DOI 10.14746/ssp.2021.4.1

Oleksandr Trukhachov[1]
University "KROK" of Kyiv
ORCID ID: 0000-0001-6868-3328

Elements of Social Engineering Methodology Used During the COVID-19 Pandemic

Abstract: The article focuses on elements of social engineering (SI) that could be used by the states in their own interests during the COVID-19 pandemic. These elements were used to form negative public opinion, change the political landscape, and reduce citizens' trust in their own governments. These elements are influence and persuasion. Traditional media and social networks play a major role in the use of these SI elements. SI has a long history of theoretical study as a scientific phenomenon. Practical elements of SI have a large arsenal, from government tools to influencing individuals. The article aims to demonstrate using SI elements, influence, and persuasion by the interested states and governments to obtain certain preferences for both foreign and domestic policies.

Key words: social engineering, information and computer technology, COVID-19 pandemic, influence, persuasion of traditional media, social networks, media exploitation

During the COVID-19 pandemic, the EU faced strong information pressure from some states and governments. The purpose was to weaken the internal ties inside the EU using the social engineering methodology. This article focuses on some elements of social engineering (SI) that, in cooperation with other mass communication technologies, could be used by individual states in their own interests. The article's tasks are: first, to describe approaches to understanding SI based on available sources, and describe the SI elements used during the pandemic. Then, it notes the results and reaction of the ES to the current situation in the framework of the pandemic. The article uses data from the EEAS SPECIAL REPORT (made by EEAS Strategic Communications and Information

[1] PhD (political sciences), Associate professor, Department of International Relations and Journalism, «KROK» University, 30-32 Tabirna St., 03113, Kyiv, Ukraine, Email: AlexanderT@krok.edu.ua.

Analysis Division) posted on the online platform EUvsDiSiNFO. Two reports from 19.03.2020 and 02.04.2020 are considered and analyzed. Relevant data from monitoring narratives and misinformation for the period are studied. The criteria for the analysis are the availability of SI methods and techniques and the known results of their use.

In literature, the unambiguous use of the term social engineering is theoretically debatable. Today, it does not have one specific designation. The sphere of modern theoretical research of SI can be traced from the works of K. Popper on the structure of social systems to the modern provisions of information and computer technologies (ICT). At the same time, the communicative component is highlighted in the approaches to understanding SI explicitly or implicitly.

One of the first uses of the term social engineering (SI) can be attributed to the monograph of the American author W. H. Tolman *Social engineering* (1909). The author pointed out: “In my studies of social and industrial problems during the last fifteen years, I was impressed with the extent and the variety of efforts that were being made to promote better relations between capital and labor. At first, there was no name for this kind of work. In 1898, for lack of a better term, I called it industrial betterment, a phrase which passed quickly into current use and literature… There is an increasing number of industrialists who are desirous of promoting mutuality in their business. ‘Social Engineering’ will serve as a handbook of suggestion and guidance for the practical application of the experience of others” (Tolman, 1909, p. vi). This interpretation of the SI differs from all subsequent ones.

Hereafter, the development of SI understanding in the modern context was greatly influenced by the research of K. Popper. In his work *The open society and its enemies* (1966), K. Popper outlined the understanding of SI as “principles of democratic reconstruction of society – principles that I call ‘social engineering of private (piecemeal) solutions’ or, equivalently, technology of gradual social transformation ‘as opposed to’ utopian (Utopean) social engineering” (Popper, 1966, p. 30). In it, Popper identifies two main SI methods – “utopian engineering” and “piecemeal engineering,” which are designated by him as, “The utopian approach can be described as follows. Every rational action has a specific purpose. Action is rational to the extent that the goal is achieved consciously and consistently, and the chosen means must be consistent with this goal. If we want to act rationally, we must first choose a goal” (Popper, 1966, p. 199), and further, “gradual, sequential or phased engineering. This approach seems

to me to be methodologically flawless… an adherent of phased engineering will develop methods for finding the most severe, unbearable social ills, to fight them, and not to seek the greatest ultimate good, seeking to bring it to life” (Popper, 1966, p. 200).

