Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Holovkin, Tavolzhanskyi, and Lysodyed
Connections QJ 20, no. 2 (2021): 75-87
https://doi.org/10.11610/Connections.20.2.07

Research Article

Corruption as a Cybersecurity Threat in the New World Order

Bohdan M. Holovkin, Oleksii V. Tavolzhanskyi, and Oleksandr V. Lysodyed

Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, https://nlu.edu.ua/

Abstract: The important topic of cybersecurity relative to the fight against corruption in the context of global challenges in the pandemic and post-pandemic world requires further research. The purpose of this article is to identify and analyze current and prospective cybersecurity issues in this context by applying general-scientific and special-legal methods of cognition. Using the dialectical method, theoretical background, and contemporary views on ensuring cybersecurity served to investigate the key current challenges. Formal-legal and comparative methods allowed to recommend measures to enhance cybersecurity in view of the massive digitalization and social transformations. The authors emphasize the need to establish a national cybersecurity policy based on society's information literacy and culture, combining respect to traditional and historical values with a modern understanding of multicultural communication and well-being.

Keywords: cybersecurity, corruption, fight against corruption, cybersecurity threats, COVID-19 pandemic, post-pandemic conditions.

Introduction

Historically, ensuring security depended on the state's power and economic and military potential. Today's state has to add one more component to the list of obligations – to protect the digitalized parts of the state and societal activities.[1] Ensuring cybersecurity is one of the obligatory functions of modern countries to support and improve the system of holistic protection of society by the state. In conditions of widespread corruption, the focus shifts from the defense of rights and freedoms to some monetary profit or other benefits.[2] Thus, in conditions of corruption, it is hardly possible to ensure any type of security. On the one hand, corruption is already conceptually determined and perceived as a danger for every country. On the other, in the processes of globalization, digitalization, rapid technological development and innovation, and the pandemic, corruption is still an attribute of modern states, social dialogue, and communication.[3] The state of cybersecurity in a particular country depends on this phenomenon that is negative by its nature and destructive to the stable functioning of public authorities, expected to adequately perform their functions and earn the trust of the people.[4]

The traditional tools available to law enforcement agencies can no longer effectively counter corruption. Recently, the interest shifted to the value of a new institutional anti-corruption approach with a lesser role of punitive and repressive mechanisms.[5]

Each legal framework has its own aims and purposes and establishes its mechanisms to achieve them.[6] 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.[7] Practically speaking, the global anti-corruption effort does

[1] Mykola O. Ovcharenko et al., "Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method," *Journal of Advanced Research in Law and Economics* 11, no. 4 (2020): 1296-1304, https://doi.org/10.14505//jarle.v11.4(50).26.

[2] Victoria V. Tsypko et al., "Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction," *Journal of Advanced Research in Law and Economics* 10, no. 6 (2019): 1664-1672.

[3] Viacheslav V. Vapniarchuk et al., "Protection of Ownership Right in the Court: The Essence and Particularities," *Asia Life Science* 21, no. 2 (2019): 863-879, http://dspace.nlu.edu.ua/handle/123456789/18141.

[4] Yu. Tavolzhanska et al., "Severe Pain and Suffering as Effects of Torture: Detection in Medical and Legal Practice," *Georgian Medical News* 10 (307) (October 2020): 185-193, http://ir.librarynmu.com/bitstream/123456789/2160/1/GMN_62-68.pdf.

[5] Sergey Vorontsov et al., "The Use of Artificial Intelligence to Combat Corruption," *Media Education* (Mediaobrazovanie) 60, no. 4 (2020): 757-763, https://doi.org/10.13187/me.2020.4.757.

[6] Dimitra Markopouloua, Vagelis Papakonstantinoua, and Paul de Hert, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation," *Computer Law and Security Review* 35, no. 6 (November 2019): 1-11, https://doi.org/10.1016/j.clsr.2019.06.007.

[7] Giulia Mugellini and Jean-Patrick Villeneuve, "Monitoring the Risk of Corruption at International Level: The Case of the United Nations Sustainable Development Goals," *European Journal of Risk Regulation* 10 (March 2019): 201-207, https://doi.org/10.1017/err.2019.16.

