Digital Risk Cultures in Human Development

Subjects: Sociology

Contributor: Răzvan Rughiniș, Emanuela Bran, Ana Rodica Stăiculescu, Alexandru Radovici

As digitalization evolves, so do the experiences and perceptions of digital hazards, leading to a multifaceted interaction involving consciousness, vulnerability, and remediation. With the growing integration of societies and individuals into the digital landscape, there is a corresponding rise in their vulnerability to cyber dangers such as security breaches and misinformation campaigns.

Keywords: cybersecurity ; digital risk culture ; risk society ; technological capital ; human development index

1. Introduction

As digitalization evolves, so do the experiences and perceptions of digital hazards [1], leading to a multifaceted interaction involving consciousness, vulnerability, and remediation. With the growing integration of societies and individuals into the digital landscape, there is a corresponding rise in their vulnerability to cyber dangers such as security breaches and misinformation campaigns. At the same time, the increased prevalence of digital platforms has led to enhanced recognition of these potential hazards, since individuals are better informed, and societies place a larger emphasis on the dissemination of knowledge on cybersecurity and general risk communication [2]. Concurrently, the progression of digitalization introduces increasingly sophisticated instruments and tactics to address these threats. Thus, this duality gives rise to a paradox: although heightened digital exposure has the potential to magnify perceived dangers, the augmented capacities for mitigation may diminish the impression of risk or even foster a state of complacency. The ongoing evolution of technology creates an ambivalent and dynamic interplay between digitization and the perception of risk [3], leading to continuous changes and adjustments.

2. Technological Capital and Digital Habitus

Concerns about digital technologies can have individual and collective dynamics underlined by ambivalence. At an individual level, technological capital [4] could account for observed risk perceptions. This extension of Bourdieu's concept of capital refers to the resources that individuals hold, enabling them to engage with digital technology. The digital habitus of an individual would thus comprise the set of lasting dispositions based on personal experiences and assimilated perspectives that shape perceptions, appreciations, and actions regarding the digital sphere [5]. The ease with which a person uses online tools, their digital consumption habits [6], and even their susceptibility or resistance to online threats are all influenced by their digital habitus. As societies become increasingly digital, a person's digital habitus interacts with their technological capital [7], affecting how they accumulate more of it and how they deploy it in different situations.

In light of Bourdieu's conceptualization of different social fields and forms of capital, researchers could talk about the four dimensions of technological capital [8]. The economic dimension is related to the availability of assets such as high-performance devices, premium membership subscriptions, and high-speed internet. The cultural dimension comprises skills and knowledge about the latest tech evolutions, including matters such as privacy issues or having certifications in IT-related fields. Another dimension is represented by the social technological capital [9], which comprises membership in relevant networks and groups and having connections with influencers on social media and the tech industry. Finally, there is symbolic technological capital that captures the prestige of digital expertise and presence within the digital sphere.

Technological capital can also be classified into embodied, institutionalized, and material forms of capital. These refer to skills and competencies that individuals control as embodied abilities, to their acquired degrees and certifications, and to their physical and digital assets, respectively. These forms of capital can be studied indirectly through proxies such as socio-economic variables and internet use when no direct indicators are available.

The technological capital of individuals does not exist independently of their social position. It frequently interplays with their social, cultural, and economic capital, amplifying or attenuating the positives and negatives connected with each. For example, an individual with high economic capital can easily invest part of it in material technological capital, while an

individual with strong social capital and limited technological capital might struggle to maintain their network of influential connections. Consequently, the conceptual relationship between technological capital and socio-economic variables is strong, which makes it possible to use the latter as proxy indicators for the former.

The frequency of internet use is a good measurement of embodied technological capital, as it implies familiarity and comfort with digital tools and services. This form of technological capital is also indirectly revealed in the age and gender of an individual. The younger generations have been socialized as “digital natives”, growing up immersed in the digital world and exhibiting intuitive interaction skills with it. Gender is also associated with STEM skills and digital savvy, though in variable forms and intensities, as boys and men are often more encouraged than girls and women to become acquainted with technologies and to invest in them emotionally.

Education indicates primarily a form of institutionalized technological capital, being an indicator of formal training and instruction in digital skills. Embodied technological capital could also be observed indirectly through education, social class, and community size, as they shape one’s encounters with the latest digital advancements. Furthermore, along with the more direct proxy estimates of material technological capital through social class and community size, gender can also act as a proxy due to the existing economic inequalities.

3. Risk Society and Digital Development

Beck’s “Risk Society” theory highlights the transforming nature of contemporary dangers and how they alter societal perceptions and priorities of digitalization [10]. The Human Development Index (HDI), the Global Cybersecurity Index (GCI), and the Digital Economy and Society Index (DESI) can be used as proxy indicators for the risk society. HDI captures socio-economic development, which is strongly linked to digital technology advancements [11], while DESI and GCI reveal society’s digital engagement and cybersecurity preparedness, respectively.

