Corruption as a Cybersecurity Threat in Conditions of the New World's Order

Bohdan M. Holovkin
Department of Criminology and Criminal Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Oleksii V. Tavolzhanskyi
Department of Criminology and Criminal Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Oleksandr V. Lysodyed
Department of Criminology and Criminal Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

Abstract---The relevance of the research topic is stipulated by the need to conduct the scientific research of a state and issues of modern cybersecurity ensuring under the fight against corruption as its threat to suggest significant directions for the further development and improvement of the cybersecurity state in the context of global challenges and the pandemic and post-pandemic world’s development. The research purpose of the paper is to determine current issues and prospective of ensuring cybersecurity under the fight against corruption as its threat in pandemic and post-pandemic world conditions. General-scientific and special-legal methods of cognition have been used. By using a dialectical method, theoretical background and current issues of cybersecurity ensuring under the fight against corruption as its threat has been investigated and the modern challenges concerning this issue have been outlined. Formal-legal and comparative methods allowed suggesting the directions of cybersecurity ensuring in conditions of the fight against corruption as its threat under the global changes, digitalization and social transformations under the innovative cyber technological development of pandemic and post-pandemic reality. Discussion concerning a concept, types, challenges, issues, and prospects of cybersecurity improvement in conditions of the modern world under the fight against corruption as its threat.
Keywords---cybersecurity ensuring, cybersecurity threats, cybersecurity, corruption, pandemic, post-pandemic conditions, the fight against corruption.

Introduction

Ensuring of security historically depended on the state’s power and its economic and military potential. Today’s state has to add one more component to the mentioned obligatory list that is represented by technical possibilities to protect digitized parts of the state and its society’s differently-natured activity (Ovcharenko et al., 2020). Cybersecurity ensuring is one of the obligatory functions of modern countries to support and improve a system of the whole society protection by its state. In corrupted conditions, a focus is shifted from rights and freedoms defense of such a society to some monetary profit or welfares (Tsypko et al., 2019). Thus, in corrupted conditions, it is mostly impossible to ensure any type of security. On the one hand, corruption is already conceptually determined and realized as a danger for every country in the world. On the other hand, in conditions of the global world’s development, digitalization, the increase of technological and innovative use, mankind achievements under the fight against COVID-2019, in post-pandemic conditions corruption is still an attribute of modern states’ activity, their social dialogue, and communication (Vapniarchuk et al., 2019).

A state of cybersecurity of a separate country and the whole world depends on this phenomenon that is negative by its nature and destructive for the stable functioning of public administration subjects, appropriate performing of state functions, and the formation of trust from the side of the people concerning the bodies of state power (Tavolzhanska et al., 2020). At the same time, recently the potentialities of the new model of anti-corruption approach have been exhausted; the old tools available to law enforcement agencies are no longer able to effectively ensure the fight against corruption. Accordingly, the search for new effective tools within the framework of the indicated paradigm of institutional counteraction to corruption is becoming the key task of the modern state, which is gradually abandoning punitive and repressive mechanisms as the main ways of fighting corruption (Vorontsov et al., 2020).

Each legal framework has its aims and purposes and establishes its mechanisms to achieve them (Markopoulou et al., 2019). The reduction of corruption is considered one of the most important steps to pave the way for sustainable development and to promote inclusive societies by building effective, accountable, and inclusive institutions at all levels (Mugellini & Villeneuve, 2019). Speaking practically, the global anti-corruption effort does not need new rules but, rather, better implementation. The human rights approach can contribute to closing the implementation gap. The full recognition that corruption undermines the enjoyment of human rights allows the universal, non-adversarial human rights monitoring bodies to legitimately address corruption in detail without overstepping their mandate. By contributing to a change of the frame of reference and by opening up new options for monitoring and litigation, the human rights perspective can usefully complement the criminal law approach to corruption and
thereby contribute to the fulfillment of the development goals of Agenda 2030 (Peters, 2018; Bohdan et al., 2019).

