ISSN: 2083-5701
e-ISSN: 2545-2568
GICID: 71.0000.1500.1589

Nr 20(1/1)/2024
Numer DOI: 10.5604/01.3001.0054.6506

Marco Marsili[1]
Cà Foscari University of Venice, Italy
ORCID ID: 0000-0003-1848-9775
e-mail: info@marcomarsili.it, marco.marsili@unive.it

Joanna Wróblewska-Jachna
University of Bielsko-Biała, Poland
ORCID ID: 0000-0002-5795-0176
e-mail: jwroblewska@ubb.edu.pl

Digital revolution and artificial intelligence as challenges for today

Research on the subsequent revolutions that will be introduced: then this is due to–disk blocking the system from reproducing itself smoothly and/or–radically new challenges that may arise and arise to be solved. And–then–"revolutionaries" appear, seeing where the opportunities are breaking[2].

Rewolucja cyfrowa i sztuczna inteligencja jako wyzwania współczesności

ABSTRAKT

Artykuł podejmuje problematykę społecznych skutków trwającej rewolucji cyfrowej poprzez krytyczną analizę literatury przedmiotu. Celem jest zrozumienie dynamiki zmian, które jest kluczem do poradzenia sobie z złożonością ery cyfrowej i wykorzystania jej potencjału w zakresie zrównoważonego rozwoju. Rewolucja cyfrowa i sztuczna inteligencja stawiają przed współczesnym społeczeństwem znaczące wyzwania. Definiowane jako samoorganizujące się zmiany społeczne, które zakłócają istniejące normy, oznaczają głęboką transformację poprzez samoorganizujące się zmiany społeczne, które zakłócają istniejące normy. Era cyfrowa zrewolucjonizowała systemy informacyjne, podobnie jak wynalezienie przez Gutenberga prasy drukarskiej z ruchomymi czcionkami. Chociaż rewolucja informacyjna umożliwia postęp naukowy i gospodarczy, budzi wątpliwości etyczne, moralne i prawne. Media społecznościowe stały się "bronią" w konflikcie hybrydowym, w którym nieuchwytnym polem bitwy są systemy poznawcze człowieka.

SŁOWA KLUCZOWE: sztuczna inteligencja, zmiany społeczne, wojna poznawcza, metaverse

[1] Data złożenia tekstu do Redakcji „MiS": 20.05.2024; data recenzji: 10.06.2024; data zatwierdzenia tekstu do druku: 24.06.2024; data publikacji: 30.06.2024/Submission date to the "Media and Society" Editorial Office: 20.05.2024; review date: 10.06.2024; article approval print date: 24.06.2024; publication date: 30.06.2024.
[2] J. Staniszkis, *Anthropology of power. Between the Lisbon Treaty and the crisis*, Wydawnictwo Prószyński Media, Warsaw, 2009. p. 181.

This article introduces the social impact of the ongoing digital revolution. The analysis conducted uses a critical analysis of the literature on the subject. The aim of the analysis is to understand the dynamics of change, which is key to dealing with the complexities of the digital age and realising its potential for sustainable development.

A revolution in the social sciences is defined as a self-organizing profound social change that breaks the continuity of the social system. A review of the literature related to the study of the revolution provides knowledge about its cause[3], the process and course[4], as well as its far-reaching effects. The revolutionary potential lies in the technique and the ability to exceed the limits imposed by nature.

The invention of the steam engine made production processes independent of the energy used by people and animals, leading to the industrial revolution. The 19th and 20th centuries were dominated by urbanization processes, world wars, competition for resources, the Cold War division into eastern and western zones of influence, impacting every level of social life. The 21st century is marked by an ongoing digital revolution, characterized by multi-level digitalization of society. These revolutions correspond to several technological transitions: from the mechanical era to the electrical era, and finally to the electronic era–the one we are currently living in[5].

In the 20th century, we have witnessed three great revolutions over sixty years: the nuclear revolution, the Internet revolution[6], and the biotechnology revolution[7]. The digital revolution has profoundly changed the information system, comparable to the revolution of movable type printing introduced by Gutenberg in 1456[8]. The development of modern information and communication technologies and the associated dynamic process of digitizing society, brings both opportunities and threats. On the one hand, it enables surpassing existing boundaries and provides tools that facilitate the daily functioning and advancement of nearly all fields of science and branches of the economy. On the other hand, it raises a number of concerns and dilemmas related to the collection and analysis of data by artificial intelligence (AI), as well as the interference of companies and institutions in the most private areas of the lives of individuals, groups and entire communities.

