Towards secured digital business ecosystems: From threats to opportunities

1st Vesna Tornjanski
Faculty of Organizational Sciences
University of Belgrade
Belgrade, Serbia
vtornjanski@gmail.com
https://orcid.org/0000-0001-9727-8364

2nd Snežana Knežević
Faculty of Organizational Sciences
University of Belgrade
Belgrade, Serbia
snezana.knezevic@fon.bg.ac.rs
https://orcid.org/0000-0003-0176-6107

3rd Dejan Ljubanić
Faculty of Mathematics
University of Belgrade
Belgrade, Serbia
dejan.ljubanic@gmail.com

4th Vladimir Glišić
Faculty of Information Technologies
Alfa BK University
Belgrade, Serbia
vladimir.glisic@gmail.com

5th Danijela Žižić
Faculty of Mathematics
University of Belgrade
Belgrade, Serbia
dana.zizic@gmail.com

6th Jovan Travica
Singidunum University
Belgrade, Serbia
jovan.s.travica@gmail.com
https://orcid.org /0000-0001-9042-1703

***Abstract*— This study aims at shedding more light on values of the security landscape in the age of rapid digital businesses ecosystems development. The purpose of the paper is to enrich existing theoretical funds by providing a deeper and extended perspective on building secured digital business ecosystems, based on secondary data collection. The paper illuminates security gaps and emphasizes opportunities to effectively shift threats to sustainable value creation. Future research and management framework rely heavily on a switch from push-based to pull-based security ecosystem, protection strategies development, adoption of AI against cyber risks, and security culture development. The transformative journey towards long-term wellbeing to stakeholders included in the secured digital business ecosystems significantly lies in the multidisciplinary knowledge, simultaneous effectiveness of strategic change, and security management on one hand, and efficiency of IT and organizational capabilities, on the other. The article may contribute to academics, business owners, shareholders, strategic change, security, innovation, and IT management.**

Keywords—Secured digital business ecosystem, pull-based security landscape, AI, security culture, effective strategic change and security management, efficient IT and organizational capabilities.

I. INTRODUCTION

Worldwide phenomena characterized by undergoing Industry 4.0 and forthcoming Industry 5.0 fashions significantly yield and reshape concepts, principles, models, methods, practices, products, services, and habits worldwide with the ultimate goal to enable and achieve a sustainable future for the long-term wellbeing and prosperity of businesses and societies at a global scale [1], [2] [3].

The ever-present phenomenon of Industry 4.0 drives strategic change and digitalization in a thrilling way [4], creates valuable opportunities, and accelerates various challenges in a business ecosystem, at the same time. Digitalization breaks down organizational, industry, country, and regional boundaries and sets new rules at the open market [5]. The advancements of digital technologies have built a strong foundation for the development of a digital business ecosystem (hereafter: DBE) [6]. DBE creates a significant shift from traditional to innovative business and operating models, consisting of various entities that jointly create values for all involved stakeholders through information and communication technologies (hereafter: ICT) [7]. DBE exceeds traditional horizons to spark open and flexible competition and strengthen partnerships with involved stakeholders in a digital business ecosystem. Many organizations have recognized DBE as a valuable innovative approach to leverage resources (e.g. technology, specialized services) in cross-industries to adequately respond to and satisfy customers and market needs [7].

Despite various valuable opportunities and exchange dynamics capabilities that the digital business ecosystem may provide, interconnected heterogeneous partners in new forms of networks founded on digital infrastructure signify challenges required to be revealed and further analyzed to prevent the entire ecosystem from potential threats. To maximize potentials from the digital business ecosystem in terms of sustainable value creation, security gaps need to be narrowed and all entities secured in a digital long-term journey [8]. With the rapid development of IoT, Big Data, Smart grid, Blockchain, 5G, 6G, Cloud Computing, and other digital innovations that enable societies and businesses to be worldwide connected, the effectiveness of cybersecurity comes to the flour. Cybersecurity, aiming at simultaneously protecting organizations from threats and ensuring business continuity without interruptions, represents one of the hottest topics for both private and public organizations globally [9], [10].

With that in mind, this paper seeks to holistically understand and integrate security risks that may disturb the digital business ecosystem and shed light on the future perspectives towards sustainable value creation, based on secondary data collection.

II. LITERATURE REVIEW

A. The digital business ecosystem development

Digital innovation and open innovation paradigms have revolutionary changed ways of how organizations collaborate, compete, sustain, grow and create values in a business ecosystem nowadays [7], [11], [12], [13], [14]. Digital business in Industry 4.0 represents a key strategic topic and leading strategic transformation patterns for organizations at a global scale [15].

The transformative journey may be viewed from different perspectives and adopted at different levels. At an organizational level, the foundation of change lies in a rethinking of existing business models and moving toward business networks [15]. A business network or networked enterprise is a concept designed for organizations to smoothly fit the external business environment conditions characterized by volatility, uncertainty, and unpredictability. The strengths of the enterprise network as the organizational form imply the shift from vertical bureaucracies to horizontal enterprise supported by the digital technology that effectively connects and relates various dispersed organizational nodes creating a model of network organization. A network organization consists of organizational components that create synergy from advantages of bureaucratic organization and structure that accelerates innovations [16], [6], [17], [18].