The development of computer, information, and communication technologies (ICT) at the end of the 20th and beginning of the 21st century influenced understanding and using SI methods. SI has received a new interpretation and, accordingly, a new practical application. It led to the formation of new methods and the emergence/use of other SI elements.

In his research *Hacking the Human. Social Engineering Techniques and Security Countermeasures* (2008), I. Mann noted that social engineering could be defined as “to manipulate people, by deception, into giving out information, or performing an action.” His definition captures the distinctive aspects of targeting people and their manipulation, combined with the two main outcomes – direct loss of information and the achievement of some action desired by the attacker (Mann, 2008, p. 11).

Chr. Hadnagy gives another SI meaning in *Social Engineering: The Art of Human Hacking* (2011): “social engineering is the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives… This definition broadens the horizons of social engineers everywhere. Social engineering is used in everyday life in the way children get their parents to give in to their demands. It is used in the way teachers interact with their students, in the way doctors, lawyers, or psychologists obtain information from their patients or clients. It is used in law enforcement, and in dating – it is truly used in every human interaction from babies to politicians and everyone in between. I like to take that definition a step further and say that a true definition of social engineering is the act of manipulating a person to take an action that may or may not be in the ‘target’s’ best interest. This may include obtaining information, gaining access, or getting the target to take certain action… Social engineering is not just one action, but a collection of the skills mentioned in the framework that when put together make up the action, the skill, and the science I call social engineering” (Hadnagy, 2011, p. 7). Ch. Hadnagy presented a more specific approach to SI designation in *Unmasking the Social Engineer: The Human Element of Security* (2014), in which the influence of communication theories is traced: “…social engineering as any act that influences someone to take an action that may or may not be in his or her best interest… Social engineering in its malicious form is usually categorized into three different areas… at each: phishing, phone

elicitation, and impersonation” (Hadnagy, 2014, p. 25). Here it can be noted that the cited quotation makes it possible to adopt the provisions on the use of SI at the national and individual levels. Therefore, the method (and level) of SI became one of the main ones used during the pandemic.

In this regard, one should pay attention to the remark of G. Pocheptsov in *(Des) information* (2020). Based on the communicative component of SI, Pocheptsov argued: “A person does not react well to what can be described as tough management, when he is forced to do something. Greater success is brought by soft (really invisible) control, because in this case there is no one to resist: as if both the object and the subject of control are absent.” Leant on this, Pocheptsov gives examples of influence (soft control): “An interesting variant of covert governance is what Jacques Ellul designated as sociological propaganda… If the propaganda we are accustomed to, in its terminology – political, goes from top to bottom, then sociological propaganda is horizontal, this is the influence of what a person sees with his own eyes around him. It turns out that political propaganda works with virtual objects, and they, in fact, can go as far as they like from reality, replacing it; meanwhile, sociological propaganda works with ‘living’ objects, only with reality, for this reason it is interpreted by the consumer as reliable” (Pocheptsov, 2020, pp. 17, 83–84).

It leads to the following intermediate conclusions. SI is an actively researched theoretical and practical area. Each researcher interprets this phenomenon in his own way, dependently on scientific interests. If Popper recognized the basic elements of SI – state, goal, methods, result, then SI expands to the following – the state (government) goal, result, method, individual from the point of view of ITC, in subsequent approaches. New elements are introduced, such as phishing, phone elicitation, impersonation, influence, persuasion, and manipulation. It should be highlighted that the SI is aimed at changes in the state. SI uses a certain methodology to achieve the set goals and desired results.

The COVID-19 pandemic developed mainly in two waves. The first wave was from mid-March to mid-May 2020, and the second wave was from January to 2021. SI methods and tools were used at each stage of the pandemic.

During the pandemic, a new phenomenon appeared in the world, European information, and political sphere. We understand it as the sum of information, communication links, processes between state, political actors, the system of traditional media, social networks, and societies.