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 exercise of human rights allows the universal, non-adversarial human rights monitoring bodies to address corruption in detail without overstepping their mandate. By contributing to a change of the frame of reference and 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.[8]

Thus, the purpose of this article is to determine current issues and prospects of ensuring cybersecurity in the pandemic and post-pandemic world order under the continuous fight against corruption. Towards this aim, it is necessary to perform the following tasks:

1) to consider the theoretical-legal fundamentals of corruption as a cybersecurity threat;
2) to analyze the current state, issues, and challenges for cybersecurity in modern conditions of the fight against corruption;
3) to investigate particularities and suggest prospects of ensuring cybersecurity under the fight against corruption in pandemic and post-pandemic reality,

while taking into account the legally regulated relations and activity in the sphere of cybersecurity and the fight against corruption.[9]

General-scientific and special-legal methods of cognition have been applied towards this purpose. The subject has been investigated and the modern challenges outlined by using the dialectical method, theoretical background, and analysis of current issues. The formal-dogmatic method contributed to the development of the author's explanation of corruption as a threat to cybersecurity. Formal-legal and comparative methods provided the opportunity to formulate recommendations on enhancing cybersecurity.

Juridical Fundamentals of Corruption as a Cybersecurity Threat

The provision of cybersecurity needs to be studied with the account of corruption as a threat in globalization and increasing digitalization processes. To pro-

[8] Anne Peters, "Corruption as a Violation of International Human Rights," *European Journal of International Law* 29, no. 4 (November 2018): 1251-1287, https://doi.org/10.1093/ejil/chy070.

[9] O.E. Kostyuchenko et al., "Robotization of Manufacturing Process: Economic and Social Problems and Legal Ways of Their Solution," *Financial and Credit Activity: Problems of Theory and Practice* 3, no. 30 (2019): 454-462, https://doi.org/10.18371/fcaptp.v3i30.179847.

vide the increasingly effective and progressive functioning of cybersecurity under the fight against corruption in conditions of pandemic and post-pandemic global order, Cherniavskyi and co-authors have made some recommendations.[10]

Cybersecurity as a domain of state security is based on the same range of requirements used by advanced countries in relation to the functioning and development of their security systems. At the same time, cybersecurity has a specific environment for its existence and development because a cyberattack focuses on the digital capacity of a state. Cyberattack consequences are dangerous for devices, network systems, data, and software and can destroy a state not just digitally but even physically. Among the variety of cyber threats, corruption plays one of the lead 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 always been a fairly significant issue. In times of pandemics, bringing increased digitalization of various services, processes, and activities, ensuring cybersecurity still includes the constant fight against corruption, hence the need for its scientific investigation as a cybersecurity threat. For example, to combat the corruption phenomenon, states, through their judicial authorities, focus on the following issues:

1) adopting a legal framework well-grounded to face pressures arising from corruption crimes;
2) strengthening the capacity to counter corruption, as well as related crimes, and thus reducing the cases of corruption;
3) setting up a professional body of specialists in all areas of activity, especially within the public area;
4) achieving efficient justice under the principles of respect to law and public dignity;
5) implementing efficient judicial mechanisms in criminal matters to provide criminal procedural functions.[11]

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 catch-all 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

[10] Serhii S. Cherniavskyi et al., "International Cooperation in the Field of Fighting Crime: Directions, Levels and Forms of Realization," *Journal of Legal, Ethical and Regulatory Issues* 22, no. 3 (2019): 1-11, https://www.abacademies.org/articles/international-cooperation-in-the-field-of-fighting-crime-directions-levels-and-forms-of-realization-8346.html.

[11] Delia Magherescu, "Criminal Investigation of the Corruption Crimes: Evidence and Procedure in an Interdisciplinary Approach," *Revista Brasileira de Direito Processual Penal* 6, no. 3 (2020): 1239-1270, https://doi.org/10.22197/rbdpp.v6i3.394.

abuse of entrusted power for private gain."[12] The popular public-office-centered definition of corruption as "the abuse of public office for private gain" is no exception, of course.[13]

Role and Significance of Corruption as a Cybersecurity Threat

The theoretical determination of corruption as a cybersecurity threat is based on its general understanding by the international community. The specifics are revealed by its connection to the particular environment for the realization of this negative phenomenon represented by cyberspace, the use of which should be as safe as possible. Security is a critical global concern manifested 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.[14]

Cross-national measures against corruption suffer from serious definitional imprecision. Since 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.[15] Corruption is a widespread phenomenon, increasingly normative behavior that can be curtailed by implementing various schedules of reinforcements, punishments, transparency, accountability, awareness, modeling, and psychological strategies to understand and combat corruption.[16] 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 cyberattacks and effective reduction of their negative consequences.

