SKHID (EAST)

2024, Vol.6, Issue 1, 9-17

https://doi.og/10.28925/2411-3093.2024.611

Reactualising the problem of social engineering and digital security

Maryna Kolinko (ORCID 0000-0002-1043-2742)
Borys Grinchenko Kyiv Metropolitan University (Ukraine)

Halyna Petryshyn (ORCID 0000-0003-3428-8789)
Ternopil Volodymyr Hnatiuk National Pedagogical University (Ukraine)

Halyna Chumak (ORCID 0000-0001-5974-9022)
Ternopil Volodymyr Hnatiuk National Pedagogical University (Ukraine)

ABSTRACT

The article explores the current aspects of social engineering in the digital age. Social engineering is considered as a strategic technology of constructing new meanings, principles, rules and facts of social interaction. The socio-philosophical concepts of K. Popper, P. Sorokin, and R. Silverstone are analyzed in the context of constructive proposals of social engineering. The application of historical and philosophical intellectual constructs to the practices of social transformations is described in the article. The article reveals the possibilities and limitations of digital technologies in social engineering. The risks of creating new tools and algorithms for manipulation, disorientation of users of virtual technologies by social engineering methods are shown within the framework of the digital security problem. The diversity of views on the essence of social engineering and the analysis of its spheres of application problematize the interpretation of its social role and meaning. The methods of constructing social events and interfering in people's lives require critical evaluation. The implementation of AI in social engineering developments leads to the new risks, which are systematized in the article. They are related to the manipulation of public consciousness, distortion of identification and personalisation methods, financial fraud, and violation of human security

KEYWORDS

artificial intelligence,
liminality,
social engineering,
digital security,
social construction,
virtual reality.

Introduction

Social being is represented by a set of objective and subjective processes and the interaction of self-organizing subjects. The inclusion of digital technologies in the modern paradigm of social changes transforms the theoretical and methodological field of social research. The practices of social engineering and influence are also changing. The technological boom of recent years is changing both physical and conceptual space and conditions of human existence. The desire to expand the boundaries of one's space, including geographical, intellectual, and sociocultural boundaries, is an integral and generic feature of human existence; but we observe new intense discussions about the impact of technological processes on social reframing, reformatting of social reality, constructing of new social landscapes, and even controlling the actions of social agents.

The ***purpose of the article*** is to identify modern interpretations of the concept of "social engineering", to analyze the implementation of the principles of social engineering in the modern digital space and the role of artificial intelligence (AI) in their use.

Research methods

Active transformations of virtual reality, digital processes, the development of AI encourage scientists to understand the perspectives of humanity and look for adequate methodological tools. At first, it is necessary to define the ***object*** in which the social engineering procedures are operating. These are different elements and spaces of social reality. Social reality is generated by people in the process of their communication and life activities. The phenomena of social reality include human life, social groups and communities, society in general, and virtual reality. The object of social changes can also be social complexes, relationships, social structures, social institutions and organizations, values and norms, public opinion, social technologies and innovations. The rapid development of virtual world technologies increases the possibilities and dangers of social engineering. The ***subject*** of our scientific investigation is the transformation of the concept of social engineering in the conditions of modern digital society and virtual reality.

Understanding the problem of the ***virtual*** begins in the history of philosophy with the objective idealism of Plato. Plato considered the existence of the Absolute, the existence of eidos to be reality. Our earthly world is only an illusion that reflects the true reality. The concept of "***virtual***"

m.kolinko@kubg.edu.ua
pgr190364@tnpu.edu.ua
chumak@tnpu.edu.ua

directly comes from the Latin "virtus", which philosophers gradually equated with the Greek term "dynamis" (δυναμις), which characterized the sphere of potential or possible. The virtual is something that opposes the phenomena that exist in reality and can manifest itself only if certain conditions are met. Medieval scholasticism gives the virtual the categorical status of the transcendent in the course of rethinking the theories of Plato and Aristotle. The scholastics pointed to the establishment of a connection between realities with the help of "virtus" and the formation of an ontological hierarchical configuration in this way. In modern times, "virtual" has received an epistemological status. It was understood as the state of existence of an object in which it is not yet manifested in actuality, but is already present in an embryonic state. "Virtus" preserves the potentialities of the world, which are realized as they are revealed to human cognition.

The modern connotation of "virtual" has been semantically "approached" to the semantics of IT phenomena. It can be argued about the hypertrophic nature of its interpretation, where the previous ontological semantic load is forgotten. Virtual as immaterial, potentially possible, something that does not exist in reality, but can happen under certain conditions according to the classical philosophical understanding, approaches to the description in the terms of the post-industrial, informational, technological world. Under the influence of information technologies, the virtual is interpreted as a world of artificial realization of possibilities of thinking. This is a symbolic and graphic simulation of the real world using digital technologies.