The first dimension of HDI is life expectancy at birth. This strongly relates to the medical infrastructure and other life sectors such as the food industry or work environment safety, all dependent on and enhanced by digital technologies. Mean years of schooling and expected years of schooling represent the second dimension of HDI. Higher levels of education can accommodate an advanced curriculum on technologies and their multifold impact on society [12]. The third dimension, GNI per capita, indicates economic prosperity. These financial resources are at risk of being targeted through cybercrime, but they also provide means for developing increased security infrastructures.

The Global Cybersecurity Index (GCI) captures how well a society is equipped to withstand cybersecurity issues from five different dimensions. The first one assesses the degree to which the legal system regulates data protection, critical infrastructures, and cybercrime. The next dimension focuses on national technical capabilities such as handling incidents by a Computer Incident Response Team (CIRT) and having Child Online Protection Reporting mechanisms. The third dimension watches for national cybersecurity strategies and agencies or organizations, with additional oversight in online child protection. Another dimension measures capacity development such as conducting cyber-awareness initiatives, fostering R&D programs, and cultivating national cybersecurity industries. The last dimension assesses cooperation in the form of partnerships and bilateral or multilateral agreements between agencies, firms, and countries.

Moving forward to DESI, its first dimension is represented by Connectivity. Highly connected infrastructures introduce risks related to cyberattacks and the spread of misinformation. Conversely, digital coordination helps mitigate such issues. The second dimension is Human Capital, which is focused on digital skills [13]. This simultaneously indicates a stronger reliance on digital technologies that could represent vulnerabilities and a higher knowledge of secure digital practices that offer protection. The use of Internet Services by citizens represents the third DESI dimension. High internet engagement may create increased access to knowledge and a higher digital footprint along with increased digital exposure, leading to cybersecurity and privacy issues [14]. The fourth dimension is the Integration of Digital Technology by businesses. A digitalized private sector is more efficient and can accommodate new business models while being at the risk of data breaches and economic espionage. Digital Public Services is the fifth dimension of DESI, and higher digitalization poses a similar threat as the previous dimension. Digitalization brings risks such as data breaches and system failures.

4. Previous Studies on Public Perception of Privacy and Cybersecurity Issues

At the date of manuscript submission (December 2023), there were no other studies that analyzed Eurobarometer 96.1 information concerning cybersecurity concerns, though Matefi [15] discusses Europeans’ perceptions of their digital rights based on the same survey.

Still, a series of authors have analyzed other Eurobarometer and dedicated surveys concerning cybersecurity and privacy concerns. For example, Lee and Wang [16] analyzed Eurobarometer 2019 data on cybersecurity fears, identifying two types of Europeans based on individual levels of online activity and cybersecurity behavior (as reported in the survey): the “at-risk class” (with higher risk) and the “cautious class” (with lower risk). At the country level, they used as predictors the Global Cybersecurity Index (GCI), GDP per capita, internet penetration, and proportion of urban population, though only internet penetration was statistically significant in discriminating between the two groups, with higher rates leading to higher proportions of the “at-risk” type. The authors also find that, at the individual level, higher digital skills are, paradoxically, associated with the at-risk class, probably due to the ambivalent relationship mediated by exposure: “Surprisingly, changes in passwords, the maintenance of security settings, and concerns about cybersecurity have all been positively associated with risky Internet users. Researchers speculate that members of the at-risk class might engage in more online activities, and while this would make them more predisposed to being targeted online, these individuals are likely also more self-aware and recognize the potential risks of their actions” (p. 22). In a different analysis of the same Eurobarometer 2019, Lee and Kim [17] conclude that fear of cybercrime is most strongly determined by individuals’ prior victimization. This finding is also supported by a systematic review of the fear of cybercrime conducted by Brands and Doorn [18].

Zamfirescu et al. [19] have highlighted the ambivalent relationships between online activity, experiences of cybersecurity incidents, and concerns and preventive measures taken to address them, based on Eurobarometer 87.4/2017. They classify European respondents into four attitudinal clusters, “avoiding”, “engaging”, “wary”, and “aware”. In a similar analysis, they show that socio-demographical differences as regards these types in relation to gender, age, difficulty of paying bills, and formal education are rather small. Still, countries differ markedly in the prevalence of the four types. This could possibly indicate the relevance of distinctive digital risk cultures that underlie individual attitudinal profiles. Lee and Kim [20] analyze similar data from a 2014 Eurobarometer and classify respondents into three types: uninformed users, disciplined users, and cautious users. They also conclude that country-level factors are better predictors of cybersecurity preparedness than sociodemographic factors, taking into account the GDP per capita and the Global Cybersecurity Index (GCI) values at the national level. Gomes and Dias [21] take a different approach to the Eurobarometer 2017 data, combining individual sociodemographic variables with internet use and the country-level Global Cybersecurity Index (GCI) into a multilevel factor model to predict an aggregated value of cybersecurity perceptions. They find that the GCI is a significant negative predictor for cybercrime risk perception, while individual-level predictors are significant just for self-confidence in one’s abilities to use the internet and age (with negative associations) and buying goods online and male gender (with positive associations).