Thus, the purpose of the article is to determine current issues and prospects of cybersecurity ensuring in pandemic, post-pandemic world’s order conditions under the constant fight against corruption. To achieve this aim it is needed to perform the following tasks:

- To consider theoretical-legal fundamentals of corruption as a cybersecurity threat.
- To analyze the current state, issues, and challenges for cybersecurity in modern conditions of the fights against corruption.
- To investigate particularities and suggest prospects of cybersecurity ensuring under the fight against corruption in pandemic and post-pandemic reality.

The mentioned tasks are to investigate the subject of the article that is cybersecurity ensuring under the fight against corruption as its threat taking into account the legally regulated relations and activity in the sphere of cybersecurity ensuring and fight against corruption that is the object of the paper (Kostyuchenko et al., 2019). To achieve the aim of the paper, general-scientific and special-legal methods of cognition have been used. By using the dialectical method, theoretical background and current issues of cybersecurity ensuring under the fight against corruption have been investigated and the modern challenges concerning this issue have been outlined. The formal-dogmatic method contributed to the development of the author’s explanation of corruption as a threat to cybersecurity in pandemic and post-pandemic reality. Formal-legal and comparative methods allowed suggesting the directions of cybersecurity ensuring under the fight against corruption in conditions of global changes, social transformations, and innovative digital development of pandemic and post-pandemic world’s reality (Andrade & Yoo, 2019; Jia et al., 2018).

**Juridical fundamentals of corruption as a cybersecurity threat**

The paper investigated cybersecurity ensuring under the fight against corruption as its threat in modern conditions of global changes, total digitalization, and the increasing development of cyber-technologies in the modern world. Special attention has been paid to the current state and issues of cybersecurity. In this concern, modern challenges to cybersecurity ensuring in conditions of the fight against corruption have been outlined (Nyandra et al., 2018). The need to modernize the current system of cybersecurity ensuring within the constant fight against corruption has been proved. To provide the further effective and progressive functioning of cybersecurity under the fight against corruption in conditions of pandemic and post-pandemic world’s order, the directions of its ensuring improvement have been suggested (Cherniavskiy et al., 2019; Samilyk et al., 2019).

Cybersecurity as a type of state’s security is based on the same range of requirements that are used by modern countries of the world in relation to efficient functioning and improvement of their differently directed security
systems. At the same time, cybersecurity has a specific environment for its existence and development since a cyberattack has its focus on the digital potential of a state. Consequences as a result of cyberattacks are dangerous for devices, network systems, data, and programs and are capable to destroy a state not just digitally but even physically (Intriago & Posligua, 2020; Ritonga et al., 2021). Among differently natured types of cybersecurity threats corruption plays one of the leading roles. It may make a protective system of a country vulnerable and even destroy it. Legal regulation of processes that may suffer under the corruption influence has been always a quite important issue for every state. In times of the fight against the world pandemic that is followed by the digitalization of various types of services, processes, and activities, ensuring cybersecurity still includes the constant fight against corruption, actualizes its scientific investigation as a cybersecurity threat. For example, to combat the corruption phenomenon, the countries through their judicial authorities have in focus the following issues:

- Adopting a legal framework well-grounded to face pressures arisen from committing corruption crimes.
- Strengthening the capacity of fighting corruption crimes, as well as those assimilated with the corruption, in such a manner to lead to diminishing cases of corruption.
- Setting up a professional body of specialists in all areas of activity, especially within the public area.
- Achieving efficient justice under the principles of respecting the law and public dignities.
- Implementing efficient judicial mechanisms in criminal matters to conclude to achieving criminal procedural functions (Magherescu, 2020).

It has to be stressed that there is no universally accepted definition of corruption. There is a tendency to use the term “corruption” loosely as a catchall term. There is also considerable disagreement over which specific acts constitute corruption. Today, probably the most used definition is the one adopted by the non-governmental organization Transparency International: “corruption is the abuse of entrusted power for private gain” (Baccio-Terracino, 2008). The popular public-office-centered definition of corruption as “the abuse of public office for private gain” is no exception, of course (Farrales, 2005).