Virtual reality was created not only for interactive communication and entertainment. It becomes an important component of economies, political discourse, and the educational sphere. Today, the virtual again acquires an ontological meaning, it begins to "inscribe" new phenomena arising in the social and scientific world into the frames of the existing social order, it supports, improves this order, or, on the contrary, denies, overthrows and changes it. Models of modern society are changing significantly under the influence of virtual structures implemented through electronic devices, such as computers and other gadgets, mobile communications, and satellites. Virtual technologies are being constantly updated and give a new status to social phenomena that belonged to everyday life: from social networks, the "gaming epidemic" that creates "detached from reality" teenage gamers, to reframing of the media space and to the description of electronic payment systems or electronic government, military technologies, unmanned combat drones and virtual reality helmets. The viral spreading of a psychological state in which a social subject does not want to make a distinction between reality and artificially created reality, losing the firm ground of the world of material things is being recorded lately. Under the influence of the virtualization of various spheres of life, new forms of perception of time and space arise, the so-called "private temporality", when life is felt and described in terms of permanent procedural reality.

Certain Western researchers argue that the rules of the digital world give rise to a paradigm of digimodernism (a term coined by the British culturologist Alan Kirby). Digitization leads to the fact that we all participate in the creation of a new fabric of social existence, create a new text of culture. It is liminal with moving boundaries. But liminality in the digital society acquires signs of permanence and normality.

It is appropriate to define the contexts of use of the methodological concept "liminality" in our research. The concept initially characterizes the experience of rites of passage in social anthropology. The definition of a transitional stage in life of a person or a group from one social status to another as a liminal state is provided by Stephen Turner as a representative of symbolic anthropology. He used the classic Latin concept of "limit". Originally it meant "border", "finity" and was opposed to infinity. The border is interpreted as a formative force, it shows the differences of phenomena, their separation, in order to realize the forms of connection and continuity. We should take into account the processes of differentiation, separation, and selection. "The borders exist and have meaning in relation to other spaces, they mark spatial intersections, border crossings, getting from one's place to someone else's" (Kolinko, 2019: 155). Therefore, there is an urgent need for a new theoretical basis capable of adequately reflecting the changing modalities of society digitalization, the liminal states of social structures and subjects. Liminality becomes the theoretical and methodological tool that describes actual processes taking place in the social, scientific, and anthropological space.

Stephen Turner describes meaningful changes in the use of the theory of liminality according to the conditions of the information technology world: «We are shocked, or put into a liminal state, when we are compelled to adjust to a different technology or environment which our pre-existing cognitive make-up, our mental and bodily habits, fails to prepare us for. Mental habits are formed by repetition. But this is not the only way that deep cognitive change occurs. Ritual behaviour is a behavioural technology that induces cognitive change" (*Turner, 2022: 98*).

The dramatic nature of procedurality, instability, and rootlessness is the main feature of the digimodern world. There are only social events and cultural acts of the present, without the past and the future. Not only political forces, social strata, and economic strategies are involved in the construction of this world, but also the everyday actions of each of us, our activities in the open digital space. In the introduction to Alan Kirby's "Digimodernism: How New Technologies Dismantle the Postmodern and Reconfigure Our Culture", the editor notes, "Beginning with the Internet (***digimodernism's*** most important locus), then taking into account television, cinema, computer games, music, radio, etc., Kirby analyzes the emergence and implications of these diverse media, coloring our cultural landscape with new ideas on texts and how they work. This new kind of text produces distinctive forms of author and reader/viewer, which, in turn, lead to altered notions of authority, 'truth' and legitimization. With users intervening physically in the creation of texts, our electronically-dependent society is becoming more involved in the grand narrative" (Kirby, 2009: 3). A. Kirby is critical and pessimistic while describing the tendency of modern society towards digimodernism. Electronic textuality, in his view, is ephemeral, illusory, and creates a fragmented reality of pastiche and comics, and primitivizes culture. Every moment someone types text in the messengers, likes, sends texts that are not confirmed by careful, meticulous work with related original sources and professional expert opinions. He is confused by the marginal level of socio-cultural reactions.

Results and Discussion

The application of technical and scientific thinking to social processes in the 20th century gave legitimacy to social engineering technologies, demonstrated the belief that positivist constructions can shape social institutions and improve the fate of humanity. Today, humanity has found itself on the verge that defines not only a new technological world, but also new meanings, tasks and radically new strategies for solving them. The problems of AI and its combination with human abilities, the involvement of social engineering methodologies in the digital world became an urgent task of philosophical reflection.

One can say, without falling into contradiction, that there are both many and few works devoted to social engineering. There are many of those studies, describing different variations of rational social transformations or the intervention of digital technologies in the social fabric of society and the life of an individual. This happens most often at the level of either common or applied scientific interest. Philosophical explorations are also contradictory, radically controversial in their assessments of the phenomenon, they do not clarify the essential characteristics of social engineering in relation to the modern technological landscape. The theoretical vagueness and inconsistency in understanding the role of social engineering in the information society reflects the contradiction of the practical application of its technologies to modern social phenomena. As a sociological branch, social engineering is focused on solving practical social problems. As an engineering activity, it implements engineering methods and developments in practices. Within the framework of social engineering, a research case is distinguished as the analysis of social processes and formations, diagnosis of their condition, expert assessment; a case of social construction as the design, programming, planning of social relations and events; a case of organizational, technological and managerial activity.