However, organizations represent both open and evolving systems on one hand, and subsystems in a business ecosystem, on the other [17], [19], [20]. The birth of a business ecosystem saw the light during the '90s as a response to a sustainable solution for businesses on which basis is innovation. More specifically, it was recognized that innovative businesses cannot survive and evolve in a vacuum, but rather should extend collaborative network that exceeds the boundaries of an organization and even industries to gain a competitive advantage [21], [6]. A business ecosystem concept has evolved, changing the way of understanding, and depth and breadth of stakeholders included in a business ecosystem [22].

Rapid technological developments and the internet boom have created a strong foundation for digital business ecosystem development (hereafter: DBE). The DBE was introduced by European Union with the primary objective to achieve sustainable socio-economic development by supporting the SME community, boosting SME presence at global trade, and an increasing presence of SMEs at the global supply chain market, using potentials of ICT [6], [22], [23]. In contrast to the business ecosystem, the DBE concept is based on digital technology. A digital business ecosystem is defined as a "socio-technical environment of individuals, organizations and digital technologies with collaborative and competitive relationships to co-create value through shared digital platforms" [7] and is multifaceted in its basis, viewed as a concept, as a technology, and as a project [7].

DBE paradigm represents a shift from traditional to innovative business and operating models, breaking down organizational, industry's, country's, and regional's bounders. DBE allows businesses worldwide to create powerful value to societies and economies through an open and flexible business model based on the strengths and potentials that the digital era brought. DBE is conceptualized with the opportunity to create a mega-region built on coherent digital space to effectively meet customers' and markets' needs on one hand and to ensure organizations' survival, growth, and long-term sustainability, on the other. Putting DBE in the context of Industry 5.0 / Society 5.0 vision, the concept yields immense potential for boosting a digital economy and increasing the quality of life for humans in a new human-centered global society [7], [2] [24] [25]. However, the effectiveness of long-term sustainable value generation in DBE is in downhill correlation with the challenges that should be adequately recognized, observed, and transformed into opportunities. The next chapter introduces DBE challenges viewed from the security risks perspective.

B. The digital business ecosystem security risks

The new-age digital technologies inspired by Industry 4.0 introduce a fast development of cyberspace nowadays, making machines and devices more connected. However, exponential growth in information access opens a door for malicious intentions to disturb DBE if security is weak. Many organizations have changed their way of doing business in recent years and in particular during the COVID-19 era. Organizations have faced increased numbers, frequency, and strength of cyberattacks. Recent researches have shown that 2019 was characterized by approximately 2 billion vulnerabilities to IoT, while business discontinuity and cyber incidents have been the biggest threat to organizations during 2020 [26], [27], [28].

Cyber threats continue to evolve and the results show that financial and non-financial losses may seriously impact governments, organizations, individuals, and all cyber world. Federal Bureau of Investigation (hereafter: FBI) report stated that the average number of ransomware attacks on organizations counts 4,000 attacks daily [29], [30]. The cost of cyber attacks amounted to more than $5 billion in 2017 and estimations show that annual losses will reach more than $6 trillion by the end of 2021. The costs encompass losses of reputation, revenue, and sensitive information that impacted around 49% of organizations globally. Accordingly, the security aspect became one of the most serious concerns for organizations of all sizes [30].

Cybersecurity is defined as the "*preservation of confidentiality, integrity, and availability of information in the Cyberspace*" (hereafter: CIA) [31] [32]. Cybersecurity aims to simultaneously prevent organizations from cyber attacks, data breaches, and other potential cyber threats and to ensure business continuity without interruptions [9], [10], [28]. In other words, cybersecurity includes the convergence of technology, processes, and people to protect organizations, employees/individuals, and networks from cyber attacks, implying reputation enhancing, core competencies facilitating, and superior organizational performance achieving [30].

To effectively protect stakeholders, cybersecurity readiness should be at a high level. In contrast, if cybersecurity readiness is absent or low, the bottom-line performance of an entity may be seriously affected [30], [33]. However, cybersecurity continuously evolves and recently has reached a new level that is in line with the digital business development growth rate [28].

Nevertheless, a significant role in the further development of DBE understood from the Industry 5.0 point of view has the cybersecurity landscape defined at a country level. Around 70 nations worldwide have recognized the

significance of designing a National Cyber and Information Security Strategy, and the legal framework to effectively protect and defend countries from cyber-attacks [35], [28]. According to the National Cyber Security Index, the top ten countries that are the best prepared against cyber risks are [34]:

1. Greece,
2. Czech Republic,
3. Estonia,
4. Lithuania,
5. Spain,
6. Poland,
7. Belgium,
8. Finland,
9. France,
10. Slovakia.

To maximize potentials from DBE in terms of sustainable value creation in the context of Industry 5.0, the paper seeks to holistically understand and integrate security risks that may disturb DBE. Besides, the paper provides future perspectives towards sustainable value creation, by narrowing security gaps to effectively create a basis for secured DBE in the long run. The research results are depicted in chapter IV of the paper.

III. Research methods

The paper opted for secondary data collection, a research method that is based on a literature review. The research method that consists of a five-stage process of the literature review is followed by Senyo, Liu, and Effah (2019) [7] and is depicted in Table I.

