DOI: https://doi.org/10.36059/978-966-397-363-0-77

STRATEGY FOR THE DEVELOPMENT OF UKRAINE'S IT SECTOR AS A DETERMINANT OF STATE SECURITY

Zavhorodnya Elizaveta
Postgraduate student of the Department of International Management,
State University of Trade and Economics
Melnyk Tetyana
Doctor of Economics,
Professor of the Department of International Management,
State University of Trade and Economics

Despite challenges such as political instability and regulatory hurdles, Ukraine's IT sector has demonstrated a strong export orientation in recent years, leveraging its skilled workforce and competitive cost advantage to allow Ukraine to attract customers from around the world, which has significantly increased export earnings and contributed to economic growth.

However, recent studies show [1; 2, pp. 53–57] that the war has added a number of problems that weaken the international competitiveness of the domestic IT sector, in particular: (1) the risk of failures in the ICT infrastructure (information and communication technology infrastructure), for example, due to physical damage, power outages, failures in Internet connection, etc; (2) the forced re-location of IT-companies both within Ukraine (leading to economic imbalance of the regions) and abroad; (3) migration of IT professionals and scientists, which leads to a weakening of the innovation potential of the information technology sector; (4) inadequate and ineffective political and legal environment in terms of establishing and guaranteeing transparency of the public administration system, protection of property rights, protection of investments, efficiency of the judicial system and government integrity; (5) vulnerability of digital infrastructure to cyberattacks; (6) reputational damage to domestic IT-companies as potentially unreliable business partners, which leads to the reduction and cancellation of projects with foreign counterparties due to the high risk of non-fulfilment of contracts; (7) mobilization of IT specialists into the Armed Forces of Ukraine; (8) imbalance in the IT labour market (shifting it from a "candidate market" to an "employer market" with a significant excess of supply over demand); (9) low ability of domestic IT-companies to compete with foreign IT-companies in terms of remuneration; etc.

In view of the above problems, there is a need to revise the strategy for the development of Ukraine's IT sector, as a new approach is crucial for adapting to a changing environment, stimulating innovation, increasing resilience and security, supporting digital transformation, and attracting international cooperation and investment. The peculiarities of Ukraine's economic development determine the specific aspects of building an IT sector development strategy.

First, the strategy for the development of Ukraine's IT sector should prioritize key areas that are crucial for ensuring the resilience, security, and continuity of the country's digital infrastructure. It should be noted that the updated cybersecurity strategy of Ukraine should take into account several key factors related to state security, in particular, it should:

1) provide for investments in technology, training and international cooperation;

2) focus on data protection and privacy, ensuring compliance with international standards and promoting awareness of data privacy;

3) develop resilience to cyberattacks, such as ransomware and DDoS attacks, to maintain the continuity of digital infrastructure;

4) protect Ukraine's national sovereignty by countering challenges such as disinformation campaigns and foreign interference;

5) to certify internal network security;

6) verify the supply chain of new network elements, update software and maintenance procedures;

7) identify and implement cloud hosting services;

8) focus on talent development, building a skilled workforce in cybersecurity and ICT through education, training programmes, and cooperation between academia, industry, and government.

Second, a review of the IT sector's foreign trade strategy in the context of national security should help proactively respond to new threats, seize economic opportunities, and protect its critical assets and interests in the digital space. Given the import dependence of the domestic IT sector on Chinese hardware production (an average share of 50% in imports of ICT goods during 2008-2022), there is an urgent need to review and diversify suppliers by imported product nomenclatures [3; 4]. It is worth noting that Chinese-made hardware and software pose risks to Ukraine's national security, including potential espionage, supply chain vulnerabilities, cyberattacks, and data privacy issues [5–6]. In addition, Chinese law requires technology companies to hand over confidential data to the Chinese government upon request [7]. Besides, the data obtained at the request of the Chinese government can be transferred to the leadership of the Russian Federation for the use in the war against Ukraine.

Third, to reduce the brain drain in the IT sector, the national strategy should focus on retaining local talent, promoting R&D (investment in innovation centres and technology clusters), improving education and training, creating collaborative ecosystems, supporting startups and entrepreneurs, facilitating international cooperation and exchange programmes, developing favourable policies and incentives, and promoting cultural and social integration. Furthermore, to retain local talent, domestic

IT companies and the state should offer competitive salaries, career opportunities, and a favourable working environment.

