Oksana Evsyukova*

Political digitalization for Ukrainian society – challenges for cybersecurity

Abstract

The article describes the stage of political digitalization of Ukrainian society, defined as a gradual multi-vector process of society's transition to digital technologies, affecting all spheres of public life, including public policy and public administration. The peculiarities of digital transformation in Ukraine are determined in the context of service state formation. The issue of cyber-security is studied. The public policy against cyber-terrorism in Ukraine is analysed. The main components of cyber-terrorism in Ukraine, related to the development of political digitalization of society, are identified and characterized, including: informational-psychological terrorism, informational-technical terrorism, cognitive terrorism, network terrorism, social-communication terrorism.

Key words: cyber-security, cyber-threats, cyber-terrorism, service state, digital transformations, political digitalization, society

* Oksana Evsyukova: Doctor of Science in Public Administration, Associate Professor, Associate Professor of the Department for Public Governance and Public Service, National Academy of Public Administration under the President of Ukraine, Ukraine, e–mail: oksana_evsyukova@yahoo.com, ORCID: 0000–0002–1299–69–55.

The stage of political digitalization of society began in Ukraine after the presidential and parliamentary elections in 2019 and it continues to this day.

Let us note that the reason to determine such stage is that modern digital technologies are changing work of government agencies and relationships between them in the social and value context. In today's informational society, digital transformations have affected cooperation between citizens and public authorities, citizens' behaviour, including political aspects (citizens receive various forms of access to political, state information, opportunities for interaction, such as creating and sharing political knowledge, skills and abilities). Thus, political digitalization of society is a gradual multi-vector process of society's transition to digital technologies, which affects all areas of public life, including public policy and public administration.

These changes are especially important in the context of service state formation in Ukraine, which, in turn, is a product of developed digital transformations.

What are the realities that confirm existing political digitalization of Ukrainian society? First of all, the President of Ukraine V. Zelensky received the support of the majority of Ukrainian citizens through the introduction of digital political technologies. Whether it is good or bad, each of us has own subjective beliefs.

It is worth mentioning certain circumstances that determine the stage of political digitalization of society in Ukraine. Today, Ukraine ranks 46th out of 193 countries in the UN e-participation ranking[1].

First, we should note that President of Ukraine V. Zelensky outlined the digitalization directions in Ukraine at the Ukrainian Forum of Netizens "iForum 2019" in May 2019: "Information about the state, communications with the state, transactions with the state, involvement in the government of the state"[2]. Secondly, the Ministry of Digital Transformation (MinDigit) is quite active in Ukraine and implements the President's initiative – "the state in a smartphone" project, which combines a mobile application and a portal of public services[3]. To implement this project, the MinDigit is already implementing a set of digital projects (Portal of public services and the application "Diia (Action)",

1 Informational materials from the website of the UN Office in Ukraine, http://www.un.org.ua/ua /.

2 Ukrainian Forum of Netizens "iForum 2019", https://2019.iforum.ua/.

3 E. Shishatsky, S. Yurasov, *Digital strategy of V.Zelensky: there is a criminal behind each register*, https://tech.liga.net/technology/interview/didjital–strateg–zelenskogo8.

Digital Education, BroadBand, e-Residence, e-Baby, etc.). The main areas of MinDigit work are the online provision of Ukrainian citizens with high-quality and affordable public services; proper use of high-speed Internet on all international highways and in all settlements; formation and acquisition of digital skills and competencies by Ukrainians; development and support of the IT industry[4]. An important task of the MinDigit today is the interaction of various registers. This agency together with other state authorities, public bodies and international partners works to ensure interoperability – the principle when different informational resources can interact with each other on the basis of unified interfaces and protocols[5]. Third, the following leading digitization technologies are used in the public sector to implement public services: multi-channel information and involvement of citizens (especially via social networks – Facebook, Twitter, Telegram) into communications and active political discussions; citizens can have opportunities to determine the conditions of their participation in the relevant processes, etc.; open data (accessible through open software interfaces so that information availability and dissemination meet citizens' needs); enhanced electronic identification of citizens (permanent authorization for each entry into a public authority's online system to confirm their identity and, consequently, unimpeded access to the requested data); comprehensive analytics (a dynamic ongoing process collecting and analyzing political information needed to obtain a sound and structured knowledge system that will help develop appropriate responses to situational requests and strategic actions); "digital" government platforms[6].

We should note that the national e-government system in Ukraine today is not sufficiently developed; it is largely used to ensure the activities of government agencies: built information systems, databases, local and corporate networks, the introduction of electronic document management, etc. There is a significant distortion towards provision of information to the population (such as reference information, news feeds, etc.), less attention

4 Official site of the Ministry of Digital Transformation of Ukraine, https://thedigital.gov.ua/.

5 The system of electronic interactions for state electronic resources "Trembita", https://trembita.gov.ua/.

6 O.V. Evsyukova, The concept of service–oriented development of the state based on the formation of mechanisms managing the service processes of public authorities, "Publichne upravlinnia i administruvannia v Ukrainie" 2018, no. 5, p. 47.

is paid to the mechanisms of active communication with citizens; special competent bodies are at a distance from citizens[7].

The COVID-19 crisis has shown that insufficient digital skills prevent citizens from having adequate access to information and services, which is crucial for the entire population. In the current situation, this is especially true for staff in the health care system, civil servants, and education personnel.

That is why the issue of cyber-security acquires fundamentally new features and goes far beyond the prevention of wars, armed conflicts or terrorist operations.