TABLE I. A five-stage research method process

No.	The systematic literature review process	
	Stage description	***Sub-stage description***
Stage 1	Research criteria definition	Relevant sources are taken into account only
Stage 2	Literature search	Kobson database and Google academic
Stage 3	Literature refinement	Manual filtering of downloaded articles
Stage 4	Analysis of selected articles	Reading and selecting the content
Stage 5	Presentation of key research results and implications	Conclusion making

IV. Research results and implications

Based on the newest literature review, research results show that a secured digital business ecosystem represents a shift from threats to opportunities by integrating all security aspects. Integrated security aspects refer to all security components required to be holistically viewed and embedded into an entire digital business ecosystem to effectively achieve business continuity, sustainable value creation, and long-term wellbeing and prosperity for societies and businesses [1], [2].

In other words, as the world becomes more connected and smaller accordingly, cyber is getting stronger and bigger [4]. To transform threats into a valuable sustainable digital environment, in the long run, research findings indicate that integrated hard and soft security components should be incorporated into a digital business ecosystem. Hard and soft components of the security landscape towards sustainability are as follows:

- Multidisciplinary knowledge continuous development
- Strategic change management on the top of the transformative journey [4]
- Strategic change leadership knowledge and skills on the top of driving change [4]
- Cyber expertise development [4]
- Security strategy development using a shift from push-based to pull-based security ecosystem approach [36]
- Security culture development and adoption [37], [38]
    - Information security culture and information protection culture development and adoption [39], [40], [41], [42], [43]
    - Cybersecurity culture development to influence behavior of employees [44]
- Security of digital services chains services [45]
- Shift from virtualization security issues to cloud protection opportunities [46], [47]
- Network protection [48]
- IoT and SIoT security [49], [50]
- Blockchain technology security [51]
- Big data security [52], [53], [54]
- 5G security and privacy [55]
- 6G security and privacy [56]
- Cybersecurity on smart grid solutions [57]
- Artificial intelligence (AI) and machine learning against cyber risks [58], [59], [60], [61]

Table II depicts the integrated digital business ecosystem components with recognized risk types and solutions for further response against threats in the cyber world. In addition, the paper provides an overview of key cybersecurity products mapped with related cybersecurity types that are shown in Table III.

TABLE II. THE INTEGRATION OF THE DBE COMPONENTS: FROM THREATS TO OPPORTUNITIES

No.	Security related component	Risk (threat) type	Opportunity for risk mitigation	Source
1	Knowledge, skills and expertise	Lack of multidisciplinary knowledge Poor cyber and cyber security expertise	• Multidisciplinary knowledge development in the area of: o Organizational design; o Strategic change management; o Organizational change management; o Cyber security management, o IT management;	[4] [17] [18] [19]
2	Strategic perspective	Low countries, organizational and individual readiness for the cyber world Lack of governments and organizational strategic management support Lack of security strategy development at country and organizational levels	• Security strategy development using a shift from push-based to pull-based security ecosystem approach; • Security landscape definition and development; • Country readiness for the cyber world; • Organizational readiness for the cyber world; • Private individuals readiness for the cyber world; • Strong and effective government support in the transformative journey; • Strong and effective strategic management support at organizational level; • Empowerment of open innovation paradigm into transformative journey;	[30] [33] [34] [36] [1] [2] [13]
3	Security culture	Low level of security culture: from governments to individuals: • Information security culture; • Cyber security culture;	• Security culture development and adoption at all levels - from governments to individuals: o Information security culture and information protection culture development and adoption; o Cyber security culture development and adoption;	[37] [38] [39] [40] [41] [42] [43] [44]
4	Security of digital services chains services	Behavior of entire system	Agile development introduces novel security and privacy models, taking into account that the sequential process of traditional security engineering does not fit into new development approaches. Key features of new solutions are based on the following characteristics: • Security services that integrate IoT and Cloud in unified security solutions at an organizational level and are beyond the perimeter model; • Centralized AI and machine learning paradigms that are applied to wide sets of data, aggregated across various multiple control points, and big data capabilities; • Efficient architectures designed to reduce the overhead of security appliances, based on the segregation of detection intelligence, monitoring tasks, agentless deployment, monitoring of probes for low-end-hardware, antivirus on-demand; • Correlation techniques' improvement with the aim to recognize unknown attacks: • Security processes integration such as vulnerability assessment, advanced search, automatic patching, and forensic analysis; • Improvement of policies that deal with the security concerns; • Continuous improvement of awareness and reaction that include: visibility into all activity systems, databases, networks, and applications in real-time; one-touch remediation actions and privacy concerns regarding logging sensitive data or events.	[45]
5	Security of virtualization models	The growing complexity of cyber-attacks founded on multi-vector approaches Outdated trust models that are based on static topologies and white-box	• Integration of security mechanism:	[46]