A separate direction of the strategy to reduce the migration of qualified specialists from Ukraine should involve the revision of the existing system of legislation on entrepreneurship, as well as professional training and retraining of the talent pool of the domestic IT sector. From our perspective, the priority components are: (1) creation of training centres and incubators, through international cooperation, donor investments, government funding, and initiatives aimed at high-tech industries or specialized segments with the aim to support young entrepreneurs in launching startups; (2) modernization of the approach to organising the educational process, in particular, it is important to revise the requirements for teachers and professors of higher education institutions, allowing experienced professionals without a degree to teach at universities; (3) involvement of students in real IT business (IT companies should offer courses and laboratories in big data analysis, artificial intelligence, the Internet of Things, blockchain, cybersecurity, augmented and virtual reality); (4) organizing regular professional events to exchange ideas, appointing faculty representatives to liaise with IT clusters, as well as providing universities with quality internship centres; and other initiatives to develop prospects for further professional development of IT specialists.

Fourth, the revision of Ukraine’s IT sector development strategy should take into account the restoration and modernization of the ICT infrastructure, as an updated approach will help improve connectivity, competitiveness, digital inclusion, efficiency, productivity and massive adoption of the latest technologies. It should be emphasized that the strategy to rebuild and modernize the ICT infrastructure should involve the following key components: (1) a comprehensive assessment to identify any weaknesses, vulnerabilities, or outdated technologies; (2) targeting investments in important areas such as broadband, cybersecurity, data centres, and digital skills training; (3) public-private partnerships to leverage expertise, funding, and resources for infrastructure development; (4) focusing on the integration of new technologies such as 5G, the Internet of Things, artificial intelligence, and cloud computing to promote innovation and competitiveness; (5) ensuring the availability of spectrum for 5G by refarming in the lower frequency band and eliminating services that use the mid-band spectrum; (6) strengthening the potential at all levels of governance to ensure the possibility of sharing ICT infrastructure; and (7) completing the upgrade of telecommunications serving the education and health sectors.

Finally, it is necessary to update the national legislation in the area of information and communication technologies and define strategic goals to ensure the provision of basic ICT services to citizens, especially in combat zones, support and protect ICT infrastructure in undamaged areas, provide for post-war goals and actions, and allocate funds by the government of Ukraine to finance the restoration and development of the IT sector. It should be noted that in wartime, ICT policy development should be based on the latest data and information on damage, and working groups should be responsible for restoring network capacity. In addition, in the long term, it is necessary to promote competition as a driving force for the development of the IT sector at the legislative and regulatory levels. Legislative protection of intellectual property and investors' rights remains an additional focus, namely: (1) modernization of intellectual property legislation should demonstrate the state's will to protect intellectual property rights by improving the system of patent registration and royalty payments, addressing international recognition through cooperation with WIPO, and developing measures to eliminate pirated content at all levels; (2) the review of investor protection legislation should include the analysis of the work of local investment support offices, consideration of IT disputes involving foreign parties in common law countries, introduction of necessary amendments to the legislation, preparation and execution of trainings on common law disputes, as well as the introduction of an investment incentive programme that would encourage businesses to invest in innovative developments, research centres, business incubators, accelerators and startups.

Therefore, there is a need to create an updated strategy for the development of the IT sector, taking into account the specified features and threats.

References:

1. Melnyk T., Zavhorodnya Ye. (2022) The IT sector of Ukraine on the world market: 2022. *Foreign trade: economics, finance, law*, vol. 125, no. 6, pp. 17–36. DOI: https://doi.org/10.31617/3.2022(125)02 (accessed February 5, 2024).
2. Zavhorodnia Ye. O., Melnyk T. M. (October 25, 2023) Problemy zabezpechennia mizhnarodnoi konkurentospromozhnosti IT-sektoru Ukrainy. *Aktualni problemy v ekonomitsi, finansakh ta upravlinni*: materialy Mizhnar. naukovo-prakt. konf. Odesa. P. 53–57. Available at: https://researcheurope.org/wp-content/uploads/2023/10/re-25.10.23.pdf (accessed February 5, 2024).
3. Website «UNCTADstat». Available at: https://unctadstat.unctad.org/EN/ (accessed February 5, 2024).
4. Website «Trade Map – Trade statistics for international business». Available at: https://www.trademap.org/Index.aspx?nvpm=1%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c%7c (accessed February 5, 2024).
5. Website «China-based Supply Chain Cyberattacks Hit Thousands of Android Devices». Available at: https://www.msspalert.com/news/human-security-disrupts-supply-chain-android-attacks (accessed February 5, 2024).
6. Website «DHS warns against using Chinese hardware and digital services». Available at: https://www.zdnet.com/article/dhs-warns-against-using-chinese-hardware-and-digital-services/ (accessed February 5, 2024).
7. Website «Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice». Available at: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html (accessed February 5, 2024).