The digital revolution has developed new forms of capital accumulation leading to surveillance capitalism[9]. The naturally traumatic processes of social change in the years 2019-2022 were intensified by the COVID-19 pandemic[10]. A state of social anomie[11] has paralyzed institutions whose role is to provide material and symbolic

[3] P.A. Sorokin, *The Sociology of Revolution*, Howard Fertig, New York, NY, 1967.
[4] C. Tilly, *From Mobilization to Revolution*, Addison-Wesley, Reading, MA, 1978.
[5] M. Marsili, *La rivoluzione dell'informazione digitale in Rete. Come Internet sta cambiando il modo di fare giornalismo*, Odoya, Bologna, 2009, p. 19. DOI: 10.5281/zenodo.33614.
[6] Also known as the Information revolution or the Third Industrial Revolution, or the Digital Revolution.
[7] *Ibidem*.
[8] *Ibidem*.
[9] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, 2018.
[10] P. Sztompka, *Socjologia zmian społecznych*, Znak, Kraków, 2005.
[11] E. Durkheim, *Suicide: a study of sociology*, The Free Press, New York, NY, 1966.

tools to facilitate adaptation to the living environment. In both developed and developing countries, poor mental health among citizens is becoming a social problem. Generations of children, teenagers, and young adults are overstimulated and exposed to multiple crises resulting from the functioning of the public information ecosystem[12].

The world that has opened up with the digital revolution is characterized by decentralization, which shifts the primary point of interest and observation (and of finalization) from the subjective vision in the village dimension to a depersonalized global vision[13]. The globalization of the "electric" village brings and stimulates more "discontinuity and division and diversity" than what happened in the previous mechanical world[14]. Change often brings opportunities, but also threats and challenges.

The development of self-learning neural networks and the creation of a new form of collective intelligence applied to AI are transforming the existing communication system. Artificial intelligence, which describes the ability of systems to perform tasks that normally require human intelligence[15], has made its place at the heart of the public policy debate in the absence of international standards and is becoming one of the central phenomena of the information society[16]. It is used–in the form of various types of algorithms–in many areas of social, cultural, economic and political life. It is neither possible nor necessary to free the existing social worlds. It is not possible for social meetings to occur without the breakdown of belief systems that create symbolic universes at the level of many social worlds experienced and invented by communities and collectives. Limited cognitive individuals, communities or collectives are conscious. The effects of digital development are recognized by research social fabrics that adapt to the new system. Observation enables the identification of entities that serve as leaders and animators of change, beneficiaries and epigons. The social costs of the digital revolution are difficult to estimate and include wars, economic, social and axio-normative destabilization. The advantages in political and economic fields are obtained through deep interference in the communication ecosystem that constructs the cognitive framework of individuals and communities.

---

[12] R. Paprocki R., J. Wróblewska-Jachna, *Empirical and Social Anxiety about the Covid-19 Pandemic: Measurement, Diagnosis, Modelling*,"ASK. Research & Methods" 31 (2022), 47-68.

[13] M. McLuhan, *Understanding Media:The Extensions of Man*, McGraw-Hill, New York, NY, 1964; M. McLuhan, Q. Fiore, War and Peace in the Global Village, Bantam Books, New York, NY, 1968.

[14] M. McLuhan, *Understanding Media*, 1964, cited in M. Marsili, *La rivoluzione dell'informazione digitale in Rete*, 2009, p. 20.

[15] For a definition of AI and related issues, see: Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *A definition of AI: main capabilities and disciplines. Definition developed for the purpose of the AI HLEG's deliverables*, European Commission, Brussels, 8 April 2019, https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines; EU-U.S. Trade and Technology Council, Working Group 1: Technology Standards, Subgroup on AI Taxonomy & Terminology, *EU-U.S. Terminology and Taxonomy for Artificial Intelligence*, 2nd ed., European Union, 5 April 2024, https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition.

[16] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, NY, 2019.

Enhanced cognitive information environment enabled by artificial intelligence

Information is "the foundation of all human interaction". The intersection of information with physical and cognitive/social domains, empowered by the digital ecosystem–Internet, social media, and communication applications–creates the conditions for cognitive hacking[17]. The wording "cognitive hacking" fits better to describe malign actions in the information environment, as already discussed[18], and suits international humanitarian law or "the law of war". On these grounds, it should be preferred instead of the term "cognitive warfare".

We define "cognitive hacking" as the practice of manipulating and falsifying information to induce changes in users' perceptions. These attacks are defined, structured, and organized to alter or mislead the thoughts of leaders and operators, members of entire social or professional classes, men and women in an army, or on a larger scale, an entire population in each region, country, or group of countries. A cognitive attack is intended to transform the understanding and interpretation of the situation on both individual and mass consciousness. It uses emotional stress to lower the rational thinking of the object of influence.

In its individual components, there is nothing new; the novelty in cognitive attacks lies in the speed and power of dissemination of beliefs–whether false or true–deeply instilled in the consciousness of targets. One of the main challenges in the digital age is the dissemination of false information, which can influence public opinions, affecting political decisions, and even the psychological well-being of individuals[19].

