

DISINTEGRATION RISKS OF IMPLEMENTING OF INFORMATION AND COMMUNICATION TECHNOLOGIES: MANIFESTATION, CONSEQUENCES, WAYS OF PREVENTION

A.V. Kolodiychuk

PhD, Associate Professor of Uzhgorod Trade and Economic Institute of the Kyiv National Trade and Economic University

Keywords: integration, Internet, phishing, bots, state mechanism, cyberwar, social networks, separatism.

After the global financial and economic crisis of 2008-2009 and in the context of the rise of international political conflicts, which are very often transcended into the economic plane, there is a tendency towards a strengthening of disintegration processes in different regions of the world. In general, an indispensable attribute of democratic social foundations, to which Ukraine also belongs, there is an extremely wide network of electronic information platforms for the expression of public opinion regarding the political, economic and social processes taking place in a state at a specific time. In countries with a dominant authoritarian political regime the Internet, other sources of information are censored, and socio-political Internet freedom is limited. In totalitarian regimes the Internet and private media are generally banned, and any manifestations of initiative free-thinking in this direction are severely punished. The latter make up a minority in the world. However, the current world is fundamentally changing, because in it disintegration and centrifu-

gal processes are increasingly causing information misuses, misinformation of users through the Internet, cyber attacks, various kinds of hacking attacks, social networking disturbances, the massive spread of hostile internet propaganda, economic cyberdiversions in instability regions, the lack of state-controlled countermeasures for leveling threats, cyberwars from different states, cyber-revolutionary separatist movements, and not just the differentiation of the level of regional development within the country, some countries within integration associations, socio-cultural contradiction between them, centrifugal political processes. If several decades ago it was believed that then computer technologies are not capable of leading to such serious consequences as the loss of sovereignty of countries over certain territories, the collapse of large integration associations, then this threat is now real, especially if it is systemic and well thought out concerned by criminal or malicious entities. This is especially urgent for Ukraine since the war in the Donbass in 2014 were preceded by

a broad informational and propaganda campaign in the region, which was carried out with the help of various information and communication means to establish ties with the local community, and then the Ukrainian central government failed to timely and effectively respond to this for a number of reasons. It is also not a secret that the Euro-Atlantic aspirations of the Ukrainian state are periodically subjected to systematic information attacks to redirect public opinion on these issues, if not throughout the country, then in its separate parts. Statistically this looks like this: since the beginning of the war on the Donbas in 2014-2017, Ukraine has suffered more than 7 thousand [1] of various cyber attacks. One of the most widespread attacks was the proliferation of the "NotPetya" virus in June 2017, which paralyzed for some time the work of the central executive authorities in Ukraine and major infrastructure facilities and infected computers in a phishing scene or through updating functions in a well-known computer program M.E.Doc for accounting and reporting. As a result, the state mechanism faces with significant obstacles in the conduct of its policy in a number of regions, which greatly undermines the international prestige of Ukraine in the eyes of key Western partner countries. Ukraine is not the only country facing such a challenge; a number of high-profile and large-scale separatist and disintegration cybercamps have swept the world: #Calexit is an Internet-based moving for the independence of the US state of California [2], #Brexit, #Frexit, #Grexit are broad information campaigns

for the UK, France, Greece exit from the European Union that starting in 2016, #Catalonia Exit is the separatist movement for the disconnect of Catalonia from Spain in 2017 (various websites for supporting the region's independence, own internet domain.cat, unlike the Spanish.es, regional internet media, about 4,500 bots are involved). Some curiosity and lively interest, especially in societies with a rich historical and cultural heritage, including Ukrainian ones, has a subgroup of historiographical risks and risks of ethno-cultural conflicts. Their essence lies in threats to national security, namely, peace, political stability and territorial integrity of the state, which are realized through the information space with the help of modern ICT carriers and technologies. This subgroup is divided into such classes of threats: propaganda risks; the threat of incitement to interethnic hostility; disinformation threats. This is especially true for Ukraine in the conditions of the war in the east of its territory, which began in 2014 and is being held against it, including in an informational way. The Internet has become quite a powerful tool for contemporary propaganda, disinformation, psychological impact on public opinion. Very often, in 90% of cases, this kind of cyber threats is being implemented through online phishing. A striking event of recent decades has been the Russian-Estonian cyber conflict, the reason for which was the transfer of the "Bronze Soldier" in Tallinn in 2007, which mainly consisted of massive DoS-attacks and defections of official government-owned Estonian websites.

Hence, the disintegration threats in which ICTs become toolkits are increasingly reminded of themselves, as they enable the carriers of these threats to act extraterritorially and often anonymously, but to neutralize them, they require significant financial resources, qualified cyber-organs.

References

1. Official site of the Association of IT of Ukraine (n.d.). Retrieved from www.itukraine.org.ua
2. Yes California Independence Campaign (n.d.). – Retrieved from <https://yescalifornia.org>