It was introduced by the World Health Organization – infodemic (pun from English infodemic = information + pandemic). The term denotes the transfer of fake information, disinformation, and information beneficial to the state that produced it to large communities. Traditional media and social networks have become the main instruments of this phenomenon. It allows a discussion on the exploitation of media and social networks as the main tools of the modern SI methodology. In this paper, the term “exploitation” is interpreted according to the Oxford dictionary as exploiting a situation in which somebody unfairly treats somebody else, especially to make money from their work (*Oxford learners dictionaries*). The chosen term is used because, in this case, to obtain the greatest benefit in the world and European politics, exploit 1) the principles of a democratic press and its foundations, and 2) the level of public confidence in traditional mass media. In other words, the identified principles maximize benefits by promoting individual narratives for the benefit of a third of countries. That is, obtaining the expected result in the form of the greatest benefit through the promotion of prepared narratives in the information space to change public opinion in the EU countries. The scope of these narratives ranges from attempts to impose a point of view about the EU’s weakness in the fight against the pandemic to attempts to lift sanctions on the Russian Federation (RF) and change the EU’s policy toward the Eastern Partnership states. According to two special reports – *EEAS SPECIAL REPORT Disinformation on the coronavirus – short assessment of the information environment EU* dated March 19, 2020, and *EEAS SPECIAL REPORT UPDATE: short assessment of narratives and disinformation around of the COVID-19/CORONAVIRUS PANDEMIC* of April 24, 2020 on the EUvsDiSiNFO website (https://euvsdisinfo.eu) – the disinformation and negative narratives are stated in the EU information sphere. In the preamble to the report *Disinformation on the coronavirus – short assessment of the information environment EU* one can read: “While disinformation includes the inadvertent dissemination of false information, disinformation campaigns involve the deliberate production and/or distribution of authentically false content disseminated for political or financial reasons.” The task of these narratives is to change the point of view and/or push the citizens of the EU countries to make false decisions (EEAS SPECIAL REPORT 19.03.2020). Here are some examples and recorded false information materials:

– The coronavirus is a biological weapon deployed alternatively by China, the US, the UK, or even Russia (to destroy the EU and NATO);

– The coronavirus did not break out in Wuhan, China – the US is concealing its true origin, which is, in fact, the US or US-owned laboratories across the world;
– The EU is not ready to provide urgent support to its Member States – instead, they have to rely on external support (e.g., Italy), with China mentioned most often as the source of such assistance;
– China is coming to rescue the EU as Brussels abandons EU Member States (EEAS SPECIAL REPORT, 19.03.2020).

Here are excerpts from the EEAS SPECIAL REPORT UPDATE: short assessment of narratives and disinformation around of the COVID-19/ CORONAVIRUS PANDEMIC of April 24, 2020, “Despite their potentially grave impact on public health, official and state-backed sources from various governments, including Russia and – to a lesser extent – China, have continued to widely target conspiracy narratives and disinformation both at public audiences in the EU and the wider neighborhood” [*EEAS SPECIAL REPORT UPDATE* of April 24, 2020]. The quotations demonstrate the identified focus on building a certain (negative) response to the actions of the ES in the fight against the pandemic. Also, their focus and number indicate planned acts, the results of which are interesting for some states/governments.

Based on the mentioned approaches to SI, one can note that researchers provide many constituent methodological elements of SI. As Chris Hadnagy (2011) argued, there are separate “social engineers:” hackers, spies, and governments. Characterizing a government as a social engineer, Hadnagy Chr. (2011) notes, “Governments: Not often looked at as social engineers, governments utilize social engineering to control the messages they release as well as the people they govern. Many governments utilize social proof, authority, and scarcity to make sure their subjects are in control. This type of social engineering is not always negative, because some of the messages governments relays are for the good of the people and using certain elements of social engineering can make the message more appealing and more widely accepted” (Hadnagy, 2011, p. 45). We add that Popper also spoke about the main role of the state in social engineering. Governments, like social engineers, use the following elements such as “influence and the art of persuasion is the process of getting someone else to want to do, react, think, or believe in the way you want them to” (ibid.).