**Role and significance of corruption as a cybersecurity threat**

The international community concerning this issue bases theoretical determination of corruption as a cybersecurity threat on its general understanding. At the same time, the specific is revealed by the condition that is connected with a special environment of this negative phenomenon functioning that is represented by cyberspace and involved technologies, the use of which should be as safe as possible for the whole county and every member of its society. Security is a critical concern around the world that manifests in problems such as protecting our cyber infrastructure from attacks by criminals and other nation-states; protecting our ports, airports, public transportation, and other critical national infrastructure from terrorists; protecting our wildlife and forests
from poachers and smugglers; and curtailing the illegal flow of weapons, drugs, and money across international borders (Sinha et al., 2015).

Cross-national measures of corruption suffer from serious definitional imprecision. Because perceptions of corruption invariably differ from country to country, most cross-national studies sacrifice breadth for depth. Case studies, therefore, will always be important because they allow for a deeper and more rigorous understanding of how and why corruption works (Farrales, 2005). Corruption is a widespread phenomenon that is increasingly a normative behavior and can be curbed through effective implementation of various schedules of reinforcements, punishments, transparency, accountability, awareness, modeling, and psychological strategies to understand and combat corruption (Chugh, 2012). We think that in pandemic and post-pandemic reality corruption as a threat to cybersecurity may be understood as a potentially destructive phenomenon with the visible and invisible retrospective consequences of security vulnerabilities in cyberspace that make it impossible to provide and guarantee the prevention of cyber-attacks and effective reduction of their negative consequences (Asri et al., 2021; Hussin et al., 2021).

Classical states in different historical periods fought against various threats to keep the state sovereignty, territorial integrity, socio-economic stability, further functioning, and prosperity. Most modern states due to the high level of their societies’ digitalization and rapid cyber technological development faced new types of threats that are cyber by their nature. Thus, modern countries have to provide effective state policies to fights against the mentioned above to keep information state sovereignty, stability, and further existence in changed digital reality. As a phenomenon, corruption is dangerous for virtual reality too (Al-Marhubi, 2000; Potrafke, 2012). Nowadays, the information state’s development except its economic and technological components depends on the decisions of the state’s power. If a country’s ruling includes corruption in the process of the differently natured decisions making, this fact lets us determine corruption as a threat to cybersecurity. Its role is quite significant due to the increase of the world informatization and the general change of the world’s look from being traditional to the digital one. The more corruption is strong, the more cybersecurity systems of separate countries and the whole world are vulnerable (Everett et al., 2007; Bhattacharyya & Hodler, 2015).

Internet infrastructure plays a crucial role in a number of daily activities. The pervasive nature of cyber systems ensures far-reaching consequences of cyberattacks. Cyberattacks threaten physical, economic, social, and political security. The effects of cyberattacks can disrupt, deny, and even disable the operation of critical infrastructure including power grids, communication networks, hospitals, financial institutions, and defense and military systems (Bakdash et al., 2018). For example, even dealing with such a form of democracy as elections, corruption may destroy it significantly. Elections are entering a new digital era in which there are new opportunities and threats for the conduct and contestation of elections. Although many of these are not entirely new – perhaps being a continuation of older problems there has been a qualitative leap like the challenges (Garnett & James, 2020).
These options may pose countervailing public harms by undermining access to information and reducing transparency and accountability. The political outcry surrounding disinformation has, possibly disproportionately, metastasized the problem in the eyes of the public, and regulators should be cautious not to regulate too broadly as a political debate is critical to an informed electorate and to supporting democratic principles (Judge & Korhani, 2020). A new corruption concept not constrained by public-sector, illegality restrictions; corruption is seen as a deal between people for the exchange of favors over time (in the most appealing example two agents, one from the private sector, the other from the public sector, trade favors over time, with the public sector agent making use of her public office investment) (Kaufmann & Vicente, 2005).

