- *Securing AI from attacks*. (Cybersecurity for AI). Where AI is a component in a system that needs protection.
- *Mitigating malicious AI*. (Misuse of AI) Where AI is used to improve and enhance conventional attack vectors or create new attack vectors.
- *Using AI to enhance security measures*. (AI for Cybersecurity) protecting systems against an attack, where using AI is part of the 'solution' or is used to improve and enhance more conventional countermeasures.

The ISG SAI's first outputs, on the other hand, will revolve around six key topics:

1. *Problem Statement* that will guide the work of the group.
2. *Threat Ontology for AI*, to align terminology.
3. *Data Supply Chain* focused on data issues and risks in training AI.
4. *Mitigation Strategy*, with guidance to mitigate the impact of AI threats
5. *Security testing of AI*.
6. *Role of hardware in the security of AI*.

It is expected that the conformity assessments are based on standards, legislation, and regulations. However, the present situation is that SMEs, as well as various critical infrastructures (most of which are considered as "risky" for AI applications), are not well involved in the standards development as they are under-represented in standardization organizations. Additionally, strong concerns about the impact of AIA on SMEs have been expressed, especially in terms of costs, technical issues, quality assurance and certification, and the impact on innovation. A special focus on SMEs and affordability, as well as opportunities for innovation and creativity, are strongly recommended by numerous published feedbacks on the proposed AIA. In addition, various specific requirements, like those regarding data quality, requiring data to be "error-free" and "complete," are unrealistic in practice for AI (machine learning) systems.

This shows that discussions on standardization and certification of Artificial Intelligence are only as fruitful as their sector-based and user-level granularity. Nonetheless, standardization bodies must continue to focus on unifying the understanding of AI, its components, applications, industrial specifics, and cross-sector commonalities, allowing space for differences in sector-based components, as well as ensuring that those components comply with the ethical and security requirements developed by international, European, and national authorities.

A quick review on the ongoing AI-related standardization work of the European standards development organizations (SDOs) – ETSI and CEN/CENELEC, as well as the publicly announced work of ISO/IEC JTC1/SC42 and ITU committees, shows that the development of AI-related standards is in a very early stage. The work in progress is related mainly to the definition of the AI threats landscape and relevant terminology, AI data lifecycle management, AI data quality for machine learning and analytics, functional safety of AI systems. There are already published ITU standards on the integration of machine learning into 5G and future networks. However, only a few of the standards under development are somehow addressing the testing and assessments, and they are in a very narrow niche and scope (like the ISO/IEC Technical Specification 4213 draft - Assessment of machine learning classification performance).

ETSI ISG SAI has published so far only a few technical reports (like "Data Supply Chain Security" and the extensive "Mitigation Strategy Report"), which are paving the way for standards.[13]

The AI Act is still a draft in a very advanced stage of discussion and near future adoption, and it will complement the GDPR, in force since 2018, and the other three proposed drafts from November-December 2020 – the Digital Services Act, the Digital Markets Act, and the Data Governance Act. However, the AIA is the one imposing the development of the AI certification framework. On the other hand, the AI systems will be forced to comply with all other regulations, plus the sectoral ones, like the already announced Health Data Space legislative proposal.[14] The AI certification framework and respective relevant standards will also need to be synchronized with the ongoing development of the Cybersecurity Certification Framework and Schemes, as stipulated by the Cybersecurity Act (in force since 2019). Since the AI systems are basically software/IT systems from the technical viewpoint, it is not straightforward how the requirements will be integrated or merged and how respective assessments and certifications will be performed.

Conclusions

Artificial Intelligence has become an important cornerstone of the technological development of this century, as well as an indispensable element for the future development of the European digital market.

This poses the requirement to ensure that artificial intelligence technology, artificial intelligence products, and AI services comply with applicable laws and regulations as much as possible. Regulations strictly abide by generally accepted ethical principles.

This can only be achieved through an adequate combination of governance and certification, leveraged by an independent auditing process.

The goal of this paper is to contribute to the ongoing discussion related to the necessity of ensuring proper implementation of human-centered artificial intelligence and ethical issues of AI.

Given the public's interest in the integration of AI in all industrial sectors, it is important to ensure compliance with ethical standards and guidelines already in place. With the realization that the multiple responsibilities for the ethical deployment of AI solutions lie within the individual organizations, which are either deploying, integrating, or developing AI, the ultimate responsibility of society to educate, set controls, and resilience mechanisms become ever more evident and crucial.

In this paper, we provided an overview of some recent European initiatives towards the standardization, policymaking, and certification in the field of Artificial Intelligence. We discussed some cornerstones necessary to steer the governance and certification of AI, as well as some challenges, which slow down the process. We argue that Europe currently needs AI regulation, standardization, and compliance with ethical principles more than it needs innovation in the field, which is already quite mature. However, a balance must be achieved between rigid regulation rules and defined "red lines" for AI applications (underlined in AIA, also as "high-risk" sectors or areas) and the ability to innovate and experiment. Some vague or very strict formulations in the AIA have provoked numerous negative comments during the public discussion. In addition, the implementation and conformity assessments cost in the context of the binding legal force by AIA (it is a Regulation, mandatory for all member states) will become yet another unbearable burden for small-medium enterprises (SMEs). A strong opinion is commonly expressed by various digital SMEs organizations,[15] stating that "the proposal, in its current form, is likely to hamper innovation and overburden SMEs."