Classical states in different historical periods fought against various threats to keep the state sovereignty and territorial integrity and provide socio-eco-

[12] Julio Bacio-Terracino, "Corruption as a Violation of Human Rights" (International Council on Human Rights Policy, January 2008), 1-36, https://ssrn.com/abstract=1107918.

[13] Mark J. Farrales, "What is Corruption?: A History of Corruption Studies and the Great Definitions Debate" (June 2005), https://ssrn.com/abstract=1739962.

[14] Arunesh Sinha et al., "From Physical Security to Cybersecurity," *Journal of Cybersecurity* 1, no. 1 (September 2015): 19-35, https://doi.org/10.1093/cybsec/tyv007.

[15] Farrales, "What is Corruption?."

[16] Divyanshi Chugh, "Psychology of Corruption," *The Learning Curve*, July 25, 2012, Lady Shri Ram College for Women Finalist, Young Psychologist 2012, National Paper Presentation Competition, Christ University, Bangalore, India, 1-11, https://ssrn.com/abstract=2117247.

nomic stability and prosperity. Most modern states, due to the high level of digitalization and rapid technological development, face new types of threats that are cyber by their nature. Thus, modern countries have to provide effective state policies to keep information sovereignty, stability, and further existence in a changed digital reality. As a phenomenon, corruption is dangerous for virtual reality too. 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 governance includes corruption in decision-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 transition from traditional to digital. The stronger the corruption, the more vulnerable are the cybersecurity systems of individual countries and the world.

Internet infrastructure plays a crucial role in a number of daily activities. The pervasive nature of cyber systems ensures the far-reaching consequences of cyberattacks. Cyberattacks threaten physical, economic, social, and political security. They can disrupt, deny, and even disable the operation of critical infrastructure, including power grids, communication networks, hospitals, financial institutions, and defense and military systems.[17] For example, even dealing with such a form of democracy as elections, corruption may destroy it significantly. Elections are entering a new digital era with 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 in the nature of the challenges.[18]

Some countermeasures may cause public harm 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. Regulators should be cautious not to regulate too broadly, as the political debate is critical to an informed electorate and supporting democratic principles.[19] In a new concept not constrained by public sector and legal restrictions, corruption is seen as a deal between people for the exchange of favors over time. Only in the most appealing example, two agents,

[17] Jonathan Z Bakdash et al., "Malware in the Future? Forecasting of Analyst Detection of Cyber Events," *Journal of Cybersecurity* 4, no. 1 (2018): tyy007, https://doi.org/10.1093/cybsec/tyy007.

[18] Holly Ann Garnett and Toby S. James, "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 111-126, https://doi.org/10.1089/elj.2020.0633.

[19] Elizabeth F. Judge and Amir M. Korhani, "Disinformation, Digital Information Equality, and Electoral Integrity," *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (2020): 240-261, https://doi.org/10.1089/elj.2019.0566.

one from the private sector and the other from the public sector, trade favors over time, with the public sector agent using his or her access to public funding.[20]

In our view, the destructive role of corruption as a cybersecurity threat may be understood only after its negative influence on the state becomes clear. The impact may make the state's cybersecurity vulnerabilities visible and a critical threat not just to the people's safety but even to the country's existence. Non-acceptance and lack of awareness of corruption as potential step-by-step destruction of the whole state is a wrong approach and one of the key features of cyberwar.

Currents Issues and Prospects of Cybersecurity under the Fight against Corruption

During the pandemic, cybersecurity and its governance became of increased importance. At the same time, corruption is a traditional phenomenon that reflects on new relations with cyber components for various reasons. Traditionally, national governance and corruption challenges have been seen as:

- particularly daunting in the poorer countries, with the more prosperous world viewed as an example or as a benchmark,
- anchored within a legalistic framework and focused on the quality of formal institutions;
- a problem of the public sector; and
- divorced from global governance or security issues, regarded as separate fields.[21]

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.[22] A large part of the project of combating institutional corruption consists of formulating rules and procedures that determine what is to count as corruption, not merely preventing conduct that is already known to be corrupt.[23] 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. Instead, the threat to democratic political systems emerges from the mismatch of new systems that now underpin the discourse and those

[20] Daniel Kaufmann and Pedro C. Vicente, "Legal Corruption," November 24, 2005, https://ssrn.com/abstract=829844.