To our point of view, the destructive role of corruption as a cybersecurity threat in every single country may be understood just after its negative influence on such a state, where the connected consequences make all the state’s cybersecurity vulnerabilities visible being critically dangerous not just for the people safety but even for such a country existence. Non-acceptance and non-awareness of corruption as potential step-by-step destruction of the whole state is a mistaken approach, which is one of the key-moments in cyberwars (Downar et al., 2010; Bojovic et al., 2020).

Currents issues and prospects of cybersecurity under the fight of corruption as its threat

The issues of cybersecurity are predisposed by modern challenges to the state’s security system as a whole that are concentrated now on the need for new governing due to the pandemic and post-pandemic conditions. At the same time, corruption is a traditional phenomenon that reflects on new relations with cyber components due to a variety of reasons. The prospects of modern cybersecurity ensuring are dictated by the urgent reaction to modern technological changes and social requirements to be protected by a state under any conditions. At the same time, traditionally, national governance and corruption challenges have been seen as:

- Particularly daunting in the poorer countries, with the richer world viewed as an example or benchmark.
- Anchored within a legalistic framework and focused on the quality of formal institutions.
- A problem of the public sector.
- Divorced from global governance or security issues, which are regarded as separate fields (Kaufmann, 2004).

Governance and corruption remain controversial and misunderstood topics. But they are now given higher priority in development circles and by the corporate sector, including multinationals (Kaufmann, 2005). A large part of the project of combating institutional corruption consists in formulating rules and procedures that determine what is to count as corruption, not merely preventing conduct that is already known to be corrupt (Thompson, 2013). However, the “hacking” of democracies that is the substance of so much punditry and practitioner reporting in recent years has relatively little to do with the direct employment of cyber
instruments to disrupt, degrade, or spy. Rather, the threat to democratic political systems emerges from the mismatch of new systems that now undergird discourse and those regulations and norms of behavior that must be adopted in years to come to safeguard the integrity of national polities (Whyte, 2020).

In our point of view, a phenomenon of corruption is predisposed by the internal development of a society that is on the way of its development to make its quite important democratic choice. Corruption is always a kind of threat that can never be controlled and reduced if such a society includes it as a form of communication. The main issue of corruption for cybersecurity is located in the internal needs and interests of societies that are now more and more digital ones. If they follow the democratic way of their development, the main prospect concerning the mentioned issue is to remove corruption from their reality (Von Solms & Van Niekerk, 2013; Jang-Jaccard & Nepal, 2014).

The increasing of the fights against COVID-2019 shifted the attention from the constant requirement to fights against corruption. But the second phenomenon is enriched in pandemic conditions especially due to the fact of the social control decrease that is conditioned by the requirement of social distancing. Nowadays, traditional challenges to state security are spread in the cyber area due to the increasing use of cyberspace and the involved technological possibilities by modern countries. These all call our attention to basic and interconnecting security situations:

- Any member of information and communication networks – whether international, state or civilian – can be a potential victim of cyberattacks;
- Cyberattacks can have serious national security and economic consequences, and can endanger the everyday life of a society;
- Defense against threats is a task at the international, national and individual user level as well (Szabo, 2019).

In the conditions of cyber reality, first, the complexity of the target software itself could render an attack unpredictable simply by obscuring what would happen when the software systems interfered with or disrupted. Second, because most computer systems are connected to other computer systems via the Internet, some kinds of attack could spread across these computers. The complexity of each system and how they are connected mean that it is hard to make predictions about the extent and speed of spread and the impact on each computer. Third, corruption of computers could generate physical effects that cascade well beyond cyberspace and are themselves difficult to predict (Farrell & Glaser, 2017).