Karl Popper's post-positivist concept is historically significant. He proposed using social engineering to build an open society. He reasoned about the transformation of social structures, which embodies the rational interactions of democratic institutions. This, according to K. Popper, will make it possible to carry out gradual social transformations without resorting to violence. The doctrine of social engineering is based on social technologies and reformist politics. Popper considered social institutions as means to achieve a noble goal - to save humanity from possible misfortunes. The applied nature of social engineering forces to develop specific methods of subjectivation of social transformations, but Popper's belief in the viability of a society subject to gradual "step-by-step transformation" through social construction seems utopian to us. Meanwhile, modern partial and gradual social engineering practices, such as design, reconstruction and management of objects as leading in various spheres of social life, make social engineering a rather flexible and interesting methodology for transformations.

In this regard, avant-garde investigations are represented by the Harvard Sociological Studies. They used a solidarist approach in creating a complex of methods for constructing a society of consent. For example, P. Sorokin proposed a program of altruistic education that took into account the method of "good deeds", the method of "heroic example", and other methods of creativity in everyday life, which contributed to socio-cultural improvement. This methodological social program is not immune to errors and idealization, but it develops in view of the new knowledge of social sciences, along with developments in conflict studies. Thus, the methodological synthesis of conflict-oriented and solidarist approaches can show effectiveness in social reforms and is promising for further research. In order to avoid the most acute forms of social conflicts, scientists are developing concepts of finding ways to social consent, social engineering technology, and social therapy of society.

In American sociology, the problem of differentiating the levels of social cognition and construction was realized already in the 30s of the last century. Today, the division of science into fundamental, applied and social engineering in America has a solid material, financial and organizational basis, although the boundary between these levels is very mobile. In general, the applied function of social theory prevails in the West today.

In India, such technologies have brought society together from different castes in the state of Bihar, but today political parties are trying to use it for their own gain and are setting society up for conflict and social "disharmony" (*Shirodkar, 2023*).

We could see the consequences of repressive social engineering in the former Soviet Union. The creation of the illusion of a rational society was based on simulacra of "scientific analysis and management" of a "cogs and gears" of society. The concept of the "new Soviet man" became the basis for the creation of an inhumane, obedient, servile Russian society. In such situations, social engineering inevitably created the technological conditions for manipulating human behavior for the benefit of the authorities. Depending on the goals of social transformations and value orientations, a social engineer can move either towards democracy or despotism. The change of social and anthropological meanings, political requirements, and cultural expectations leads to the need to transform social laws, norms, rules and institutions. Social engineering provides effective mechanisms for constructing new meanings, laws and principles of social interaction. It can be used both for the improvement and construction of transparent, democratic social structures, and work to the detriment of the public. As it was stated above, it all depends on the agents of social change and their tasks.

The emergence of new power discourses in connection with the paradigms of the "information society", "knowledge society" continue and improve the concepts of technocratism ("the power of technical experts" by Thorstein Veblen, "the power of managers" by James Burnham, "the technostructure" by John Kenneth Galbraith, "silent revolution" by Daniel Bell, "power of experts" of the modern digital environment). Advancing the idea of the technological world as the power of a highly educated class, which shapes public opinion and corrects the mental landscapes of society, changes the interpretation of social engineering in the space of digital culture. Built on the principles of social construction, the digital world increasingly uses social engineering algorithms. It is a dynamic and moving world that is constantly reproduced, interpreted and further transformed under the influence of new knowledge. The question is about the manipulative possibilities of its interference in people's lives. It is no longer an open discursive space for democratic changes and harmony of society, but an instrument of " mass personal social engineering" (*Gehl, Lawson, 2022*), technological influence on "a public mind with limited intelligence", which needs help in making decisions, is not capable of socially responsible and timely reactions in a world of rapid changes. In this case social engineering is articulated as a set of operations, psychological methods and techniques, the purpose aimed to obtain confidential information from social subjects. According to analysts' forecasts, such attacks on people will only increase in future.

Productive options include municipal and urban projects. We consider the construction of polycentric models of the modern city as "creative city", "fifteen-minute city" (chrono-urbanism) (*Kolinko, 2023*), etc., which work in the paradigms of "smart space" and "shaping a happy life" to be successful programs of social engineering.

Another interesting example of engineering practices relates to the creation of a solidary social environment as the concept of "consent engineering" was formulated and developed. It is built on communication strategies and the development of communication channels. The term "the engineering of consent" is used to describe an action-based method of contriving the populace to develop liking for or support a program or idea" (*Arqoub et al., 2019*). Communication technologies determine the vector for the development of social engineering, also called Public Relations. They are one of the most vivid examples of the successful implementation of the theory and practice of social engineering. PR is a system of methods, technologies and techniques used in a certain sequence to influence public opinion. PR seeks to construct the reality in which a group, an organization, a firm or an institution operates. Thus, the communicative turn in modern culture and the increasing role of PR management created conditions for the game of social engineering in a new social field. One of its interpreters was Edward Bernays, "One of the borrowed terms was "social engineering." For example, in a chapter in "The Engineering of Consent," Bernays describes public relations as "a broad social-engineering process." Like the social reformers and managerialists, the mass social engineers recognized the rhetorical power of claiming to do "engineering" … Bernays cautioned that we must recognize that the emerging tools and techniques of mass communication could be used for good or evil, to promote or to subvert democracy, and that, as a result, "mastering the techniques of communication" for promoting socially constructive ends would be necessary for the maintenance of democratic societies. If done right, the consent engineers can become an "invisible government the true ruling power of our country" (*Gehl, Lawson, 2022*).