[21] Daniel Kaufmann, "Corruption, Governance and Security: Challenges for the Rich Countries and the World," *SSRN Electronic Journal* (October 2004), https://doi.org/10.2139/ssrn.605801.

[22] Daniel Kaufmann, "Myths and Realities of Governance and Corruption," *SSRN Electronic Journal* (November 2005), https://doi.org/10.2139/ssrn.829244.

[23] Dennis F. Thompson, "Two Concepts of Corruption," Edmond J. Safra Working Papers, No. 16 (August 2013): 1-24, https://ssrn.com/abstract=2304419.

regulations and norms of behavior that must be adopted in years to come to safeguard the integrity of national polities.[24]

From our point of view, the corruption phenomenon is predisposed by the internal development of a society that is on the way to its own development towards the realization of its 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. If they follow the democratic way of their development, the main prospect is to remove corruption from their reality.

The increasing effort to constrain the pandemic shifted the attention from the constant requirement to fight corruption. But the second phenomenon is enriched in pandemic conditions, primarily due to the reduced societal control as a result of social distancing. Nowadays, traditional challenges to state security spread in the cyber area due to the increasing use of cyberspace and the involved technological possibilities. These call our attention to basic and interconnected 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 daily life of a society;
- defense against threats is a task at the international, national, and individual user levels.[25]

In reality, the complexity of the target software could render the effects of an attack unpredictable by obscuring what happens when the attacker interferes with or disrupts the software systems. Second, since most computer systems are connected to other computer systems via the Internet, some attacks could spread across different systems. The complexity of each system and its connections mean that it is hard to predict the extent and speed of spread and impact. Third, corruption of computers could generate physical effects that cascade well beyond cyberspace and are themselves difficult to predict.[26]

The use of Artificial Intelligence (AI) for ensuring cybersecurity may be an object of corrupt manipulation, too. That is why the fight against this phenomenon is quite significant even here. Nowadays, AI is neither magic nor intelligent in the

[24] Christopher Whyte, "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare," *Journal of Cybersecurity* 6, no. 1 (2020): tyaa013, https://doi.org/10.1093/cybsec/tyaa013.

[25] Zsolt Szabó, "The Effects of Globalization and Cyber Security on Smart Cities," *Interdisciplinary Description of Complex Systems* 17, no. 3-A (2019): 503-510, https://doi.org/10.7906/indecs.17.3.10.

[26] Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (March 2017): 7-17, https://doi.org/10.1093/cybsec/tyw015.

human-cognitive sense of the word. Instead, today's AI technology can produce intelligent results without intelligence by harnessing patterns, rules, and heuristic proxies that allow it to make valuable decisions in specific, 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.[27] As a result, corruption may negatively impact even investments in security. For example, an executive 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.[28]

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, reputational harm, and theft of intellectual property.[29] At the same time, the most serious 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.[30] Thus, on the one hand, the use of technologies in a digital world is the present reality. On the other hand, corruption in this area is a permanent challenge that may lead to states' destruction. Thus, the global community should fight against this negative phenomenon not just in the physical domain but in the invisible cyber reality as well.

Prospects for Ensuring Cybersecurity under the Threat of Corruption

Today's prospects of ensuring cybersecurity within a systematical fight against corruption depend on the economic performance of a country. The dominant position of the economic factor impacts the developments in every security field, including the cyber one. A corrupt environment that does not have society's and state interests in its essence may never guarantee either cyber or any other type

[27] Harry Surden, "Artificial Intelligence and Law: An Overview," Georgia State University Law Review 35, no. 4 (2019), https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8.

[28] Sasha Romanosky, "Examining the Costs and Causes of Cyber Incidents," *Journal of Cybersecurity* 2, no. 2 (December 2016), 121-135, https://doi.org/10.1093/cybsec/tyw001.

[29] Tabrez Ahmad, "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity" (April 5, 2020), http://dx.doi.org/10.2139/ssrn.3568830.

[30] James Shires, "Cyber-noir: Cybersecurity and Popular Culture," *Contemporary Security Policy* 41, no. 1 (2019): 82-107, https://doi.org/10.1080/13523260.2019.1670006.

of security. Corruption is still a threat to technological development and innovation. It has to be understood that it is potentially and practically dangerous not just for cyber but for state security.