Emotions play a significant role in how people interpret and react to online information[20] influencing their susceptibility to manipulation[21]. Previous studies[22]

[17] Cognitive hacking is a cyberattack that seeks to manipulate the perception of people by exploiting their psychological vulnerabilities and is considered a threat from disinformation. For a discussion on the meaning of the term, see: G. Cybenko, A. Giani, P. Thompson, *Cognitive Hacking: A Battle for the Mind*, "IEEE Computer" 35, no. 8 (2002): 50-56; J. Bone, *Cognitive Hack: The New Battleground in Cybersecurity... the Human Mind*, 1st ed., Auerbach Publications, New York, NY, 2017. DOI: https://doi.org/10.1201/9781315368412.

[18] M. Marsili, *L'evoluzione delle forze speciali nelle Multi-Domain Operations (MDO). La necessaria capacità di operare nell'ambiente cyber e spaziale. La capacità di utilizzo del Metaverso*, IRAD-Istituto di Ricerca e Analisi della Difesa, Roma, 2024; M. Marsili, *Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse*, "Applied Cybersecurity & Internet Governance" (ACIG), 2, no. 1 (2023): 1-11. DOI: 10.60097/ACIG/162861; B. Forrester, M. Rosell, V. Dragos, M. Marsili, *Value Differences: A Starting Point for Influence*, [in:] *Mitigating and Responding to Cognitive Warfare. Proceedings of the HFM-361-RSY Symposium held on 13-14 Nov. 2013 in Madrid, Spain*, NATO Science & Technology Organization (STO), Paris, 2024, pp. P3-1-P3-18. DOI: 10.14339/STO-MP-HFM-361.

[19] A. Guess, B. Nyhan, J. Reifler, *Exposure to untrustworthy websites in the 2016 US election*, "Nature Human Behaviour" 4, no. 5 (2000): 472-480.

[20] L. Pessoa, *How do emotion and motivation direct executive control?*, "Trends in cognitive sciences" 13, no. 4 (2009): 160-166.

[21] J. Diemer, G.W. Alpers, H.M. Peperkorn, Y. Shiban, A. Mühlberger, *The impact of perception and presence on emotional reactions: A review of research in virtual reality*, "Frontiers in Psychology" 6 (2015): 1-9. DOI: 10.3389/fpsyg.2015.00026.

[22] K.M. Lee, C. Nass, *Experimental tests of normative group influence and representation effects in computer-mediated communication: Evidence for the social identity model of deindividuation effects*,"Communication Research" 30, no. 1 (2023): 36-52.

have highlighted the role of emotions, anger, and personality traits in influencing susceptibility to fake news and decision-making. Additionally, cognitive biases, personality tendencies, and individual decision-making processes can shape people's propensity to believe and spread unverified news contents[23].

Therefore, as human cognition is highly susceptible to manipulation and deception, a cognitive strategy aims to influence thinking processes, such as perceptions, decision making and behavior. Cognitive attacks affect perceptions, beliefs, interests, aims, decisions, and behavior by deliberately targeting the human mind. This weaponized use of information serves to build and reinforce biased or false narratives to alter the perception and the behavior of individuals and, finally, of society by undermining social cohesion[24]. Indeed, cognitive operations target influential individuals, specific groups, and large numbers of citizens selectively and serially in society, with the potential to fracture and fragment an entire society or disrupt alliances[25].

The human-machine interaction, accelerated and expanded by technologies at a tempo and scale previously unimaginable, is a fundamental component of cognitive operations, and plays a central and crucial role due to the way our perception and judgment are affected, thus posing an unprecedented challenge to contemporary society[26].

Cognitive activities are a component of modern warfare and do not necessarily carry a kinetic component or directly tangible outcomes, such as territorial or resource acquisition–unlike other hybrid threats[27]. These activities vary greatly and may encompass supportive or conflicting cultural or personalized components–social psychology, game theory, and ethics are all contributing factors.

Cognitive Warfare is conducted throughout the continuum of conflict and aims to stay below the threshold of armed conflict[28]. Cognitive warfare can be functionally defined as "the weaponization of public opinion, by an external entity, for the purpose of influencing public and governmental policy and destabilizing public institutions"[29]. An operational definition of Cognitive Warfare is provided by the NATO Allied Command Transformation (ACT), NATO's Strategic Warfare Development Command:

---

[23] D. Kahneman, A. Tversky, *Prospect theory: An analysis of decision under risk*, "Econometrica" 47, no. 2 (1979): 263-291. Reprinted [in:] MacLean, L.C., Ziemba W.T (eds.), *Handbook of the Fundamentals of Financial Decision Making*, World Scientific Handbook in Financial Economics Series Vol. 4, World Scientific Publishing, Singapore, 2013, pp. 99-127. DOI: 10.1142/9789814417358_0006.

[24] A. Bovet, H.A. Makse, *Influence of fake news in Twitter during the 2016 US presidential election*, "Nature Communications" 10, no. 1 (2019): 1-10.

[25] M.E. Kosal, H. Regnault., *Introduction,* [in:] M. Kosal (ed.), *Disruptive and Game Changing Technologies in Modern Warfare. Advanced Sciences and Technologies for Security Applications*, Springer, Cham, 2020, pp. 1-11. DOI: 10.1007/978-3-030-28342-1_1.