The fascination with social engineering has spread to economic, political, even everyday activities. Robert Gehl and Sean Lawson argue, "Managerialism even found its way into the home. Frank Gilbreth's partner Lillian ...made scientific management a way of life in the home" (Gehl, Lawson, 2022). They give the example of «engineered model kitchens – one was called the Kitchen Efficient – and purported to eliminate, for instance, five out of every six steps in the making of coffee cake. To make a lemon-meringue pie, a housewife working in an ordinary kitchen walked two hundred and twenty-four feet; in the Kitchen Efficient, Gilbreth claimed, it could be done in ninety-two" (*Gehl, Lawson, 2022*).

In other sources, this strategy is called the Domestication. We previously studied this problem, which is relevant in Western sociological literature, and noted that "in modern discourse, domestication is considered as a way of interpreting and using information and communication technologies, their sociocultural adaptation, that is, the actual meaning of this concept is the process of introducing information and communication technologies into everyday life" (*Kolinko, 2018*). The concept was introduced by R. Silverstone and expanded by E. Hirsch, L. Haddon (*2011*), K. Lacey. It reveals urgent technological changes, but opposes models of technological determinism. This procedure outlines the movement of technology from scientific management to people's everyday lives. The perception of virtuality as a purely technological phenomenon of the information society strives to blur, sharpen, and in certain cases, change the meaning of everyday life as a total human existence, to take on its qualitative characteristic of a "shelter of stability", an understandable and familiar home world in which a person feels comfortable, confident, can hide from individual anxieties and social challenges. The methodological operation of domestication can be aimed at forming a sense of the domestic world, where technologies are reconfigured in conditions of dynamic changes and people adapt to these changes. Avant-garde technological strategies lead out of the "comfort zone", force society to abandon stereotypical thinking, work to achieve common success in collective actions and public communication.

The development of media technologies has substantially changed the perspective of social engineering from theoretical discussions to communicative practices of influencing and managing public opinion. M. McLuhan's idea of media means "human extension" reflects the key direction of this process. McLuhan argues that media are languages, with their own structures and grammar systems. He believed that media continually shape and re-shape the ways in which individuals, societies, and cultures perceive and understand the world. Media engineering has become an actual problem for studying the construction of meanings. Today, the term "social engineering" is increasingly articulated in the context of technological forecasting and intervention, creative generation of new information products with the help of artificial intelligence. The neural networks exist in everyday life and professional activities, they teach us and learn themselves. The implementation of the AI in the practice of social engineering increases the effectiveness of planning and prediction in social processes, accelerates the resolution of problematic issues in the field of social construction and social policy. However, the ethical issues in the use of artificial intelligence are not resolved at all, and there are no effective regulators that would prevent mistakes and intentional illegal actions directed against people. Because of these processes, there is a narrowing of the interpretation of the term "social engineering" as information manipulation and, even, "information theft". IT specialists classify the wording "social engineering" as the phenomena of information fraud and theft. Criminal techniques in the information space, of course, belong to the field of engineering, but their identification with social engineering creates a false impression of the entire industry, which leads to a false understanding of its general goals and processes. Wrongly or not, but such an interpretation of social engineering is actualized in modern media texts, professional and everyday discussions, discussions of IT. Therefore, it is important to analyze and systematize the characteristic manifestations of this negative phenomenon.

The attacks of social engineering can be carried out against a person, a group or an organization from the outside, or they can occur inside the company when hackers get into the system itself. These can be methods of influencing human actions without the use of technical means (using people's weaknesses, psychological features) and interfering with the work of technical facilities.

When artificial intelligence comes into play, the problem of social engineering attacks rises to a new level of social challenges. If AI is tasked with obtaining confidential information about a person or group for the purpose of manipulation, it becomes an imitator of human actions, can synthesize voice, behavior algorithms, disorient the object of manipulation, offer deceptive maneuvers, influence vulnerable centers. The problem of using AI in the information space exacerbates the issue of cybersecurity by protecting the computers, laptops, iPads and other devices used for Internet resources from fraudsters and phishing companies. Current Internet publications record that such risks, social engineering attacks and the need for cyber security are considerably underrated. Researchers Fatima Salahdine and Naima Kaabouch are concerned about the involvement of artificial intelligence in social engineering in the space of virtual communication. “Communication systems are vulnerable and can easily be penetrated by malicious users through social engineering attacks. These attacks aim at tricking individuals or enterprises into accomplishing actions that benefit attackers or providing them with sensitive data such as social security number, health records, and passwords. Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust” (*Salahdine, Kaabouch, 2019: 1*). A phone call under the guise of selling useful things or current offers can unexpectedly collect information about one’s personal data in order to be used by fraudsters. “A robocall is a device or computer program that automatically dials a list of phone numbers to deliver prerecorded messages” (*Salahdine, Kaabouch, 2019: 8*). The program can change messages, read your data, fix locations for further attacks. Such attacks create big problems in countries with a developed digital environment. There are impressive gaps in the meaningful understanding of these problems, there are no umbrella strategies that would provide action algorithms to protect social entities from information fraud. The only thing cyber security experts advise in such cases is not to answer unfamiliar and unwanted calls. So, the first protection algorithm calls into question the dreams of humanity of an open world, returns us to philosophical problems of the Stranger as a possible enemy, the problem of distance, borders and boundaries.