		models	o Virtual models protection: ▪ Kernel-based counter-measure; ▪ Secure software management; ▪ Application-based counter-measure; o Hypervisor protection: ▪ Storage and networking protection; ▪ Execution environment counter-measure; ▪ Granularity of the Hypervisor architecture; • Adaptation based on security programmability: o Security programmability; o Monitoring built resources; o Orchestration of security mechanisms; • Minimization of the attack surface: o Formal code verification; o Outsourcing of virtual models software management; o Unnecessary capability dropping;	
		Heterogeneity of management and control interfaces related to cyber-security appliances without available standard		
		A low degree of automation that implies the need to rely on the skills and expertise of humans, resulting in human errors and subjectivity		
		The improper location of sensitive and personal data		
		The software sanity		
		The whole services availability		
		The availability to carry out quick remediation and mitigation actions in case of discontinuity		
		The rigid architectures		
		Flaws in security appliances that allows the attack surface growth		
		Limited visibility as a result of difficulties to install security agents in large, distributed and heterogeneous systems		
		Memory deallocation		
6	Cloud security	Runtime variable type checking	• Confidentiality: o Hybrid cryptography; o Public Key Infrastructure; o Public Key Infrastructure trusted CA certificate enabled IPSec or SSL communication; o TTP; o Hardware enabled trusted computing platform: ▪ Excalibur; ▪ TCCP; ▪ TPM and vTPM; • Integrity: o Hybrid cryptography; o Public Key Infrastructure; o TTP; o Trusted computing platform - VM migration; • Availability: o Fault tolerant mechanism; o Hardware enabled trusted computing platform - VM machine replication; o Continuous monitoring of attribute to enforce SLAs; o Framework for enhanced hardware and attribute-based adaptive trust management scheme for SLAs	[47]
		Access control		
		Code injection		
		Kernel inference in user space		
		Development software flaw		
		Concurrency		
		Configuration issue		
		Dependency solving error		
		Configuration issue		
		Kernel criticality		
		Access to user space		
		Hardware exposure		
		Co-residence		
		Shared networking		

		Resource sharing with the host Implementation of virtualization method Hypervisor oversight Management console oversight H-OS and H-OS Kernel configuration and service issues, access to user space and hardware exposure Hardware oversight, physical property, physical access and upgradability Data breaches	guarantee; • Accountability: o TTP certificates from CA adopted in communication chain of TrustActivity, traffic logging and event; • Privacy: o Hybrid cryptography trusted computing platform - user trusted entity, MyCloud, privacy preserving access control in SOA, public auditing and data anonymization; • Authentication: o Public Key Infrastructure; o TTP; o Digital signatures with SSO and LDAP; o Trusted computing platform; o Security domains with common security tokens; • Authorization: o Public Key Infrastructure; o TTP; o Security domains with common security tokens; o Hardware enabled access control; o Attribute-based certificates by CA; ** Detailed specification of countermeasures mapped with vulnerabilities and security requirements may be further analyzed in the cited article.*	
7	Network protection	Weak identity, access management and credentials Account hijacking Malicious insiders Insecure APIs System and application vulnerabilities Data loss Insufficient due diligence Advanced persistent threats Denial of service Shared technology vulnerabilities Abuse and nefarious use of cloud services Cyber attacks - Ransomware	• CSE-CIC-IDS2018 cyber dataset • Data loss prevention (DLP); • User behavior analytics; • Network traffic intelligence; • Security incident and event management (SIEM); • Privileged access management; • User training and awareness; • Employee monitoring and surveillance; • Threat intelligence sharing; • Strict third party vetting procedures; • Incident response management (IRM); • Artificial intelligence and machine learning	[48] [62]
8	IoT and SIoT security	Cyber attacks - General malware Cyber attacks - Phishing / Spear phishing Cyber attacks - Password attacks	• User awareness; • User habit modification;	[63]

		Cyber attacks - Advanced targeted attacks Cyber attacks - IoT attacks Brute-force attacks Password cracking Botnet attacks Heartbleed attacks Denial of service and distributed denial of service Inside network infiltration Web attacks Human factor	• Password management; • Install security software; • Monitor user habits; • Establish a clear and concise device usage policy; • Encrypting and reducing device visibility; • Segmenting data / software on devices; • Access control; • Information flow control; • Integrity mode; • Sanitization; • Degaussing; • Education / training;	
9	Blockchain technology security	Hacking attack Loss / Theft attack Unauthorized access / disclosure Improper disposal Double spending threats	• Monitoring installation in the network; • Effective identity and authentication management system; • Build semantic legal layer; • Establish interoperability and integrity; • Achieve trust and transparency; • Manage cyber attacks, vulnerabilities, protocols; • Effectively resolve data privacy at distributed contracts;	[51] [64]
10	Big data security	Network threats Mining pool threats Wallet security threats Sophisticated cyber attacks Sophisticated cyber crime	A novel security scheme Lightweight Hybrid Scheme (LHC) that is based on Diffie-Hellman key exchange and Elliptic Curve Cryptogpraphy;	[52] [53]
11	5G security and privacy	Hijacking attacks DoS attack Resource (slice) theft Signaling storms Configuration attacks Penetration attacks Saturation attacks User identity theft TCP level attacks Scanning attacks Timing attacks	• Predictive analytics; • Centralized control points security using DoS, DDoS detection; • Ensure security to control channels using Link security; • Flow rules verification in SDN switches using configuration verification; • Ensure identity users and security of location using identity and location security; • Ensure user identity verification for roaming and clouds services using identity verification; • Secure the subscriber identity through encryption using IMSI security; • Control access to SDN and core network elements using access control; • Ensure isolation for VNFs and virtual slices using traffic isolation; • Anti-malware technologies to secure mobile terminals using mobile terminal security;	[55] [65]