[26] H. Allcott, M. Gentzkow, S*ocial media and fake news in the 2016 election*, "Journal of Economic Perspectives" 31, no. 2 (2017): 211-236.

[27] M. Marsili, *Guerre à la Carte*, 2023.

[28] Id. See also: M. Marsili, *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*, "Honvédségi Szemle–Hungarian Defence Review" (HDR) 150, no. 1-2 (2022): 36-48. DOI: 10.5281/zenodo.5578016.

[29] A. Bernal, C. Carter, I. Singh, K. Cao, O. Madreperla, O., C*ognitive Warfare: An Attack on Truth and Thought*, NATO, Bruxelles, 2021. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf.

"activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviors, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary. Designed to modify perceptions of reality, whole-of-society manipulation has become a new norm, with human cognition shaping to be a critical realm of warfare"[30].

The U.S. joint doctrine and the NATO policy have already recognized cyberspace[31] as an operational military domain and are striving to include the cognitive realm among the battle spaces[32]. As the cognitive dimension becomes increasingly relevant in present and future geopolitical challenges, NATO takes the necessary action against "weaponized information" in modern warfare, and cognitive warfare has been acknowledged as a military priority for the Alliance[33]. NATO ACT, tasked by the Military Committee (MC), drafted a Cognitive Warfare Exploratory Concept as part of the Warfare Development Agenda (WDA) and is meant to enhance the Alliance's knowledge of the emerging threats in the cognitive dimension while exploring potential future warfare development[34]. The Concept, delivered in May 2023 and to be refined and aligned with Allied Command Operations (ACO) for MC approval, defines cognitive warfare and illustrates its impact on society, political decision-making, military capability, readiness, effectiveness, and response[35].

While fast technological change makes the future of warfare uncertain and unpredictable, the metaverse, with its growing popularity and immersive nature, provides a unique context for exposure to this distorted information, and seems to be the "natural" environment to conduct information and cognitive attacks. The term "metaverse" was coined in 1992 by visionary author Neal Stephenson in his dystopian sci-fi thriller *Snow Crash*[36], which predicted the metaverse as a convergence

[30] NATO Allied Command Transformation (ACT), *Cognitive Warfare: Strengthening and Defending the Mind*, 5 Apr. 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind; NATO Allied Command Transformation (ACT), *Cognitive Warfare: Beyond Military Information Support Operations*, 5 Apr. 2023. https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations.

[31] Although there is no consensus on what "cyberspace", in the scope and for the purpose of this research, we refer to operative definitions provided by NATO STO in *Allied Joint Publication AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*: "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data". A similar definition is set forth in U.S. Joint Chiefs of Staff, *Joint Publication JP 3-12 on Cyberspace Operations*: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers". A broader definition is provided in 50 USC §1708(d)(2) and by NIST https://csrc.nist.gov/glossary/term/cyberspace, and a last one in the *EU Cyber Defence Policy Framework* (2018 update). For a discussion, see: M. Marsili 2019, 2022, 2023.

[32] M. Marsili, *The War on Cyberterrorism*, "Democracy and Security" 15, no. 2 (2019): 172-199; M. Marsili, *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*, 2022; M. Marsili, *Guerre à la Carte*, 2023; M. Marsili, *L'evoluzione delle forze speciali nelle Multi-Domain Operations (MDO)*, 2023.

[33] NATO STO, *HFM-377 Call for Papers Symposium on Meaningful Human Control in Information Warfare: Encompassing Control of Future Operations across Warfare Domains and the use of Advanced AI* (No. 18/24), STO Collaboration Support Office–HFM Panel, Neuilly-sur-Seine Cedex, p. 4, https://events.sto.nato.int/index.php/upcoming-events/event-list/download.file/3238.

[34] M. Marsili, *Guerre à la Carte*, 2023.

[35] The *Concept* is not public due to security restrictions.

[36] N. Stephenson, *Snow Crash*, Bantam Books, New York, NY, 1992.

between the real and virtual world – a universe beyond the physical, where physical reality merges and interacts with digital virtuality[37]. The metaverse is expected to be an immersive experience where real-world people, problems, and models come to life in a virtual world determined by artificial intelligence, enhancing human-machine interactions[38].

The metaverse is the next disruptive technology, a transformative or revolutionary technology that, because of its dual use nature[39], is poised to have a significant effect (positive and negative) on societies and decision-makers over the next 20 years. Still in its early stages of development, the metaverse is expected to be mature by 2030, reaching a scale far beyond what is available today, with an estimated 1 billion users by then[40], and a huge impact on society in the coming decades. The metaverse may revolutionize aspects of our societies; therefore, the implications of culture, concepts, risk-tolerance, organizational structure, policies, treaties, human capital, morals and ethics must be fully appreciated.