The study of chatbots with the Indirect Prompt Injection technique led to the conclusions about the threats of constructing situations by chatbots with artificial intelligence that are not in favor of users of Internet services. “From chatbots that mimic human interactions to voice synthesis and deepfakes that disorient and deceive, these mechanisms exploit trust and exploit human vulnerabilities. As we venture into the intricacies of these technologies, it becomes crucial to understand their operational mechanisms, the risks they present, and the defenses necessary to thwart their malevolent intentions” (*The Role of AI in Social Engineering, 2023*). Website Zvelo at the end of 2023 presented the systematization of such risks, namely human-like interaction, voice synthesis, and deepfakes. Fraudsters can also use the AI for data analysis and targeting. We offer a generalized analysis of the forms of disorientation and deception in the field of social engineering cited by the researchers of Website Zvelo.

The ability of AI to learn and automate problem-solving processes exacerbates the risks of abuse and manipulation of information, material and intellectual resources. Automating target profiling means that “AI takes on the task of automating research to profile potential targets. This falls within the domain of data analytics and machine learning algorithms specialized for pattern recognition and data mining. These algorithms can swiftly scrape data from public records, social media platforms, company websites, and various other sources to gather comprehensive information about the intended victims” (*The Role of AI in Social Engineering, 2023*).

Data collecting becomes more effective: “Instead of laboriously searching for targets across multiple social media sites and online platforms, AI can be programmed to perform this search more efficiently. This streamlines the reconnaissance phase of social engineering attacks” (*The Role of AI in Social Engineering, 2023*). If a person's or a company's mail server is configured incorrectly or poorly secured, AI can interfere with data personalization: “AI algorithms excel at analyzing the data collected to create highly personalized phishing emails. By studying social media and other public data, AI can craft messages that appear tailored to the individual target’s interests and preferences. This personalization not only increases the chances of the victim falling for the deception but also shortens the timeline required for research and message crafting” (*The Role of AI in Social Engineering, 2023*).

HR analytics carries the risk of influencing individual decision-makers or priority statuses: “AI can identify key personnel within an organization who have access to sensitive information. By profiling an organization’s workforce and their roles, malicious actors can pinpoint individuals who may be valuable targets for their social engineering campaigns. This information can then be exploited to launch attacks specifically tailored to these employees” (*The Role of AI in Social Engineering, 2023*).

The case entitled "Simulating insider knowledge" articulates that "AI, through generative algorithms, can simulate insider knowledge. By analyzing the data collected during profiling, AI can craft emails or messages that convincingly appear to come from a colleague, family member, or trusted source within the target’s network. This tactic adds an extra layer of credibility to social engineering attempts, making them more convincing" (The Role of AI in Social Engineering, 2023). To prevent such tactics, one should pay attention to authorization algorithms and the possibility of changing the sender. Moreover, AI is capable of creating new segments of already existing data and a person does not notice a cover-up: “Data Enrichment. Once a target profile is created, generative AI can further enrich this data. It can generate plausible additional information that could be used in an attack, such as a list of likely security questions and answers based on the target’s profile. This augmented information enhances the attacker’s ability to manipulate and deceive the target effectively” (*The Role of AI in Social Engineering, 2023*).

The multi-vector nature of virtual attacks on clients should be noted.” AI’s capabilities extend beyond a single attack vector. It can seamlessly manage multiple attack vectors simultaneously, including email, voice calls, and text messages. Generative AI can coordinate these various types of attacks, enhancing the overall effectiveness of the campaign. For example, it can send a phishing email while simultaneously generating a script for a voice phishing (vishing) attack. This coordinated approach increases the chances of luring victims into the deception” (*The Role of AI in Social Engineering, 2023*).

Artificial intelligence is characterized by an important feature required by the mechanism of social engineering, Such as adaptability, changeability, flexibility of reactions. It reformats the messages in real time. “Learning algorithms enable AI to adjust its tactics based on the success or failure of previous attempts. For instance, if a target does not respond to a phishing email, the AI can swiftly generate a follow-up email with different content designed to be more enticing to the target, or leave a voicemail message. The software to generate convincing two-way conversations is already available, so leaving a voice message is far easier. This real-time adaptation makes the role of AI in attacks more agile and effective" (*The Role of AI in Social Engineering, 2023*). The more actions an intelligent system performs, the more functional it becomes. AI constantly searches for optimal algorithms of persuasion, which contributes to the formation of a certain opinion in social groups. Chatbot technologies work to create a certain ideological environment, where people are convinced not by arguments, but by emotional load, by an avalanche of messages that highlight the event in one color, in a way that is beneficial to the creators of chatbots. For example, Ukraine faced such aggressive information technologies in the war with Russia. There are groups in social networks where there are few real people, and the majority are bots that promote hostile narratives, misinformation, impose opinions and create the impression of an active discussion that does not exist in reality. People trust the social environment more than the IT. If they are sure that they are communicating with people and not machines, they are open to a sincerely contact and disclose important data and valuable information. "Therefore, they are the weakest link in the security chain. Malicious activities accomplished through human interactions influence a person psychologically to divulge confidential information or to break the security procedures. Due to these human interactions, social engineering attacks are the most powerful attacks because they threaten all systems and networks. They cannot be prevented using software or hardware solutions as long as people are not trained to prevent these attacks" (*Salahdine, Kaabouch, 2019*).