To illustrate this point, we should follow the example: “During December 2020 and the first quarter of 2021, the Russian campaign to pro-

mote the Sputnik V vaccine has accelerated and developed into a *whole-of-government approach* including state authorities, state companies and state mass media in almost daily interventions. Russian officials not only promote the Sputnik V vaccine but also engage in antagonistic messaging, using disinformation to accuse the West and the EU of sabotaging the Russian vaccine” (*EEAS SPECIAL REPORT UPDATE April 24, 2020*) or “President Putin appearing regularly in state media reports promoting Sputnik V and commenting on western vaccines recently, in his State of the Union” (ibid.). The result of these efforts was the consent of some states, like members of the EC (Czech Republic, Hungary, Slovenia) and non-members of the Commonwealth (Moldova, Belarus), to allow the Sputnik V vaccine for being used in their territories.

Thus, we can draw the following intermediate conclusion: traditional media are actively exploited in SI to disseminate the necessary narratives and form given points of view, which can be converted into practical components to gain benefits.

As noted, in the modern approach to SI, the use of ITC was indicated. This approach is driven by the social engineering’s task to influence individual thinking. Therefore, using social networks in SI provides an opportunity to address the individual directly and anonymously. In this methodology, widespread social networks play a special role, primarily Facebook, Twitter, etc.

J. Willemo noted: “Malign actors are able to hide behind anonymous social media accounts, pages, or groups, exploiting a system designed to protect privacy rights. Much of the news we now consume is being promoted without source attribution and without advertising transparency. This provides many opportunities for malign actors to target unsuspecting audiences with disinformation and other forms of information activities without users ever knowing about it… These are the broader vulnerabilities that enable the abuse of the online information environment through which malign actors can manipulate public opinion, trick people, and undermine trust in society. Other vulnerabilities, such as lack of training and education, and trust in media and governmental actors, are contextual and vary from nation to nation. The malicious use of social media is not merely a question of abuse of the terms and policies of the social media platforms; it is as much a question of abuse of the human mind and the fundamental tenets on which our democratic societies are based” (Willemo, 2019).

It should also be noted that popular social networks do not fully control their users’ content. As a result, it is possible to use the SI for the

interested actors. This problem is indicated in the Report *How Facebook can Flatten the Curve of the Coronavirus Infodemic* (Avaaz, 2020). “Facebook’s reluctance to retroactively notify and provide corrections to every user exposed to harmful misinformation about the coronavirus is threatening efforts to ‘flatten the curve’ across the world and could potentially put lives at risk” (Avaaz, 2020).

A separate component of modern SI is hacking and planned cyberattacks. These elements are used to form negative attitudes toward governments and state institutions and attempts to break their activities.

European Medical Agency (EMA) said that the “ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines have been leaked on the internet. This included internal/confidential e-mail correspondence dating from November, relating to evaluation processes for COVID-19 vaccines. Some of the correspondence has been manipulated by the perpetrators prior to publication in a way which could undermine trust in vaccines… Dutch media involve Chinese and Russian hackers in attack on EMA” (EMA, 2020).

Thus, we can note that the use of ICT, particularly popular social networks in modern SI methodology, is aimed at changing the thinking of individuals and their influence on decision-making. Another approach to using ICT in SI is cyberattacks and hacking, which aim to damage a reputation and undermine trust. To illustrate, we give an example of practical cooperative use of modern SI methodology, which included such components as – traditional media, social networks, and speeches of interested actors. The main elements were influence and persuasion by broadcasting the necessary information in the media and social networks. As a clear example, consider the Russian Federation’s “humanitarian aid” for Italy in March 2020.