Stephenson wrote that everything in the metaverse "depends upon the ability of different computers to swap information very precisely, at high speed, and at just the right times" and that "people who go into the metaverse…understand that information is power"[41]. «The metaverse may be virtual, but the impact will be real' is the slogan of Meta (formerly Facebook)[42].

Challenges we are currently facing, such as the dissemination of false information and disinformation, will be boosted and facilitated by the intrusive, engaging, and manipulative nature of the metaverse, far beyond our current experience[43]. The metaverse shifts the user experience from simple observation to participation, increasing the emotional impact, and poses the challenge of how (and whether) to "import" the rules of the real world into the virtual world[44]. The lack of international rules will leave the metaverse available for cognitive hacks perpetrated by non-state actors, and in the hands of companies with the power to determine who can have access to the "middle world" as happens on social media platforms[45].

---

37 M. Marsili, *Guerre à la Carte*, 2023, p. 7.

38 M. Marsili, *L'evoluzione delle forze speciali nelle Multi-Domain Operations (MDO)*, 2024, p. 59.

39 Dual-use technologies are advanced solutions deriving from civilian or defence industries with military and commercial end uses.

40 McKinsley & Co., *Value creation in the metaverse*, June 2022, https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf; I. Tucci, D. Needle, *What is the metaverse? An explanation and in-depth guide*, TechTarget, Newton, Mass., Sept. 2023, https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know; D. Crawford, D. Aulanier (eds.), *Technology Report 2023, Reset and Reinvent: The Thriving Landscape of Tech Innovation*, Bain & Company, Boston, Mass., 2023, https://www.bain.com/globalassets/noindex/2023/bain_report_technology_report_2023.pdf.

41 Stephenson, *Snow Crash*, p. 400, 431 [cited in M. Marsili, *Guerre à la Carte*, 2023, p. 7-8].

42 M. Marsili, L'evoluzione delle forze speciali nelle Multi-Domain Operations (MDO), 2023, p. 59-60.

43 *Ibidem.*

44 *Ibidem.*

45 *Ibidem.*

The rapid developments in AI technology, such as deep learning, have led to an increased pervasiveness and proliferation of misinformation through deep fakes, which are a type of synthetic AI-generated media (including video, images, text and audio) that are becoming increasingly difficult to detect both by the human eye and by existing detection technologies[46]. The rise of generative AI technology calls for a focus on international standards to determine the authenticity of multimedia through the adoption of policy measures, codes of conduct and regulations – such as watermarking and blockchain technology, enhanced security protocols and extensive cybersecurity awareness–aimed to enhance the trustworthiness of AI systems[47].

The challenges posed by the use of AI can impact multiple layers. AI-generated content can closely resemble or even reproduce intellectual property, raising questions about copyright infringement. Generative AI in content creation could make it more challenging for human creators to attest and defend ownership of their content.

In the near future, AI-based technology will play an increasingly significant role in the digital information environment, where the speed of machine-driven decision-making process leaves little to no time for the human to intervene– to maintain any meaningful oversight, let alone control. This scenario triggers concerns and poses serious challenges associated with information accountability and assessment (discerning between intentional mal/mis/disinformation and valid counter hypotheses/arguments/evidence)[48]. AI-assisted operations are expected to have an immense impact in the information environment, influencing virtual, physical, and cognitive dimensions[49]. Emerging and advanced AI capabilities such as large language models (LLMs), foundation models,[50] generative adversarial networks (GANs)[51], unsupervised machine learning (ML)[52], generative AI[53] (where algorithms generate content), next-gen AI and cyber-enabled large-scale socio-cultural influence operations are likely to play an increasingly significant role in the future digital information environment.

[46] AI for Good, *Detecting deepfakes and Generative AI: Standards for AI watermarking and multimedia authenticity*, International Telecommunication Union (ITU), Geneva, 2024, https://aiforgood.itu.int/event/detecting-deepfakes-and-generative-ai-standards-for-ai-watermarking-and-multimedia-authenticity/.

[47] *Ibidem.*

[48] *HFM-377 Call for Papers*, p. 4.

[49] *Ibidem*, p. 5-6.

[50] Foundation models are a form of generative AI, based on complex neural networks including generative adversarial networks (GANs), which generate output from one or more inputs (prompts) in the form of human language instructions.

[51] Generative adversarial network (GAN) is a deep-learning-AI based generative model. This powerful class of neural networks are used for unsupervised learning machine.

[52] Unsupervised machine learning is a type of ML that learns from data without human supervision.

[53] Learning the patterns and structure of their input training data, and enabled by deep neural networks, particularly LLMs, generative AI can create text, images, videos, or other new data with similar characteristics, often in response to prompts.

The EU is strongly concerned about the impact of cognitive actions that convey AI-manipulated or AI-generated content on social media platforms and has recently adopted measures to mitigate such risks.