In the following example, the carelessness and gullibility of people led to the loss of 40 million dollars by The Ubiquiti Networks company. It turned out that no one had to hack operating systems and steal personal data. The safety regulations were violated by the employees themselves. The fraudsters sent an email on behalf of the company's top manager and asked financiers to transfer a large amount of money to a specified bank account. Social engineering was used to manipulate human weaknesses and the desire to serve the superiors, when employees trust the text if it is signed by the name of a senior employee and their neglect of safety regulations.

Psychologist Robert Cialdini in his work "The Psychology of Influence" (*Cialdini, 2021*) described similar case. The researchers called the nurses on behalf of the chief physician, giving orders to administer a lethal dose of medication to the patient. Of course, the nurses were aware of the consequences of this order, but in 95% of cases they followed the command without trying to confirm the doctor's identity and clarify whether the order was erroneous. At the entrance to the ward, the nurses were stopped by the authors of the study. Why did the nurses do this? They did it because of trust in authority, following orders and being obedient actors who do not think critically. The same thing happened in the story with The Ubiquiti.

The problem of social manipulation and the construction of false virtual spaces requires the production of effective tools of resistance and protection. A coalition of the most powerful AI development companies called the AI Alliance has been created to join forces in collaboration to develop protection strategies in the field of AI technologies.

The drive to provide free cutting-edge technology is embedded in the challenge of open access to the source code for artificial intelligence. Increasing the entities that provide innovative technology is an important strategy for analyzing viable tools and optimistic scenarios in the field of AI.

Latvian scientists Rudolph Kalnynš, Janis Purinš and Gundars Alksnis conducted a sociological survey of average citizens of the country to find out how much people are aware of the protection against the interference of social engineering methods in their virtual existence. 140 respondents were interviewed on Facebook and Twitter (twice as many women as men). "A survey was conducted online with the goal to determine the knowledge about network security of the public, and their attitude towards it" (*Kalniņš, Puriņš, Alksnis, 2017: 39*). Investigation of the intervention of social engineering in the communication of social networks led to the conclusion about the effectiveness of the following practices: "In social engineering, the hacker retrieves credentials and login information from the end user applying deceiving social dialog and/or messaging. Using social engineering can be the only way to hack the password in such cases, when there are not any technical vulnerabilities" (*Kalniņš, Puriņš, Alksnis, 2017: 43*). The researchers created testing conditions similar to the actions of fraudsters, although "the attack was performed as a proof of the concept of social engineering, without any malicious intent" (*Kalniņš, Puriņš, Alksnis, 2017: 43*). Riga researchers proved the validity of the hypothesis: "Hypothesis has been proven to be true – most users are not well informed about the security of wireless networks… Networks that use enterprise-grade encryption are safer, because each user has a unique user name and password (where as in the personal mode a pre-shared key is used, which is the same for all users, and there are no usernames) and an additional server needs to be set up to handle password distribution… Results of the conducted survey show that the respondents are not well informed about the security of wireless networks. More than 69 % of respondents do not even know if the WPS function is enabled or not" (*Kalniņš, Puriņš, Alksnis, 2017: 43-44*). This study correlates with Ukrainian research on this issue.

To strengthen digital security, experts suggest improving methods of identifying a person: "One path forward is to better leverage Public Key Encryption, a technology that offers more than just confidentiality; it offers the means for authentication and non-refutability that we desperately need. Here's how public key encryption answers two critical questions. Authentication: How can we be certain you are who you claim to be? Non-refutability: How can we trust that this message hasn't been tampered with?" (*The Role of AI in Social Engineering, 2023*). In addition, a digital signature proving the authenticity of the information product will become an effective tool. "News stories, clips, and podcasts come with digital signatures, which are verified automatically, displaying a badge of authenticity. This doesn't just keep content private; it certifies its authenticity, crucial in an era where AI can generate convincing forgeries" (*The Role of AI in Social Engineering, 2023*). The open key infrastructure has already been implemented in the virtual space, but it is not enough to be informed about the technology, one must agree with the necessity of its use, to be an informed user. Social engineering of educational strategies should work against social engineering of information fraud.

It would be a mistake to classify all manifestations of social engineering in the digital world as criminal phenomena. Thus, a social engineer can find out the data of an anonymous commenter or informer, insist on the removal of a negative review, slander or illegal statement, and thereby restore the company's reputation after an attack by competitors. Communication with a negative audience using social engineering methods (for example, neuro-linguistic programming techniques, audio-visual cases) encourages the public to open discussion and acceptance of arguments, changes people's opinion in a productive direction.

With the help of gadgets, every person can create a "personal universe", and artificial intelligence can become a personal assistant, a priority convenient communicator, which fulfills wishes and supports your thoughts. Are there any threats to humans in these processes? Of course, there are. But let's remember K. Jaspers, who argued that technology is not to blame for human failures, it is not the person who creates the danger, but the person who conceptualizes the technical world, constructs and develops it, and invests his meanings in technological processes. Reputational risks of social engineering by Modern theorists, ignoring effective methods of engineering in the socio-humanitarian sphere due to engineerophobia of the digital world can lead to the loss of a productive field of social research and constructive activity.