The authors of the SI Act tried to take advantage of the situation that developed during the beginning of the COVID-19 epidemic in the EU. The form was chosen for the performance “humanitarian mission.” The action was held using the SI methodology with the support of mass communication and information technologies: PR technology, influence, disinformation, and propaganda. The action was carried out as follows: fourteen planes of the RF Ministry of Defense delivered “humanitarian cargo,” which turned into a whole PR campaign. Russian military trucks drove half of the country to deliver aid from Rome to the north. The action took place against the background of increasing information pressure. Sputnik Italia was involved, managing misinformation and publish-

ing news about the action, which had three million reactions on Twitter. Moreover, e-mails were sent to Russian-speaking citizens of the EU, describing “assistance from the Russian Federation.” Further, in early May, the Italian media “Linkiesta” published a letter from the chairman of the international affairs committee of the Russian Dumaw Leonid Slutsky, which the Russian ambassador to Italy addressed to Slutsky’s counterpart in the Senate, Vito Petrocelli. The letter does not mention the humanitarian aid that Russia has provided to Italy. The Italian newspaper explains the Russian appeal precisely as a demand to “pay for the support,” nevertheless. The result of this act of the SI can be considered a decrease in the Italians’ trust in the EU and its internal politics. According to the “Demopolis” organization, trust in the EU among already skeptical Italians in April 2020 fell to 27%, compared with 42% in January (over the past ten years, a low level of trust, according to Eurobarometer, was recorded only in 2013 – then it was 24%). Italians were so disappointed in the EU that the number of those who would be ready to vote to leave the European Union (by analogy – Italexit) is almost equal to those who would vote to stay (42% versus 44%, according to the Tecnè Institute). Moreover, according to the SWG survey, 52% of Italians consider China their friend (which is 42% more than in 2019), and 32% – Russia. As for the enemies, in the minds of 45% of the Italian public, the enemy no. 1 is Germany, which has admitted to the treatment of fifty Italian patients with coronavirus [Zarembo K. 2020].

The former prime minister of Italy, Enrico Letta, said in an interview for the “Guardian”: “We are facing a crisis that is different from previous crises,” partly because of the unpredictable progression of the virus, and partly because “Europeanism” has been weakened by other crises of the past decade. The communitarian spirit of Europe is weaker today than 10 years ago,” he said, adding that the biggest danger for the EU was “the Trump virus.” If everyone takes the strategy of “Italy first,” “Belgium first,” or “Germany first,” he said, “we will all sink altogether” (The Guardian, 2020).

The information is marked by the formation using the SI methodology of destabilizing factors in information security, which could affect the internal structure of the EU, especially integrity.

SI methodology and the rest of methods set against the EU did not go unnoticed by top officials of the European Union. It was stated very specifically by the High Representative of the EU Joseph Borrell, in Declaration… *on behalf of the European Union, on malicious cyber activities*

exploiting the coronavirus pandemic (30.04.2020), “as the coronavirus pandemic spreads around the world, the European Union and its Member States have observed cyber threats and malicious cyber activities targeting essential operators in Member States and their international partners, including in the healthcare sector. Since the pandemic’s beginning, significant phishing and malware distribution campaigns, scanning activities and distributed denial-of-service (DDoS) attacks have been detected, some affecting critical infrastructures that are essential to managing this crisis. The European Union and its Member States condemn this malicious behavior in cyberspace, express solidarity with all countries that are victims of malicious cyber activities and underline their continued support to increase global cyber resilience” (European Council, 30.04.2020).

Confirmation of the signs of exploitation of traditional and social media for the application of the SI methodology was the *Joint Statement by the Ministers of Foreign Affairs of France, the Netherlands, the United Kingdom and Germany on the Occasion of World Press Freedom Day* (May 3, 2020), in which it was said, “A free press is crucial for a comprehensive response to the ongoing COVID-19 pandemic. We must oppose all attempts by any state to use the pandemic to adopt restrictions on press freedom, silence debate, abuse journalists or spread misinformation. It is deeply concerning to see that across the world, publications are contracting and closing, and journalists being made redundant because of falling revenues. Especially in these times, we depend on independent, fact-based and reliable journalism. A free press is crucial for a comprehensive response to the ongoing COVID-19 pandemic. Only by keeping the public informed can we prevent a further spread of COVID-19” (Statement on the Occasion of the World Press Freedom Day, 3.05.2020).