The Artificial Intelligence Act will entered into force on 1 August 2024 warns about AI-enabled manipulative or deceptive techniques, facilitated by machine-brain interfaces or virtual reality, that can deliver multimedia subliminal contents to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices with negative effects on democratic processes, civic discourse and electoral processes, including through disinformation[54], and hence prohibits such techniques within the EU[55].

The AI Act acknowledges that generative AI systems have a significant impact on the integrity and trust in the information ecosystem, raising new risks of misinformation and manipulation at scale of text image, audio or video content (deep fakes)[56] and call for implementation of measures for mitigating such risks through the detection and labelling of AI generated or manipulated content[57].

A previous EU regulation, the Digital Services Act (DSA) 2022, updates the Electronic Commerce Directive 2000 regarding illegal content, transparent advertising, and disinformation. The DSA is meant to "govern the content moderation practices of social media platforms" and introduces obligations for illegal content removal from very large online platforms (VLOPs) with more than 45 million monthly active users, including Facebook, Twitter, TikTok, and Google's subsidiary YouTube.

The EU legal frawemork, while on the one hand makes clear how timely and urgent is the need for preventing and mitigating cognitive maligne actions in the digital enviroenment, on the other hand stresses the importance for safeguarding fundamental human rights, media pluralism and the freedom of expression and information[58]. A week point of the AI Act is that it does not apply to AI-systems used for military, defence or national security purposes[59] – the latter has such a vast scope that any topic can be encompsssed, from environmental to security, to food security and health security, including the broader term of "human security" currently under development by the NATO[60].

[54] AI Act 2024, §§29, 120, 136.

[55] AI Act 2024, Art. 5 §1(a) and Art. 50 §§2, 4.

[56] The AI Act 2024 in Art. 3(§60) provides the following official definition of the term "deep fake": AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.

[57] AI Act 2024, §§ 133, 134, 135.

[58] DSA 2022, §§ 3, 22, 51, 52, 54, 63, 81, 90, 149, 150, 153, Art. 14.4, Art. 34.1(b), Art. 48.4(e), Art. 91.2(f); AI Act 2024, §§ 48, 134.

[59] AI Act 2024, Art. 2.3, Art. 2.6.

[60] M. Marsili, Shifting Terms and Concepts: From Defence to (Human) Security, [in:] Book of Abstracts of the XII Portuguese Congress of Sociology (XII APS Congress). Lisbon: Portuguese Association of Sociology (APS), 2023, p. 277. DOI: 10.5281/zenodo.7810950. M. Marsili, D. Hughes, Legal Framework Supporting Human Security, [in:] Human Security: Frameworks, Concepts, Actors and Challenges in Relevance to NATO. Paris: Science and Technology Organization (STO), 2024, p. 19-22. DOI: 10.14339/STO-TR-HFM-ET-201.

Conclusions

What triggers major concerns among true human rights advocates is the attitude of Western governments that present themselves as champions of fundamental rights and freedoms[61]. Democratic countries took advantage of the COVID-19 pandemic to strengthen control over freedom of speech, delegating the implementation of soft censorship to social media platforms[62]. This trend has become even more pronounced in the context of the confrontation with Russia and the conflict in Ukraine[63]. Special agencies tasked to monitor cognitive malign actions have been established in the US, Sweden, France, Spain, Slovakia, and a bill aimed at establishing an Agency on Disinformation and Cognitive Security[64], tasked to counter "fake news" and to preserve "freedom and democracy", has recently been introduced in the Italian Parliament[65]. History teaches us that control is a germinal form of censorship, a turning point in the crackdown of fundamental rights and freedoms. A notorious example is the Red Scare that pervaded the United States in two waves (1917-1920 and 1947-1957), the second of which is known as "McCarthyism", a witch hunt that resulted in serious restrictions of civil liberties in the name of security, including limitations on free speech. In liberal democracies, freedom of expression implies that all people should have the right to express themselves through their writings, or in any other way of conveying personal opinions or creativity– whether orally, in writing or in print, through art, or via any other media.[66] That is why freedom of speech and freedom of expression are cornerstone principles to be defended above all else– regardless of security or other pseudo-values. Human freedoms are never definitive achievements; they are precious assets that must be defended day by day.

Bibliography

Allcott H., Gentzkow M., S*ocial media and fake news in the 2016 election*, "Journal of Economic Perspectives" 31, no. 2 (2017): 211-236.
Bone J., *Cognitive Hack: The New Battleground in Cybersecurity... the Human Mind*, 1st ed., New York, NY, Auerbach Publications, 2017. DOI: 10.1201/9781315368412.
Bovet A., Makse H.A., *Influence of fake news in Twitter during the 2016 US presidential election*, "Nature Communications" 10, no. 1 (2019): 1-10.
Cybenko G., Giani A., Thompson P., *Cognitive Hacking: A Battle for the Mind*, "IEEE Computer" 35, no. 8 (2002): 50-56.