Finally, we put forth the proposition that regulating Artificial Intelligence and ensuring the development of ethical AI solutions has become a fundamental approach not only towards the evolution of the potential of AI solutions but also for protecting the basic human rights of European citizens, as well as a leader by example in the global stage of AI innovation.

References

[1] European Commission's High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI," 2020, https://doi.org/10.2759/346720.

[2] Luciano Floridi, "The European Legislation on AI: a Brief Analysis of its Philosophical Approach," *Philosophy & Technology* 34 (2021): 215–222, https://doi.org/10.1007/s13347-021-00460-9.

[3] European Commission, "Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts," EUR-Lex - 52021PC0206, 21 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR:e0649735-a372-11eb-9585-01aa75ed71a1.

[4] European Commission, "White Paper on AI - A European approach to excellence and trust," 19 February 2020, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[5] Stefan Larsson, "AI in the EU: Ethical Guidelines as a Governance Tool," in *The European Union and the Technology Shift,* edited by Antonina Bakardjieva Engelbrekt, Karin Leijon, Anna Michalski, and Lars Oxelheim (Cham: Palgrave Macmillan, 2021), 85-111, https://doi.org/10.1007/978-3-030-63672-2_4.

[6] Bryce Goodman and Seth Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation,'" *AI Magazine* 38 no. 3 (2017): 50–57, https://doi.org/10.1609/aimag.v38i3.2741.

[7] Joshua Kroll, Joanna Huey, Solon Barocas, Edward Felten, Joel Reidenberg, David Robinson, and Harlan Yu, "Accountable Algorithms," *University of Pensilvania Literature Revue* 165, no. 3 (2017): 633, https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/.

[8] Corinne Cath, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi, "Artifcial Intelligence and the 'Good Society': The US, EU, and UK approach," *Science and Engineering Ethics* 24, no. 2 (2018): 505–528, https://doi.org/10.1007/s11948-017-9901-7.

[9] Marijn Janssen, Paul Brous, Elsa Estevez, Luis S. Barbosa, and Tomasz Janowski, "Data Governance: Organising Data for Trustworthy Artificial Intelligence," *Government Information Quarterly* 37, no. 3 (2020): 101493, https://doi.org/10.1016/j.giq.2020.101493.

[10] Araz Taeihagh, M. Ramesh, and Michael Howlett, "Assessing the Regulatory Challenges of Emerging Disruptive Technologies," *Regulation and Governance*, (March 2021), https://doi.org/10.1111/rego.12392.

[11] Stefan Larsson, "On the Governance of Artificial Intelligence Through Ethics Guidelines," *Journal of Law and Society* 1, no. 23 (2020).

[12] ETSI Technical Committee on Cybersecurity, "Cybersecurity for Consumer Internet of Things: Conformance Assessment of Baseline Requirments," DTS/CYBER-0050, 2021, https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

[13] ETSI ISG SAI, "Latest Publications," September 2021, https://www.etsi.org/committee/1640-sai. accessed September 1, 2021.

[14] European Commission, "European Health Data Space," 2021, https://ec.europa.eu/health/ehealth/dataspace_en.

[15] SBS (Small Business Standards), "Artificial Intelligence Act: The harmonised approach to support SMEs, encourage SME participation in standardisation and promote

innovation," position paper, September 2021, www.sbs-sme.eu/news/artificial-intelligence-act-harmonised-approach-support-smes-encourage-sme-participation, accessed September 13, 2021.

About the Authors

George Sharkov is a former Cybersecurity Adviser to the Minister of Defense and served as a National Cybersecurity Coordinator for the Bulgarian Government within the period 2014-2017. He was leading the development of the National Cybersecurity Strategy of Bulgaria, adopted in 2016. He holds a Ph.D. in Artificial Intelligence (AI), with a specialization in applied informatics, thermography, genetics, and intelligent systems. Since 2003 he is the Director of the European Software Institute – Center Eastern Europe and Lead of the Cyber Resilience Lab (CyResLab) of ESI CEE in partnership with CERT-SEI, Carnegie Mellon University. Since 2016, he is also Head of the Cybersecurity Lab at Sofia Tech Park. He is a trainer and an appraiser in software engineering quality management, cybersecurity, and resilience (SEI/CERT RMM), while also lecturing in software quality, cybersecurity, and business resilience in three leading Bulgarian universities. https://orcid.org/0000-0001-5086-311X

Christina Todorova is a researcher at the European Software Institute – Center Eastern Europe and an expert at the Research and Development and Innovation Consortium (Sofia Tech Park JSC) with a particular area of expertise being design of digitally enhanced learning experience and curricula, especially through educational robotics, mobile applications, and virtual learning environments. Her most recent research focuses on projects for cybersecurity education for teachers and high-school students, cybersecurity training, and exercises, as well as human-centered artificial intelligence higher education curricula. https://orcid.org/0000-0002-8061-2941

Pavel Varbanov is a project coordinator at the European Software Institute – Center Eastern Europe and a researcher at the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences. The main focus of his work revolves around the design, development, and management of projects in the field of training and education, digital innovation, and cybersecurity. His scientific interests cover innovative educational methods, competence frameworks and taxonomies, digital divide solutions, as well as and social and professional communications. His most recent research is directed towards the adaptation of cyber-defense training content to the specific needs of the industry and professionals from other domains, cybersecurity certification, and security of new technologies. https://orcid.org/0000-0002-1868-8638