References

1. Rughini, R.; Rughini, C.; Vulpe, S.N.; Rosner, D. From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. Comput. Law Secur. Rev. 2021, 42, 105585.
2. de las Heras-Pedrosa, C.; Sánchez-Núñez, P.; Peláez, J.I. Sentiment Analysis and Emotion Understanding during the COVID-19 Pandemic in Spain and Its Impact on Digital Ecosystems. Int. J. Environ. Res. Public. Health 2020, 17, 5542.
3. Budeanu, A.-M.; Ţurcanu, D.; Rosner, D. European Perceptions of Artificial Intelligence and Their Social Variability. In An Exploratory Study. In Proceedings of the 2023 24th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 24–26 May 2023; pp. 436–443.
4. Romele, A. Technological Capital: Bourdieu, Postphenomenology, and the Philosophy of Technology Beyond the Empirical Turn. Philos. Technol. 2021, 34, 483–505.
5. Liébana-Cabanillas, F.; García-Maroto, I.; Muñoz-Leiva, F.; Ramos-de-Luna, I. Mobile Payment Adoption in the Age of Digital Transformation: The Case of Apple Pay. Sustainability 2020, 12, 5443.
6. Talwar, S.; Talwar, M.; Kaur, P.; Dhir, A. Consumers’ resistance to digital innovations: A systematic review and framework development. Australas. Mark. J. AMJ 2020, 28, 286–299.
7. El-Haddadeh, R. Digital Innovation Dynamics Influence on Organisational Adoption: The Case of Cloud Computing Services. Inf. Syst. Front. 2020, 22, 985–999.
8. Budeanu, A.-M.; Rosner, D. Big Data as Capital. A Case Study on the Innovation Labs Tech Accelerator. In Proceedings of the 2021 23rd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 26–28 May 2021; pp. 469–475.

9. Graziano, T. Social Media in Risk Perception and Disaster Management: A Geographical Perspective. In Disaster Resilience and Human Settlements: Emerging Perspectives in the Anthropocene; Dahiya, B., de Pascale, F., De Pietro, O., Farabollini, P., Lugeri, F.R., Mercatanti, L., Eds.; Advances in 21st Century Human Settlements; Springer Nature: Singapore, 2023; pp. 139–153.
10. Sundberg, L. Towards the Digital Risk Society: A Review. Hum. Aff. 2023, 1–14.
11. Bolpagni, M. Cyber risk index: A socio-technical composite index for assessing risk of cyber attacks with negative outcome. Qual. Quant. 2022, 56, 1643–1659.
12. Lesjak, D.; Zwilling, M.; Klein, G. Cyber crime and cyber security awareness among students: A comparative study in Israel and Slovenia. Issues Inf. Syst. 2019, 20, 80–87.
13. Vasiloiu, I.-C. Cybersecurity education in Romania—Competitive advantage in the EU market. In Proceedings of the International Conference on Virtual Learning, 17th ed.; The National Institute for Research & Development in Informatics—ICI Publishing House: Bucharest, Romania, 2022; pp. 297–307.
14. Vimalkumar, M.; Sharma, S.K.; Singh, J.B.; Dwivedi, Y.K. 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. Comput. Hum. Behav. 2021, 120, 106763.
15. Matefi, R. Digital Rights and Their Protection in the Online Environment in the Representation of EU Citizens. Rev. Universul Jurid. 2022, 52, 52–55.
16. Lee, C.S.; Wang, Y. Typology of cybercrime victimization in Europe: A multilevel latent class analysis. Crime Delinq. 2022, 1–28.
17. Lee, C.S.; Kim, J.H. How victims perceive fear of cybercrime: Importance of informed risk. Crim. Justice Stud. 2023, 36, 206–227.
18. Brands, J.; Doorn, J.V. The measurement, intensity and determinants of fear of cybercrime: A systematic review. Comput. Hum. Behav. 2022, 127, 107082.
19. Zamfirescu, R.-G.; Rughinis, C.; Hosszu, A.; Cristea, D. Cyber-security profiles of European users: A survey. In Proceedings of the 2019 22nd International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 28–30 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 438–442.
20. Lee, C.S.; Kim, J.H. Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. Comput. Secur. 2020, 97, 101995.
21. Gomes, A.; Dias, J.G.; da Força Aérea, A. A multilevel factor analysis of the cybercrime risk perception in the European Union. In Proceedings of the Program and Book of Abstracts XXVII Meeting of the Portuguese Association for Classification and Data Analysis (CLAD), Lisboa, Portugal, 22–24 October 2020; p. 57.