[61] M. Marsili, *The Protection of Human Rights and Fundamental Freedoms at the Origins of the European Integration Process*, "Europea" 5, no. 1 (2018): 191-203. DOI: 10.4399/978882551597810.
[62] M. Marsili, *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus*, "Europea" 10, no. 2 (2020): 147-170. DOI: 10.4399/97888255402468.
[63] M. Marsili, *Inside and beyond the Russo-Ukrainian War: The Pitfalls of the European Union*, "Newsletter of the Academy of Yuste" 16 (2022): 4-5. DOI: 10.5281/ZENODO.6595805. Reprinted in: *Newsletter Annual of the Academy of Yuste: Reflections on Europe and Ibero-America*, Vol. 3, Year 2022, 1st ed., Fundación Academia Europea e Iberoamericana de Yuste, Cuacos de Yuste, 2023, pp. 430-431. DOI: 10.5281/ZENODO.8075295.
[64] Italian: *Agenzia per la disinformazione e la sicurezza cognitiva*.
[65] Senate of the Republic, XIX Legislature, *Meeting record n. 277 of 19 May 2024*, Joint Committee 1 and 2, Amendments to bill no. 1143, § 8.0.1, pp. 23-25, https://www.senato.it/service/PDF/PDFServer/DF/437423.pdf.
[66] M. Marsili, *The Press: Fourth Power or Counter-power?*, "ArtCiencia.com", 24-25 (Dec. 2019-July 2021): 2. DOI: 10.25770/artc.18415.

Diemer J., Alpers G.W., Peperkorn H.M., Shiban Y., Mühlberger A., *The impact of perception and presence on emotional reactions: A review of research in virtual reality*, "Frontiers in Psychology" 6 (2015): 1-9. DOI: 10.3389/fpsyg.2015.00026.
Durkheim E., *Suicide: a study of sociology*, The Free Press, New York, NY, 1966.
Forrester B., Rosell M., Dragos V., Marsili M., *Value Differences: A Starting Point for Influence*, [in:] *Mitigating and Responding to Cognitive Warfare. Proceedings of the HFM-361-RSY Symposium held on 13-14 Nov. 2013 in Madrid, Spain*, NATO Science & Technology Organization (STO), Paris, 2024, pp. P3-1-P3-18. DOI: 10.14339/STO-MP-HFM-361.
Guess A., Nyhan B., Reifler J., *Exposure to untrustworthy websites in the 2016 US election*, "Nature Human Behaviour" 4, no. 5 (2000): 472-480.
Kahneman D., Tversky A., *Prospect theory: An analysis of decision under risk*, "Econometrica" 47, no 2 (1979): 263-291. Reprinted [in:] MacLean, L.C., Ziemba W.T (eds.), *Handbook of the Fundamentals of Financial Decision Making*, World Scientific Handbook in Financial Economics Series Vol. 4, World Scientific Publishing, Singapore, 2013, pp. 99-127. DOI: 10.1142/9789814417358_0006.
Kosal M.E., Regnault H., *Introduction*, [in:] M. Kosal (ed.), *Disruptive and Game Changing Technologies in Modern Warfare. Advanced Sciences and Technologies for Security Applications*, Springer, Cham, 2020, pp. 1-11. DOI: https://doi.org/10.1007/978-3-030-28342-1_1.
Lee K.M., Nass C., *Experimental tests of normative group influence and representation effects in computer-mediated communication: Evidence for the social identity model of deindividuation effects*, "Communication Research" 30, no. 1 (2023): 36-52.
Marsili, M., *La rivoluzione dell'informazione digitale in Rete. Come Internet sta cambiando il modo di fare giornalismo*, Odoya, Bologna, 2009, p. 19. DOI: 10.5281/zenodo.33614.
Marsili M., *The Protection of Human Rights and Fundamental Freedoms at the Origins of the European Integration Process*, "Europea" 5, no. 1 (2018): 191-203. DOI: 10.4399/978882551597810.
Marsili M., *The War on Cyberterrorism*, "Democracy and Security" 15, no. 2 (2019): 172-199.
Marsili M., *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus*, "Europea" 10, no. 2 (2020): 147-170. DOI: 10.4399/97888255402468.
Marsili M., *The Press: Fourth Power or Counter-power?*, "ArtCiencia.com", 24-25 (Dec. 2019-July 2021): 1-11. DOI: 10.25770/artc.18415.
Marsili M., *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*, "Honvédségi Szemle– Hungarian Defence Review" (HDR) 150, no. 1-2 (2022): 36-48. DOI: 10.5281/zenodo.5578016.
Marsili M., *Inside and beyond the Russo-Ukrainian War: The Pitfalls of the European Union*, "Newsletter of the Academy of Yuste" 16 (2022): 1-31. DOI: 10.5281/ZENODO.6595805. Reprinted in: *Newsletter Annual of the Academy of Yuste: Reflections on Europe and Ibero-America*, Vol. 3, Year 2022, 1st ed., Fundación Academia Europea e Iberoamericana de Yuste, Cuacos de Yuste, 2023, pp. 429-445. DOI: 10.5281/ZENODO.8075295.
Marsili M., *Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse*, "Applied Cybersecurity & Internet Governance" (ACIG) 2, no. 1 (2023): 1-11. DOI: 10.60097/ACIG/162861.
Marsili M., *L'evoluzione delle forze speciali nelle Multi-Domain Operations (MDO). La necessaria capacità di operare nell'ambiente cyber e spaziale. La capacità di utilizzo del Metaverso*, IRAD-Istituto di Ricerca e Analisi della Difesa, Roma, 2024.
McLuhan M., *Understanding Media:The Extensions of Man*, McGraw-Hill, New York, NY, 1964.
McLuhan M., Fiore, Q., *War and Peace in the Global Village*, Bantam Books, New York, NY, 1968.
Paprocki R., Wróblewska-Jachna J., *Empirical and Social Anxiety about the Covid-19 Pandemic: Measurement, Diagnosis, Modelling*, "ASK. Research & Methods" 31 (2022), 47-68.
Pessoa L., *How do emotion and motivation direct executive control?*, "Trends in cognitive sciences" 13, no. 4 (2009): 160-166.
Sorokin P.A., *The Sociology of Revolution*, Howard Fertig, New York, NY, 1967.
Staniszkis J., *Anthropology of power. Between the Lisbon Treaty and the crisis*, Wydawnictwo Prószyński Media, Warsaw, 2009.
Stephenson N., *Snow Crash*, Bantam Books, New York, NY, 1992.
Sztompka P., *Socjologia zmian społecznych*, Znak, Kraków, 2005.
Tilly C., *From Mobilization to Revolution*, Addison-Wesley, Reading, MA, 1978.
Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, 2018.