The political digitalization of Ukrainian society is characterized by challenges to the political stability of modern Ukraine, including: lack of citizens' consolidated political identity; dysfunction of institutions of public control and participation. These challenges destroy the stability of social transformations toward democracy, create conditions for preserving the state of electoral democracy, prevent their transition to the consolidation phase, lead to increased dysfunction of public authorities, inhibit the development of service-state institutional architecture, thus, the service state cannot actually be formed.

The formation and implementation of public policy to combat cyber-terrorism in Ukraine is closely linked with globalization and current regional processes that are related to the threats of a global nature, as well as the armed confrontation at the east of Ukraine. Counterwork against these threats is an essential and necessary scientific and practical objective for our country. The spread of informational systems, mediatization and computerization of society has led to the growth of real and potential threats to national interests in the informational sphere and revealed many issues regarding ensured cyber-security[8].

Thus, cyber-terrorism is a fundamentally new terrorist activity aimed at using modern information technologies to disrupt or destroy government infrastructure (critical infrastructure, potentially vulnerable anti-terrorism facilities, etc.). Its feature is the manipulation of people's consciousness through the active use of psychological influence.

7 Digital Agenda of Ukraine – 2020: Conceptual principles (version 1.0). Priority areas, initiatives, projects of „digitalization" of Ukraine until 2020. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.

8 K.I. Dolzhenko, *Informational security of the region: the essence and content of the concept*, "Nashe pravo" 2014, no. 2, p. 47–48.

It is worth highlighting the main components of cyber-terrorism in Ukraine, associated with the development of political digitalization of society: 1) informational-psychological terrorism, which means control over the media to spread misinformation, rumours, demonstrate terrorist organizations' power; influence on operators, developers, representatives of information and telecommunication systems through violence or threat of violence, use of methods of neurolinguistic programming, hypnosis, means of creating illusions, multimedia means for entering information into the subconscious, etc.; 2) informational-technical terrorism, which means causing damage to certain physical elements of the state informational environment; creating obstacles, using special programs that stimulate control system destruction, or, conversely, external terrorist control over technical facilities; destruction or active suppression of communication lines, incorrect addressing, artificial overload of switching nodes, etc.; 3) cognitive terrorism, which means the legitimization of violent ways to achieve illegal terrorist goals by influencing the emotional and behavioural components of human society, public consciousness, the formation of social radicalized stereotypes with unconscious, emotionally charged stimuli, the formation people's attitudes, views (especially of young people) by cognition of the world around and oneself via extremist and radical actions. This leads to such cognitive concepts as radicalism, extremism, bigotry, chauvinism, fundamentalism; 4) network terrorism, which means massive coordinated actions of large social networks (self-governing private or non-governmental organizations) having destructive terrorizing influence on society, changing its consciousness and management; 5) social-communicative terrorism, which means the destruction of social foundations through specially created programs that teach people to thoughtlessly perceive any information and believe in it (manipulation with public opinion via communications, presented using physiological and psychological objective laws for perception)[9].

In conclusion, public authorities' inability to establish an effective mechanism combating cyber threats has created the preconditions for the growth of different types of cyber-terrorism. Therefore, during political digitalization of society, it is necessary to take into account that the terrorist threat will only increase, and the Ukrainian state and civil society must find an

9 R.R. Marutyan, *Recommendations for improving Ukraine's information security policy*, http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90(=uk.

agreement to achieve an optimal balance between security, freedom of speech and democratic freedoms. As our state has an active armed conflict and hybrid informational confrontation, it is necessary to initiate at the international level the development of unified legislation for cyber-terrorism combating, as well as to introduce a unified system to combat this crime, rather than declaring populist views.

Bibliography

Dolzhenko K.I., *Informational security of the region: the essence and content of the concept*, "Nashe pravo" 2014, no. 2.

Evsyukova O.V., *The concept of service-oriented development of the state based on the formation of mechanisms managing the service processes of public authorities*, "Publichne upravlinnia i administruvannia v Ukrainie" 2018, no. 5.

Marutyan R.R., Recommendations for improving Ukraine's information security policy, www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90(=uk.

Shishatsky E., Yurasov S., *Digital strategy of V. Zelensky: there is a criminal behind each register*, https://tech.liga.net/technology/interview/didjital-strateg-zelenskogo8.

Cyfryzacja polityczna społeczeństwa ukraińskiego – wyzwania w obszarze cyberbezpieczeństwa

Streszczenie

W artykule opisano stan cyfryzacji politycznej społeczeństwa ukraińskiego, definiowany jako stopniowy, wielowektorowy proces transformacji społeczeństwa w kierunku technologii cyfrowych, wpływający na wszystkie sfery życia publicznego, w tym na politykę i administrację publiczną. Specyfika transformacji cyfrowej na Ukrainie jest prezentowana w kontekście kształtowana się państwa usługowego. Badana jest problematyka cyberbezpieczeństwa. Analizowana jest również ukraińska polityka publiczna wobec cyberterroryzmu. W artykule zidentyfikowano i scharakteryzowano główne aspekty cyberterroryzmu na Ukrainie, związane z rozwojem procesu cyfryzacji politycznej społeczeństwa, w tym: terroryzm informacyjno-psychologiczny, terroryzm informacyjno-techniczny, terroryzm kognitywny, terroryzm sieciowy i terroryzm społeczno-komunikacyjny.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, cyberterroryzm, państwo usługowe, transformacje cyfrowe, cyfryzacja polityczna, społeczeństwo