It makes it possible to conclude that the EU member states’ governments and the Commonwealth governing bodies understand the danger of using the SI methodology against them. There is no direct evidence confirmed by scientific methods (sociological survey) of the impact of the considered efforts for today. Nevertheless, the existence of the narratives themselves is a fact, and we cannot deny their presence in the information and communication of European politics. The construction of the Commonwealth’s defensive line was a reaction to the unfriendly SI activities of some states. Emphasis should be placed on using the SI methodology by the Commonwealth as a means of countering threats. First of all, there are elements of SI – influence and the art of persuasion. They should be used to explain the actions of EU institutions, to inform the public about

the progress of the pandemic. As an example of the use of TIC, let us pay attention to the launch and operation of the European information resource EUvsDiSiNFO (https://euvsdisinfo.eu/), which constantly refutes false narratives and fake news. The result of these efforts is a growing number of EU citizens who understand and accept the main settings for victory over pandemics. Among them, the basic norms are quarantine and vaccination.

In opposition to unfriendly states and the response to their negative use of SI against the EU, the following provisions may arise: 1) a clear and open system of communication between EU member states, 2) interaction between the EU and the states within the Eastern Partnership project, 3) internal communication between the state and the citizen based on truthful and wide information on pandemic measures. It will help overcome the destabilizing factors caused by the COVID-19 pandemic and its accompanying infodemia and vaccinophobia.

To predict that as the effectiveness of pandemic control increases in the EU and the rest of the world, the use of SI methodology and related technologies by some countries and governments will increase the negative perception of EU citizens of the actions of their governments in combating the pandemic.

Conclusion

We note that during the pandemic, some states (Russia, China, and others) used elements of SI to organize the impact on both individuals and governments of EU member states.

The modern approach to the understanding and specific designation of SI is debatable. At the same time, the modern understanding of SI includes several general provisions presented by different authors, including the following: a purpose, a manipulation, an influence, a persuasion, the motivation to perform certain actions, change of thinking, changes in politics, economics, military affairs. In this context, the modern understanding of SI can be considered a set of methods and technologies subordinated to one goal and aimed at obtaining a given result.

The main tools of modern SI are traditional media and social networks, making it possible to reach the widest audience. Traditional media are actively exploited in SI to disseminate and construct the necessary narratives, the formation of given points of view, which are converted into productive activities. The use of ICT and popular social networks in

modern SI methodology is aimed at changing the thinking of individuals and influencing their decision-making. Another approach to the use of ICT in SI is the organization of cyberattacks and hacking to damage the reputation and reduce trust in government institutions. Destabilizing factors have become the result of the use of SI during the period of pandemics. The narratives formed within the framework of the influence were aimed at creating negative perceptions of the actions of states, members of governments, and political movements of the EU and their partners.

With the increasing effectiveness of the fight against the pandemic in the EC member states and the rest of the world, the use of the SI methodology and related technologies will be intensified by some countries and governments to enhance the negative perception by citizens and governments of individual countries – members of the EC of the complex to combat the pandemic.

An effective response to the use of SI is the constant analysis of disinformation and fake news, the constant attraction of the attention of the mass audience to acts of disinformation. And the construction of our own SI methodology aimed at explaining the directions for overcoming the crisis, which gives the general public an understanding of the real picture of confronting the pandemic.

Bibliography

EEAS SPECIAL REPORT: *Disinformation on the coronavirus – short assessment of the information environment EU*, EUvsDiSiNFO, March 19, 2020, https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-informationenvironment/?highlight=01%D0%BC%D0%B0%D1%80%D1%82%202020, 15.05.2021.

EEAS SPECIAL REPORT UPDATE: *Short assessment of narratives and disinformation around of the COVID-19/CORONAVIRUS PANDEMIC*, EUvsDiSiNFO, update 2–22 aprile, https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/?highlight=01%D0%BC%D0%B0%D1%80%D1%82%202020, 21.05.2021.