Online references
Bernal A., Carter C., Singh I., Cao K., Madreperla O., *Cognitive Warfare: An Attack on Truth and Thought*, NATO, Bruxelles, 2021, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf.
Crawford D., Aulanier D. (eds.), *Technology Report 2023, Reset and Reinvent: The Thriving Landscape of Tech Innovation*, Bain & Company, Boston, Mass., 2023, https://www.bain.com/globalassets/noindex/2023/bain_report_technology_report_2023.pdf.
EU-U.S. Trade and Technology Council, Working Group 1: Technology Standards, Subgroup on AI Taxonomy & Terminology, *EU-U.S. Terminology and Taxonomy for Artificial Intelligence*, 2nd ed., European Union, 5 April 2024, https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition.
AI for Good, *Detecting deepfakes and Generative AI: Standards for AI watermarking and multimedia authenticity*, International Telecommunication Union (ITU), Geneva, 2024, https://aiforgood.itu.int/event/detecting-deepfakes-and-generative-ai-standards-for-ai-watermarking-and-multimedia-authenticity/.
Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *A definition of AI: main capabilities and disciplines. Definition developed for the purpose of the AI HLEG's deliverables*, European Commission, Brussels, 8 April 2019, https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.
McKinsley & Co., *Value creation in the metaverse*, June 2022, https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20metaverse/Value-creation-in-the-metaverse.pdf.
NATO Allied Command Transformation (ACT), *Cognitive Warfare: Strengthening and Defending the Mind*, 5 Apr. 2023, https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind.
NATO Allied Command Transformation (ACT), *Cognitive Warfare: Beyond Military Information Support Operations*, 5 Apr. 2023, https://www.act.nato.int/article/cognitive-warfare-beyond-military-information-support-operations.
Senate of the Republic, XIX Legislature, *Meeting record n. 277 of 19 May 2024*, https://www.senato.it/service/PDF/PDFServer/DF/437423.pdf.
STO Collaboration Support Office–HFM Panel, *HFM-377 Call for Papers Symposium on Meaningful Human Control in Information Warfare: Encompassing Control of Future Operations across Warfare Domains and the use of Advanced AI* (No. 18/24), STO Collaboration Support Office, Neuilly-sur-Seine Cedex, 2024, https://events.sto.nato.int/index.php/upcoming-events/event-list/download.file/3238.
Tucci I., Needle D., *What is the metaverse? An explanation and in-depth guide*, TechTarget, Newton, Mass., Sept. 2023, https://www.techtarget.com/whatis/feature/The-metaverse-explained-Everything-you-need-to-know.

Digital Revolution and Artificial Intelligence as Challenges for Today

Summary

This article addresses the social impact of the ongoing digital revolution through a critical analysis of the literature on the subject. The aim is to understand the dynamics of change, which is key to dealing with the complexities of the digital age and realising its potential for sustainable development. The information revolution and artificial intelligence pose significant challenges to modern society by marking a profound transformation through self-organising social changes that disrupt existing norms. The digital age has revolutionized information systems, much like Gutenberg's invention of movable-type printing press. While it enables scientific and economic progress, the information revolution raises ethical, moral and legal concerns. Social media have become "weapons" in a hybrid conflict, where the intangible battleground is human cognitive systems.

Keywords: artificial intelligence, social changes, cognitive warfare, metaverse