The modern approach to cybersecurity has to be based on the understanding that corruption has to be under constant control. And when we discuss corruption, civil society has to control its country by all the possible means to remove the potential danger to the development and prosperity of its state. On the other hand, corruption will always be a strong factor in making citizens active participants in state governance. From this point of view, the gains of corruption, even on a rather low level, motivate the involvement of citizens in counter-corruption activities. Thus, citizens contribute to the common aim of development and well-being.

Nowadays, the approach to guaranteeing cybersecurity should be rational and practically oriented. It has to include two components – adequately educated and ideologically trained public administration, on the one hand, and members of a society with similar qualities on the other. The control of cybersecurity and the prediction of threats directly depend on the technical capacity. Cybersecurity in the fight against corruption needs to be ensured by protecting data, devices, networks, and software. The access of corrupt structures to their functioning should be limited.

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 and power plants in the wake of natural disasters and in military conflict. Advanced cybersecurity systems build on the coexistence of people, technologies, and processes preventing and protecting against cyberattacks. The creation and systematic support of a national cybersecurity strategy have to be added by the constant training of the population to know and observe cybersecurity principles and see corruption as an attribute of not just an economically weak but ideologically disorganized society.

Corruption is countered on several fronts. 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 high discretionary power. Recruiting and promoting civil servants on their merits and paying them a salary competitive to the private sector help attract high-quality civil servants with personal integrity. International pressure on corrupt countries, including criminalizing bribing foreign officials by multinational firms, is also a sound measure. But the success of any anti-corruption campaign ultimately depends on the reform of domestic institutions in currently corrupt countries.[31] A study of trends, drivers, and implications for the

[31] Shang-Jin Wei, "Corruption in Economic Development: Beneficial Grease, Minor Annoyance, or Major Obstacle?" (February 1999), https://ssrn.com/abstract=604923.

cyber security environment in Canada[32] delivers the following recommendations.

1) 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 cyber security;
2) 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 and their private partners to quickly detect emerging digital risks and limit their impact on a constantly evolving ecosystem;
3) 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 new needs;
4) Intensify empirical research on the transformation of risks, standards, and practices associated with privacy protection in the digital ecosystem;
5) Accentuate coordination and knowledge-transfer initiatives of national and provincial authorities to accelerate and standardize the development of local capabilities.[33]

Therefore, with the need to counter corruption, progressive and efficient implementation of cybersecurity policies may be supported and improved by a society with the 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. Only a high level of deep respect and appreciation to own country, its heritage, values, and culture, and a modern understanding of multicultural communication for continuing personal and national development and well-being may create a reliable platform for cybersecurity.

Preserving cybersecurity is challenging. 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 ignore the var-

[32] Benoit Dupont, "The Cyber Security Environment to 2022: Trends, Drivers and Implications" (2012), https://ssrn.com/abstract=2208548.

[33] Dupont, "The Cyber Security Environment to 2022."

ious 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.[34]

Conclusions, Recommendations, and Limitations

It has been proved that the current cybersecurity system identifies corruption as its threat. A modern conceptual understanding of cybersecurity in pandemic and post-pandemic times of the fight against corruption builds on a variety of technical, economic, political, and even psychological tools and means to protect data, devices, networks, and software, reduce the risk of corruption undermining them, and provide a safe environment as a base of constructive activity.

This process includes two mandatory components represented by properly educated and ideologically trained public administration, on the one hand, and members of a society with similar qualities, on the other. The technical side of cybersecurity depends on the state's economic development and determines relevant models. At the same time, under the need to fight corruption in pandemic and the post-pandemic order, only societies with an appropriate level of information literacy and culture and deep respect to both traditional values and modern development may support and improve the progressive and efficient implementation of a national cybersecurity policy.

The materials in this article may be useful for researchers aiming to modernize the current cybersecurity system to respond to emerging challenges. However, in the research process, new questions and issues arose that are needed to be solved. Therefore, it is necessary to continue the investigation of methods and details of the effective practical implementation of a cybersecurity policy and its enhancement in the face of technological developments and corruption risks.

[34] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity" *American Journal of International Law* 110, no. 3 (2016): 425-479, https://doi.org/10.1017/S0002930000016894.

Disclaimer

The views expressed are solely those of the authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.

About the Authors

Bohdan M. Holovkin is a Doctor of Legal Sciences and Professor in the Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.
https://orcid.org/0000-0002-0333-9806

Oleksii V. Tavolzhanskyi is with the Department of Criminology and Criminal and Executive Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.
E-mail: tavolzhanskyi8020@sci-univ.com

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