European Council *Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic*, 30.04.2020, https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/, 01.05.2021.

European Medical Agency (EMA) Cyberattack on EMA, update 5 News 15.01.2021, https://www.ema.europa.eu/en/news/cyberattack-ema-update-5, 22.05.2021.

Exploitation. Mind. Oxford learners’ dictionaries, https://www.oxfordlearnersdictionaries.com/definition/english/exploitation?q=exploitation, 20.06. 2021.

Guardian *Coronavirus could be final straw for EU, European experts warn*, https://www.theguardian.com/world/2020/apr/01/coronavirus-could-be-final-straw-for-eu-european-experts-warn01.04.2020, 31.05.2021.

How Facebook can Flatten the Curve of the Coronavirus Infodemic, Study indicates Facebook is rife with bogus cures and conspiracy theories that remain on the platform long enough to put millions of people at risk, AVAAZ, April 15, 2020, https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/, 23.05.2021.

Mann I. (2008), *Hacking the Human. Social Engineering Techniques and Security Countermeasures*.

Hadnagy Chr. (2011), *Social Engineering: The Art of Human Hacking*, Indianapolis.

Hadnagy Chr. (2014), *Unmasking the Social Engineer: The Human Element of Security*, Indianapolis.

Oxford learners’ dictionaries. Meaning of *exploitation*, https://www.oxfordlearnersdictionaries.com/definition/english/exploitation?q=exploitation, 20.06.2021.

Pocheptsov H. (2019), *(Des) information*, Kyiv.

Popper C. (1966) *The open society and its enemies*, vol, 1 THE SPELL OF PLATO, London–Henley.

Persuasion, Mind, *Oxford learners dictionaries*, https://www.oxfordlearnersdictionaries.com/definition/english/persuasion_1?q=persuasion, 20.06.2021.

Statement on the Occasion of the World Press Freedom Day, Federal Foreign Office, 3.05.2020, https://www.auswaertiges-amt.de/en/newsroom/news/world-press-freedom-day/2338390.

Tolman H. W. (1909), *Social engineering*, New York.

Willemo J., *Trends and Developments in the Malicious Use of Social Media* (StratComCo), 19th August 2019, https://stratcomcoe.org/publications/trends-and-developments-in-the-malicious-use-of-social-media/81, 15.05.2021.

Zarembo K., *Life after the disaster: how the pandemic changed the political mood of Italians*, “Evropeyskay Pravda”, 13.05.2020, https://www.eurointegration.com.ua/rus/articles/2020/05/13/7109708/, 24.05.2021.

Elementy metodologii inżynierii społecznej stosowane podczas pandemii COVID-19

Streszczenie

Artykuł koncentruje się na elementach inżynierii społecznej (SI) wykorzystywanych przez poszczególne państwa we własnym interesie podczas pandemii COVID-19. Elementy te wykorzystano do kształtowania negatywnej opinii publicz-

nej, zmiany krajobrazu politycznego i zmniejszenia zaufania obywateli do własnych rządów. Zaliczają się do nich wpływ i perswazja. Tradycyjne media i sieci społecznościowe odgrywają główną rolę w wykorzystaniu tych elementów SI. SI ma długą historię studiów teoretycznych jako zjawiska naukowego. Praktyczne elementy SI mają duży arsenał, od narzędzi rządowych po metody wpływania na jednostki. Celem artykułu jest wykazanie wykorzystania elementów SI, wpływu i perswazji przez zainteresowane państwa i rządy w celu uzyskania określonych preferencji zarówno dla polityki zagranicznej, jak i wewnętrznej.

Słowa kluczowe: socjotechnika, technologia informatyczna i komputerowa, pandemia COVID-19, wpływ, perswazja mediów tradycyjnych, sieci społecznościowe, eksploatacja mediów

Article submitted: 05.11.2021; article accepted: 08.12.2021.