The use of Artificial Intelligence for cybersecurity ensuring may be an object of corruption manipulation tool. That is why even here the fight against this phenomenon is quite significant. Nowadays, AI is neither magic nor is it intelligent in the human-cognitive sense of the word. Rather, today’s AI technology can to produce intelligent results without intelligence by harnessing patterns, rules, and heuristic proxies that allow it to make useful decisions in certain, narrow contexts. However, current AI technology has its limitations. Notably, it is not very good at dealing with abstractions, understanding meaning, transferring knowledge from one activity to another, and handling completely
unstructured or open-ended tasks (Surden, 2018; Getman & Karasiuk, 2014). Corruption may have its negative impact even on investments to security. An executive who is skeptical of security investments may believe that unless a firm incurs a breach every year, it is wasting its IT security investment every year it does not suffer a breach. Alternatively, it may imply that a firm can expect to lose the equivalent of its IT security budget each time it suffers a data breach or security incident (Romanosky, 2016).

Cybercrime costs include damage and destruction of data, forensic investigation, restoration and deletion of hacked data and systems, fraud, post-attack disruption to the normal course of business, stolen money, lost productivity, theft of personal and financial data, embezzlement, and reputational harm and theft of intellectual property (Ahmad, 2020). At the same time, the deepest difficulty in maintaining the legitimate/malicious binary – and therefore constructing a stable foundation for cybersecurity itself – is not the range of technological, social, and economic pressures explicitly recognized by cybersecurity experts, but their implicit embrace of cyber-noir (Shires, 2020). Thus, on the one hand, the use of technologies in a digital world is a present need of reality. On the other hand, corruption in this area is a permanent challenge that may stipulate states’ destruction in this direction. Thus, the whole world’s community should fight against this negative phenomenon not just in visible reality but in invisible, that is a cyber-one.

**Prospects of the cybersecurity ensuring under the threat of corruption in modern times**

Today’s prospects of cybersecurity ensuring within a systematical fight against corruption depend on economic stability and improvement of a country. The prevailing position of economic factor plays a leading role in the development of every type of security ensuring, including the cyber one. The corrupted environment that does not have society and state interests in its essence may never guarantee neither cyber nor any other type of security. In modern times of technological development and innovative achievements, corruption is still a threat. More else, it has to be understood that it is potentially and practically dangerous not just for cyber, but for a state of security of the whole country.

We think that the modern approach to ensure cybersecurity has to be based on the understanding that corruption, on the one hand, has to be under constant state control. And if we are talking about corruption in such a state, so civil society has to control its country all the possible means to remove potential danger for the further development and prosperity of its state. On the other hand, corruption will be always a strong factor for society members to be not passive but active participants of the state’s processes and activity. From this point of view, the presents of corruption even on rather a low level motivates society to be involved in the process to prevent its increase. Thus, it integrates society to reach the common aim and develop its existence and well-being.

Nowadays, we insist that there should be a rational and practically oriented approach to cybersecurity ensuring. It has to include a two-component structure that is represented by properly educated and ideologically trained public
administration, on the one hand, and members of a society with similar qualities, on the other hand. The functioning of the cybersecurity control and threats prediction in this sphere directly depends on the technical side of this issue. We insist that modern cybersecurity ensuring in conditions of the fight against corruption has to be made on the level of protection of data, devices, networks, and programs functioning from being overused by corrupted structures.

Prevention of cyberattacks and elimination of their negative consequences on critical infrastructure facilities should be under constant control not only by the state but also by public organizations and individuals since corruption in this area can block access to financial and medical institutions, power plants in critical conditions of natural disasters, as well as military conflicts. The modern system of cybersecurity ensuring requires the coexistence of people, technologies, and the process of the use of the second by the firsts to be protected against cyberattacks. The creation and systematic support of the whole country’s cybersecurity strategy have to be added by the constant training of the population to know and observe cybersecurity principles and have a negative attitude to corruption as an attribute of not just economically weak but ideologically disorganized society.