		IMSI catching attacks Boundary attacks Semantic information attacks Man-in-the-middle attack Reset and IP spoofing Security keys exposure	• Data security and storage systems in clouds security using integrity verification; • Cloud web services security using HX-DoS mitigation; • Service-based access control security for clouds using service access control; • Capabilities to isolate vulnerable devices; • Network segmentation; • Data in rest and data in transit encryption; • Continuous monitoring and alerting;	
12	6G security and privacy* **Appropriate for the DBE in the context of Industry 5.0*	AI/ML based intelligent attacks Quantum attacks PHY layer attacks for VLC, THz and other	• Ultra Lightweight security; • Extremely low latency; • Extreme scalability; • Zero-touch security; • High privacy; • Proactive security; • Security via Edge; • Domain specific security;	[56]
13	Cyber security on smart grid solutions	Confidentiality related attacks: • Social engineering; • Traffic analysis; • Eavesdropping; • Unauthorized access; • Password pilfering; • Sniffing; • MITM; • Replay; • Data injection attack; • Masquerading; Integrity related attacks: • Replay, • Tampering; • False data injection; • Wormhole; • Data modification; • Spoofing; • MITM; • Time synchronization;	• Technical solutions: o Firewall; o VPN; o Encryption; o Early warning systems; o IDS; o Access control; o Antivirus software; o Dynamic reconfiguration systems; • Security management perspective: o Solutions should include risk assessment of asset during attack and post attack phase; o Key management; o Security policy exchange; o Security incident; o Vulnerability report; o Integration of various security techniques incorporated in AI and Machine Learning; o Effective control of wireless propagation; o Network segmentation; o Authentication; o Certification;	[57]

		• Load-drop attacks; • Masquerading; Availability related attacks: • Denial of services; • Low-rate Dos; • Jamming; • Wormhole; • Buffer overflow; • Smurf; • Teardrop; • Puppet; • Masquerading; • MITM; • Spoofing attacks; • Time synchronization;	○ Proactive real-time IPS-IDS; ○ Authorization; ○ Effective adoption of resilient, adaptive, and scalable security techniques that do not impact smart grid operations; • Requirements for secured framework: ○ Attack detection and countermeasures application in the entire smart grid solution; ○ Authentication and access control establishment everywhere in smart grid solution; ○ Light-weight cryptographic functions embedded in the every node; ○ Design of network protocol security: from the application layer to MAC layer; ○ Cyber security test bed platforms implementation;	

TABLE III. KEY CYBERSECURITY PRODUCTS ACCORDING TO CYBERSECURITY TYPE: AN OVERVIEW [45]

Cybersecurity type	Product / Technology / Functions	Key features
Embedded industrial and IoT devices	Kaspersky Embedded Systems Security Kaspersky Industrial Cybersecurity Symantec Industrial Control Systems Protection Fortinet	• Secured every industrial layer, encompassing: SCADA servers, network connections, HML engineering workstations, PLCs; • File Integrity Monitoring and Audit Log; • Efficient and effective design for low-end hardware; • On-Demand Antivirus; • Default rejection for Drivers, Applications, and Libraries; • Resolves specific security concerns for embedded systems, such as rare updates and geographical dispersion; • Mono-domain;
Endpoint protection	Cisco AMP for Endpoints Kaspersky Endpoint Detection and Response Symantec Endpoint Protection Trend Micro Endpoint Security	• Centralized detection and analysis based on Machine Learning and threat intelligence; • Maximal protection of applications, devices, and the web; • Vulnerability assessment and automatic patching; • GDPR-compliant; • Mono-domain;
Cloud protection	Kaspersky Hybrid Cloud Security; Symantec Cloud Workload Protection Suite McAfee Cloud Security	• Efficient and effective support to the public (e.g. AWS, Google, Azure) and private clouds (e.g. Vmware, KVM, Xen); • Integration of public and private clouds; • Usage of public cloud APIs, and agentless deployment by providing services in targeted marketplaces;

		• Analysis integration with enterprise networks;
	Trend Micro Cloud-native Security	• Effective segmentation and access control; • Mono-tenant;
SIEM / Security analytics	Cisco Cognitive Threat Analytics	• Application of AI and machine learning to a wide variety set of data;
	McAfee Security Analytics	• Enables real-time visibility into all activities on systems, databases, networks, and application;
	McAfee SIEM	• Enables in-depth threat visibility across multiple control points;
	Kaspersky Threat Management and Defense	• Aggregation of intelligence across multiple control points;
	IBM QRadar	• Correlation of threat events;
	Symantec Advanced Threat Protection	• Enables in-depth threat visibility across IT environments in a comprehensive database;
	Micro Focus Arc Sight	• Big data capabilities;
	Solar Winds SIEM	• Resolves security concerns from an end-user point of view regarding privacy and sensitive data or events; • Enables advanced search mechanisms and forensic analysis;
Network visibility and segmentation	Cisco Stealthwatch	• Effectively supports cloud, industrial and enterprise networks; • Based on AI and machine learning technologies and network topology 3D visualization; • Cisco provides network segmentation; • Enables inspection of network traffic, utilization of sensors or flow-monitoring protocols; • Closed (vendor lock-in) and single-domain solution; • No mechanisms for tracing user data; • Anomaly and malware detection, DDoS protection, and zero-day exploitation. A solution is founded on query-based filtering;

Based on the research results depicted in Tables II and III, the paper integrates and holistically analyzed the DBE components, risks, and solutions to create an effective basis for a sustainable future for businesses and societies in a cyber world. However, the paper has some limitations that require future research.