Conclusion

Social engineering is an interdisciplinary field of knowledge that offers practices of influence and regulation of relations between people and social groups on the basis of scientific and applied research and operates by means of the organization of social systems and technologies of various levels of complexity. It is necessary to distinguish fundamental scientific developments in the field of social philosophy and sociology with applied investigations of social engineering. Social engineering is guided by pragmatic goals and objectives regarding the influence and change of specific social objects or models.

Scientific and technical thinking articulates the rationalization of all spheres of human existence and the ability of engineering to cope with social challenges. It started as a resource for combating social crises, terrorism, challenges of war and migration waves. But absolute faith and trust in the rationalization of human existence has already shown its utopian nature in the concepts of Modern philosophy. Critical attitude to social engineering in the 21st century is associated with rethinking the concept of "progress" as an outdated modern project, boosted by disappointment in the possibilities of rational management of all social processes without taking into account the spontaneous nature of some practices, their unpredictable results or manipulative nature. Analysis of the concepts of the technocratic elite draws attention to the danger of using digital technologies for anti-democratic purposes. It is also related to the subjectivity that accompanies the definition of "desired goals", "beneficial interests", "normal behavior", etc. To what social class or group do these desires and interests belong? Does social engineering work for democratic change in society, or is it used by a particular group or government to further its goals? Applied efforts to find compromise solutions in social conflicts can not only limit the rights and freedoms of the parties, but also affect the interests of potential participants in social interaction as well as the latent values and needs of subjects falling into the field of social construction, and could lead to unpredictable consequences. These issues show the problematic nature of the introduction of social engineering into socio-political processes and the urgent need for further research.

Changes in the media bring the problem of media communication engineering to the foreground of the research, emphasize the importance of communication tools and PR technologies in the construction of social concepts. Understanding the problem of mass media development and their influence, including the ability of information resources to construct reality and change attitudes towards the course of socio-cultural processes, sets a new perspective in the study of social engineering. The article discusses one of the examples of a socially oriented approach to communication and information technologies, in particular, the concept of Domestication introduced by R. Silverstone, while his followers E. Hirsch, L. Haddon, K. Lacey discovered the everyday dimension of the problem, concerned about the intense influence of media communication on people, their social environment, and the family members.

With the development of virtual reality, digital space, and neural networks, the possibilities of social construction reach the level of automated systems. Applying the resources of AI to the development of social engineering, modern social designers face with the awareness of the possibilities and limitations of digital technologies in social construction. This is due to the moral assessment of intervention technologies, the choice of a solution and tools that will ensure the optimal performance of the task within legitimate limits. This not only does not simplify, but complicates the problem of the danger of social manipulation. The role of social engineering is being redefined, as well as involving people in processes of interest to the engineer, persuading the audience, controlling the intentions and actions of subjects, propaganda and manipulation for the benefit of certain social groups or individuals.

The concept of digimodernism is analyzed in this context, demonstrating how the processes of digitalization of social life, in particular, the introduction of AI into the cultural fabric of social processes, change the logic of perceiving the real world as a space of endless narratives. The hegemony of digital technologies mixes public and private space, deprives us of security, but at the same time accustoms us to openness and transparency. The revolutionary technologies of recent years force us to look in a new way at the possibility of constructing social interactions and the danger of imitating them with technical devices. The anthropomorphism of these systems causes unreasonable trust, often deprives a person of prudence and caution in providing information.

The content analysis of modern Internet resources made it possible to generalize about the forms of manipulation, disorientation, and deception of users of digital technologies by methods of social engineering. The conducted research showed that the use of AI in the methodologies and practices of social engineering could be dangerous and could threat to violate the privacy of a person, manipulating the opinion of social subjects of various levels. In this process, reliable antivirus programs and the powerful work of firewalls could not provide a reliable protection and filter all potentially threatening and harmful content. The insufficient level of digital competence of active Internet users while surfing social networks and chats that use AI technologies was noted. It is necessary to increase the level of knowledge, awareness, and competence of internet users.

We can no longer avoid the rapid development of technology is the current reality, but must accept and adapt to it. The techniques of social engineering and manipulation of public opinion are being improved, which encourage the reorientation of our knowledge, the training of algorithmic thinking, the formulation of urgent tasks and the search for new means of protection against its dangers. Algorithms for protection in the digital environment include various options for security policy, training users, improving information and digital competence, establishing clear instructions and rules for using devices (personal or corporate computer, smartphone, etc.), creating warning systems about possible threats, forming professional and expert groups responsible for technical support, organization of multi-level verification.

The phenomenon of social construction testifies not only to the processes of self-reproduction, autopoiesis in society, but also requires our self-reflection regarding the rules and caveats that need to be produced and made public so that the methods of social engineering do not compromise people's expression of will, their freedom of action, but work for the benefit of human needs. There is no universal recipe for protecting society from manipulative influences. The implementation of the principles and methods of social engineering requires developed critical rethinking, the creation of socially friendly models taking into account the experience of digital transformations and the discursive space of information technologies.

REFERENCES

Arqoub, Omar Ahmad Abu, Özad, Bahire Efe, Elega, Adeola Abdulateef (2019). The Engineering of Consent: A State-of-the-Art Review. *Public Relations Review,* 45(5). https://doi.org/10.1016/j.pubrev.2019.-101830.