The fight against corruption has to be multi-fronted. While laws and law enforcement are indispensable, countries serious about fighting corruption should also pay attention to reforming the role of government in the economy, particularly those areas that give officials discretionary power which are hotbeds for corruption. Recruiting and promoting civil servants on a merit basis, and paying them a salary competitive to private sector alternatives help to attract high-quality, moral civil servants. International pressure on corrupt countries, including criminalizing bribing foreign officials by multinational firms, is useful. But the success of any anti-corruption campaign ultimately depends on the reform of domestic institutions in currently corrupt countries (Wei, 1999). Investigating trends, drivers, and implications for the cybersecurity environment to 2022 in Canada Dupont B. (2020) determines the following recommendations.

- Design and deploy procedures and tools for ongoing monitoring, the objective of which will be to monitor the development of the digital ecosystem and survey the various actors and interactions, and assess the effects of these transformations on cybersecurity.
- Align the regulatory regimes applicable to the various infrastructures, applications and content with the resources and strategies implemented by a growing number of government actors, as well as their private partners, to quickly detect emerging digital risks and limit their impact on a constantly evolving ecosystem.
- Initiate an in-depth consultation and reflection exercise to formulate proposals on how to restructure existing government institutions or create new ones to adapt the Canadian government’s intervention and coordination abilities to the new needs.
- Intensify empirical research on the transformations of risks, standards and practices associated with privacy protection in the digital ecosystem;
Accentuate coordination and knowledge-transfer initiatives of national and provincial authorities in order to accelerate and standardize the development of local capabilities (Dupont, 2012).

With the mentioned above, we insist that under the need to fight against corruption, the progressive and efficient implementation of cybersecurity ensuring may be supported and improved just by a society with an appropriate level of information literacy and culture in the symbiosis with deep respect to traditional and historical values of their nations within the ideology of national development and prosperity. Just a quite high level of internal deep respect and appreciation to own country, its heritage, values, and culture with a modern understanding of the need to make differently-oriented multicultural communication for the further personal and, more else, own state development and well-being may create a reliable platform for cybersecurity ensuring.

Preserving cybersecurity is hard. So, it turns out, is constructing cyber norms... Desired outcomes remain in the ether until there are norms (among other instruments) that spell out social expectations for the behavior that might achieve them. How these constructions come into being can be complicated, but neither cyberspace nor its norms are so impenetrable that actors should ignore the various contexts, ingredients, and process tools involved. On the contrary, understanding the actual processes by which cyber norms form, diffuse, and evolve is likely to influence the future shape of cybersecurity (Finnemore & Hollis, 2016).

**Conclusion, Recommendations and Limitations**

It has been proved that the current system of cybersecurity ensuring estimates corruption as its threat. A modern conceptual understanding of cybersecurity ensuring in pandemic and post-pandemic times of the fight against corruption is based on a variety of technical, economic, political, and even psychological tools and means to stabilize the level of data, devices, networks and programs protection, reduce the corruptive potential to overuse them with a destructive purpose, and constantly improve a safe environment as a base of constructive activity in this area.

This process includes two obligatory components that are represented by properly educated and ideologically trained public administration, on the one hand, and members of a society with similar qualities, on the other hand. The technical side of cybersecurity ensuring issue depends on the economic development of a state and defines the further types of cybersecurity system functioning and improvement. At the same time, under the need to fight against corruption in pandemic and the post-pandemic world only societies with an appropriate level of information literacy and culture in the symbiosis with deep respect to traditional and historical values of their nations within the ideology of national development and well-being with a modern understanding of the need to make differently-oriented multicultural communication for the further personal and, more else, own state development may support and improve the progressive and efficient implementation of a national cybersecurity policy.
The materials in this paper may be useful for researchers in the sphere of cybersecurity ensuring in conditions of the fight against corruption with the purpose to modernize a current cybersecurity system, for specialists focused on developing the suggestions and improving its quality under modern challenges of the pandemic and post-pandemic reality. In the research process, new questions and issues arose that are needed to be solved. It is necessary to continue the investigation of methods and details of the effective practical implementation of cybersecurity ensuring its development and improvement in conditions of the fight against corruption under pandemic and post-pandemic circumstances under the progress of cyber technologies.

References