V. Limitations and Future Research

The integration layer of all DBE components and solutions for risk mitigation inspired by Industry 4.0 requires different approaches in doing business between included stakeholders. The proper application of the open innovation collaboration model has a significant role during the integration process to boost multidisciplinary knowledge development as a step towards maximal value creation for all involved parties. The future research requires primary data collection from different stakeholders (e.g. governments, universities, organizations, individuals) to understand readiness towards application of secured digital business ecosystem viewed from Industry 5.0 perspective.

When cybersecurity products are in question, it has been recognized that all products are based on black-box design without transparent internal monitoring hooks and detection algorithms that vary between different vendors. More importantly, there is no interoperability with products from other vendors. Accordingly, to produce effective DBE protection, it is important to integrate different features from different products for all cybersecurity types. Future research heavily relies on primary quantitative and qualitative data collection to understand the readiness of proper adoption of open innovation collaboration model to simplify the combination of different heterogeneous appliances, data formats, and interfaces through effective industry and cross-industry collaboration [45].

Finally, IoT security still faces some threats that should be further analyzed and developed without any delay. The open threats refer to [66]:

- Privacy;
- Security protocols and light-weighted cryptographic systems;
- Software system susceptibility;
- Malicious programs that impact IoT network;
- Android security limitations;
- Entity recognition.

VI. Conclusion

To maximize potentials from the digital business ecosystem in terms of sustainable value creation for businesses and societies in a new human-centric global society, the paper aimed at narrowing security gaps and provided the basis for a secured digital business ecosystem in the long run.

The paper integrates digital business ecosystem components inspired by Industry 4.0 and holistically analyzes security aspects inspired by Industry 5.0 to create a basis for a sustainable future. To transform threats into a valuable sustainable digital environment, in the long run, research findings indicate that integrated hard and soft security components should be holistically understood. Hard and soft components of the security landscape towards sustainability are as follows:

- Multidisciplinary knowledge continuous development
- Strategic change management on the top of the transformative journey
- Strategic change leadership knowledge and skills on the top of driving change
- Cyber expertise development
- Security strategy development using a shift from push-based to a pull-based security ecosystem approach
- Security culture development and adoption
    - Information security culture and information protection culture development and adoption
    - Cybersecurity culture development to influence behavior of employees
- Security of digital services chains services
- Virtualization security
- Cloud protection opportunities
- Network protection
- IoT and SIoT security
- Blockchain technology security
- Big data security
- 5G security and privacy
- 6G security and privacy
- Cybersecurity on smart grid solutions

To effectively achieve business continuity, sustainable value creation, and long-term wellbeing and prosperity for societies and businesses, all components should be integrally embedded into a comprehensive digital business ecosystem as a prerequisite for sustainability.

Future research and management framework rely heavily on a switch from push-based to pull-based security ecosystem, protection strategies development, adoption of AI against cyber risks, and security culture development. The transformative journey towards long-term wellbeing to stakeholders included in the secured digital business ecosystems significantly lies in the multidisciplinary knowledge, simultaneous effectiveness of strategic change, and security management on one hand, and efficiency of IT and organizational capabilities, on the other. The open innovation collaboration model has a significant role in this journey.

VII. Contributions

The article may contribute to academics, business owners, shareholders, strategic change, security, innovation, and IT management.

REFERENCES

[1] V. Tornjanski, S. Knežević and S. Milojević, "Synergetic effects of integrated collaboration between humans and smart systems in banking: An overview," in XVII International Symposium SYMORG, Zlatibor, 2020.

[2] V. Tornjanski, M. Čudanov and S. Marinković, "Shaping a new business landscape by empowering collective intelligence: Synergetic effects of open innovation, human and artificial cognitive and emotional intelligence," in 2nd Virtual International Conference: Path to a Knowledge Society-Managing Risks and Innovation - PaKSoM 2020, Niš, 2020.

[3] U.-i. Chung, Y. Tei, S. Mitsuyoshi and S. Tokuno, "How to reconcile morality and diversity in globalization and multidisciplinary integration," Econophysics, Sociophysics & Other Multidisciplinary Sciences Journal (ESMSJ), vol. 6, no. 1, pp. 4-7, 2016.

[4] Deloitte, "The future of cyber survey 2019 - Cyber everywhere. Succeed anywhere.," Deloitte, 2019.

[5] V. Tornjanski, S. Marinković, G. Săvoiu and M. Čudanov, "A need for research focus shift: Banking industry in the age of digital disruption," Econophysics, Sociophysics & Other Multidisciplinary Sciences Journal, vol. 5, no. 3, pp. 11-15, 2015.

[6] E. Commission, Digital Business Ecosystem, Luxembourg: Office for Official Publications of the European Communities, 2007.