Cialdini, Robert B. (2021). *Influence, New and Expanded: The Psychology of Persuasion*. Harper Business. 592 p.

Gehl, Robert & Lawson. Sean.(2022, Jun, 29). Masters of Crowds: The Rise of Mass Social Engineering. *The MIT Press*. Posted on, 2022. https://thereader.mitpress.mit.edu/masters-of-crowds-the-rise-of-mass-social-engineering/

Haddon, L. (2011). Domestication Analysis, Objects of Study, and the Centrality of Technologies in Everyday Life. *Canadian Journal of Communication*. 36, 311-323. https://doi.org/10.22230/cjc.2011v36n2a2322 .

Kalniņš, R., Puriņš, J., Alksnis, G. (2017). Security Evaluation of Wireless Network Access Points. *Applied Computer Systems*, 21, 38–45. https://www.researchgate.net/publication/318180928_Security_Evaluation_of_Wireless_Network_Access_Points#fullTextFileContent. DOI: 10.1515/acss-2017-0005

Kirby, A. (2009). *Digimodernism: How New Technologies Dismantle the Postmodern and Reconfigure Our Culture*. Continuum. 288 p.

Kolinko, M. (2018). Metodolohichnyy potentsial kontseptsiyi domestykatsiyi. *Skhid,* 5 (157), 47-51 https://doi.org/10.21847/1728-9343.2018.5(157).148996 (In Ukrainian).

Kolinko, M. (2019). *Mizhkulturna komunikatsiya: topolohichnyy vymir*. Vinnytsya, TVORY Ltd. (In Ukrainian).

Kolinko, M. (2023). P'yatnadtsyatykhvylynne misto»: politsentrychna struktura suchasnoho mehapolisu. Kyyivs'ki filosofs'ki studiyi-2023: Conference Papers. Kyiv, Borys Grinchenko Kyiv University, pp. 39-43. https://fshn.kubg.edu.ua-/images/stories/Departaments/kaf_f/KFS-2023/%D0%B7%D0%B1%D1-%96%D1%80%D0%BA%D0%B0_%D0%9A%D0%A4%D0%A1-23.pdf (In Ukrainian).

Kolinko, M., Petryshyn, H. (2022). Simulacra and fakes in the information warfare. *Skhid*, 3 (3), 9-14 https://doi.org/10.21847/1728-9343.2022.3(3).266049 (In Ukrainian).

The Role of AI in Social Engineering. (2023, November, 8). *Website "zveloLIVE".* URL: https://zvelo.com/the-role-of-ai-in-social-engineering/.

Salahdine, F., Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11 (89), 1-17. https://doi.org/10.3390/fi11040089.

Shirodkar, N. (2023, November, 26). "Social engineering" experiments in full swing in Bihar in run-up to 2024. PUNE.NEWS. https://pune.news/nation/social-engineering-experiments-in-full-swing-in-bihar-in-run-up-to-2024-94072/.

Turner, S. (2022). Digital affordances and the liminal. In «The Technologisation of the Social A Political Anthropology of the Digital Machine». P. 98-111. https://doi.org/10.4324/9781003052678-6

Реактуалізація проблеми соціальної інженерії і цифрова безпека

Марина Колінько (ORCID 0000-0002-1043-2742)
Київський столичний університет імені Бориса Грінченка (Україна)

Галина Петришин (ORCID 0000-0003-3428-8789)
Тернопільський національний педагогічний університет
імені Володимира Гнатюка (Україна)

Галина Чумак (ORCID 0000-0001-5974-9022)
Тернопільський національний педагогічний університет
імені Володимира Гнатюка (Україна)

Статтю присвячено актуальним аспектам соціального конструктивізму в цифрову добу. Соціальна інженерія розглядається як стратегічна технологія конструювання нових смислів, принципів, правил і фактів соціальної взаємодії. Показано застосування історико-філософських інтелектуальних конструктів до практик соціальних перетворень. Проаналізовано соціально-філософські концепції К. Поппера, П. Сорокіна, Р. Сілверстоуна в контексті конструктивних пропозицій соціальної інженерії. Різноманітність поглядів на сутність соціальної інженерії та аналіз сфер її застосування проблематизують інтерпретацію її суспільної ролі і значення. Розкрито можливості та обмеження цифрових технологій у соціальній інженерії. В межах проблеми цифрової безпеки показано ризики створення нових інструментів і алгоритмів маніпуляцій, дезорієнтації користувачів віртуальних технологій методами соціальної інженерії. Методи конструювання соціальних подій і втручання в життя людей потребують критичної оцінки. Впровадження можливостей штучного інтелекту у соціоінженерні розробки призводить до нових ризиків, які систематизовано у науковій статті. Вони пов'язані з маніпуляціями суспільною свідомістю, спотворенням способів ідентифікації, персоналізації, фінансовим шахрайством, порушенням гуманітарної безпеки.

Ключові слова: штучний інтелект, лімінальність, соціальна інженерія, цифрова безпека, соціальне конструювання, віртуальна реальність

Received (Надійшла до редакції): 19.12.2023,
Accepted (Прийнята до друку): 1.02.2024
Available online (Опубліковано онлайн) 30.04.2024