[7] P. K. Senyo, K. Liu and J. Effah, "Digital business ecosystem: Literature review and a framework for future research," International Journal of Information Management, vol. 47, pp. 52-64, 2019.

[8] K. Lenkenhof, U. Wilkens, M. Zheng, T. Süße, B. Kuhlenkötter and X. Ming, "Key challenges of digital business ecosystem development and how to cope with them," Procedia CIRP, vol. 73, pp. 167-172, 2018.

[9] D. P. David, M. M. Keupp and A. Mermoud, "Knowledge absorption for cyber-security: The role of human beliefs," Computers in Human Behavior, vol. 106, no. 106255, 2020.

[10] S. Bryukhovetskaya, K. Artamonova, A. Gibadullin, S. Ilminskaya and Z. Kurbonova, "Management of digital technology development in the national economy," in IOP Conference Series: Earth and Environmental Science, 2020.

[11] V. Tornjanski, S. Marinković, M. Levi Jakšić and V. Bogojević Arsić, "The prioritization of open innovation determinants in banking," Industrija, vol. 43, no. 3, pp. 81-105, 2015.

[12] V. Tornjanski, D. Petrović and M. Milanović, "The effects of IT and open innovation strategies on innovation and financial performances in the banking sector," Bankarstvo, vol. 45, no. 1, pp. 70-91, 2016.

[13] H. W. Chesbrough, Open innovation: The new imperative for creating and profiting from technology, Harvard Business Press, 2003.

[14] D. Fasnacht, Open Innovation in the financial services: growing through openness, flexibility and customer integration, Springer Science & Business Media, 2009.

[15] L. Sun, C. Tan, S. Robertson, K. Liu, M. Cook and C. Collins, "Open Digital Business Ecosystems: A Pathway for Value Co-Creation," in 17th International Conference on Informatics and Semiotics in Organisations (ICISO), Campinas, Brazil, 2016.

[16] M. Castells, The space of flows. The rise of the network society, Blackwell: Oxford, 1996, pp. 376-482.

[17] Ž. Dulanović and O. Jaško, Organizaciona struktura i promene, Beograd: Fakultet organizacionih nauka, 2009.

[18] O. Jaško, M. Čudanov, M. Jevtić and J. Krivokapić, Projektovanje organizacije, Beograd: Fakultet organizacionih nauka, 2013.

[19] N. Janićijević, Upravljanje organizacionim promenama, Beograd: Centar za izdavačku delatnost Ekonomoskog fakulteta u Beogradu, 2011.

[20] I. Adizes, "Organizational passages—diagnosing and treating lifecycle problems of organizations," Organizational Dynamics, vol. 8, no. 1, pp. 3-25, 1979.

[21] J. Moore, "Predators and Prey: A New Ecology of Competition," Harvard business review, vol. 71, no. 3, pp. 75-86, 1993.

[22] R. Gupta, C. Mejia and Y. Kajikawa, "Business, innovation and digital ecosystems landscape survey and knowledge cross sharing," Technological Forecasting and Social Change, vol. 147, pp. 100-109, 2019.

[23] K. Korpela, K. Mikkonen, J. Hallikas and M. Pynnönen, "Digital Business Ecosystem Transformation: Toward Cloud Integration," in 49th Hawaii International Conference on System Sciences (HICSS), 2016.

[24] L. Weimin and W. Xiaoyang, "The role of Beijing's securities services in Beijing–Tianjin–Hebei financial integration: A financial geography perspective," Cities, vol. 100, no. 102673, 2020.

[25] M. Fukuyama, "Society 5.0: Aiming for a new human-centered society," Japan Spotlight, vol. 27, pp. 47-50, 2018.

[26] M. Riegler and J. Sametinger, "Multi-mode Systems for Resilient Security in Industry 4.0," Procedia Computer Science, vol. 180, pp. 301-307, 2021.

[27] A. Rashid, "Looking to the future of the cyber security landscape," Network Security, vol. 3, pp. 8-10, 2021.

[28] J. Kaur and K. .. Ramkumar, "The recent trends in cyber security: A review," Journal of King Saud University - Computer and Information Sciences, vol. Article in press, pp. 1-16, 2021.

[29] FBI, "Ransomeware Prevention and Response for CISOs.," Federal Bureau of Investigation, 2017.

[30] S. Hasan, M. Ali, S. Kurnia and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, no. 102726, pp. 1-16, 2021.

[31] ISO, "Guidelines for Cyber Security," [Online]. Available: http://www.iso27001security.com/html/27032.html. [Accessed 03 June 2021].

[32] J. Kaur and K. Ramkumar, "The recent trends in cyber security: A review," Journal of King Saud University - Computer and Information Sciences, vol. Article in press, pp. 1-16, 2021.

[33] M. Čudanov, V. Tornjanski and O. Jaško, "Change equation effectiveness: Empirical evidence from South-East Europe," Business Administration and Management, vol. 22, no. 1, pp. 99-114, 2019.

[34] NCSI, "National Cyber Security Index," [Online]. Available: https://ncsi.ega.ee/ncsi-index/?order=-ratio&type=c. [Accessed 03 June 2021].

[35] K. Pipyros, C. Thraskias, L. Mitrou, D. Gritzalis and T. Apostolopoulos, "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual," Computers & Security, vol. 74, pp. 371-383, 2018.

[36] K. Fukuda, "Science, technology and innovation ecosystem transformation toward society 5.0," International Journal of Production Economics, vol. 220, no. 107460, 2020.

[37] L. Gerhold, G. Bartl and N. Haake, "Security culture 2030. How security experts assess the future state of privatization, surveillance, security technologies and risk awareness in Germany," Futures, vol. 87, pp. 50-64, 2017.

[38] A. Ruighaver, S. Maynard and S. Chang, "Organisational security culture: Extending the end-user perspective," Computers & Security, vol. 26, no. 1, pp. 56-62, 2007.

[39] A. D. Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," Computer Law & Security Review, vol. 31, no. 2, pp. 243-256, 2015.

[40] A. D. Veiga, L. V. Astakhova, A. Botha and M. Herselman, "Defining organisational information security culture—Perspectives from academia and industry," Computers & Security, vol. 92, no. 101713, 2020.

[41] A. AlHogail, "Design and validation of information security culture framework," Computers in Human Behavior, vol. 49, pp. 567-575, 2015.

[42] A. Nasir, R. A. Arshah, M. R. A. Hamid and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," Journal of Information Security and Applications, vol. 44, pp. 12-22, 2019.

[43] J. V. Niekerk and R. V. Solms, "Information security culture: A management perspective," Computers & Security, vol. 29, no. 4, pp. 476-486, 2010.

[44] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security, vol. 98, no. 102003, 2020.

[45] M. Repetto, A. Carrega and R. Rapuzzi, "An architecture to manage security operations for digital service chains," Future Generation Computer Systems, vol. 115, pp. 251-266, 2021.

[46] M. Compastié, R. Badonnel, O. Festor and R. He, "From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models," Computers & Security, vol. 97, no. 101905, 2020.

[47] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Computer Science Review, vol. 33, pp. 1-48, 2019.

[48] P. Chapman, "Defending against insider threats with network security's eighth layer," Computer Fraud & Security, vol. 2021, no. 3, pp. 8-13, 2021.

[49] R. Faqihi, J. Ramakrishnan and D. Mavaluru, "An evolutionary study on the threats, trust, security, and challenges in SIoT (social internet of things)," Materials Today: Proceedings, 2020.

[50] J. Neeli and S. Patil, "Insight to security paradigm , research trend & statistics in internet of things (IoT)," Global Transitions Proceedings, vol. 2, no. 1, pp. 84-90, 2021.

[51] B. Bhushan, P. Sinha, K. M. Sagayam and J. Andrew, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," Computers & Electrical Engineering, vol. 90, no. 106897, 2021.

[52] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, G. Wang, T. Wang, M. M. Ahmed and J. Li, "Economic perspective analysis of protecting big data security and privacy," Future Generation Computer Systems, vol. 98, pp. 660-671, 2019.

[53] M. P. Kumari and T. S. Rao, "A lightweight hybrid scheme for security of big data," Materials Today: Proceedings, 2021.

[54] B. Delibašic, J. E. Hernández, J. Papathanasiou, F. Dargam, P. Zaraté, R. Ribeiro, S. Liu and I. Linden, "Decision Support Systems V–Big Data Analytics for Decision Making," in First International Conference, ICDSST, Belgrade, 2015.

[55] S. Sicari, A. Rizzardi and A. Coen-Porisini, "5G In the internet of things era: An overview on security and privacy challenges," Computer Networks, vol. 179, no. 107345, 2020.

[56] P. Porambage, G. Gurkan, D. P. Moya Osorio, M. Liyanage and M. Ylianttila, "6G security challenges and potential solutions," in IEEE Joint Eur. Conf. Netw. Commun.(EuCNC) 6G Summit, 2021.

[57] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, no. 107094, 2020.

[58] B. Alhayani, H. J. Mohammed, I. Z. Chaloob and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," Materials Today: Proceedings, 2021.

[59] M. S. H. A. J. M. A. Faezeh Farivar, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716 - 2725, 2020.

[60] K. G. Narcisa Roxana MOȘTEANU, "ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

– FACE TO FACE WITH CYBER ATTACK – A MALTESE CASE OF RISK MANAGEMENT APPROACH," ECOFORUM, vol. 9, no. 2(22), 2020.

[61] T. D. A. D. Mauro Conti, Cyber Threat Intelligence: Challenges and Opportunities, Springer, Cham, 2018, pp. 1-6.

[62] V. Kanimozhi and T. Prem Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," ICT Express, pp. 1-5, 2020.

[63] K. Hughes-Lartey, M. Li, E. F. Botchey and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," Heliyon, vol. 7, no. e06522, pp. 1-13, 2021.

[64] N. Upadhyay, "Demystifying blockchain: A critical analysis of challenges, applications and opportunities," International Journal of Information Management, vol. 54, no. 102120, pp. 1-26, 2020.

[65] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "5G Security: Analysis of Threats and Solutions," in IEEE Conference on Standards for Communications and Networking (CSCN), 2017.

[66] J. Neeli and S. Patil, "Insight to Security Paradigm, Research Trend & Statistics in Internet of Things (IoT)," Global Transitions Proceedings, vol. 2, no. 1, pp. 84-90, 2021.