UNIFIED DIGITAL LAW ENFORCEMENT ENVIRONMENT – NECESSITY AND PROSPECTS FOR CREATION IN THE "BRICS COUNTRIES"

EVGENII NIKITIN,

South Ural State University (Chelyabinsk, Russia)

MENSAH COCOU MARIUS,

University of Maribor (Maribor, Slovenia)

https://doi.org/10.21684/2412-2343-2020-7-2-66-93

The article examines the prospects for the development of an interstate association of BRICS member nations and concludes that it is necessary to expand cooperation in addition to the economic sphere through other areas, in particular, the organization of interaction to combat crime. The article focuses on the fact that an important area of joint cooperation between the BRICS member nations will be activities in the field of security and combating crime. The main promising areas of cooperation between the BRICS member nations in the field of security are formulated and forms of joint activities in these areas are proposed. This area of cooperation of the BRICS member nations should be based on modern information technologies, which is due to the need for coordination of law enforcement activities of the BRICS member nations. The article analyzes the joint system for preventing international crime in the BRICS member nations and concludes that no improvement of this system is possible without appropriate information support for law enforcement based on general principles and approaches. To this end, the necessity of creating a Unified Digital Environment for Law Enforcement Services in the BRICS member nations is substantiated, which implies the speed of achieving the objectives of law enforcement in the BRICS member nations; reduction of corruption risks in this area; as well as automation of individual work processes by replacing a human resource with software. The article describes the concept of a Unified Digital Environment for Law Enforcement Services of the BRICS member nations, substantiates the components that make up its structure. The modern methods of information processing that can be used to build the specified information system are presented. Possible interested users of this environment are highlighted and the capabilities of the Unified Digital BRICS Law Enforcement Services Environment provided to these users are presented.

Keywords: digital law; digitalization of law; information technology; law enforcement; BRICS; international cooperation; fight against crime; law digital environments.

Recommended citation: Evgenii Nikitin & Mensah Cocou Marius, *Unified Digital Law Enforcement Environment – Necessity and Prospects for Creation in the "BRICS Countries*," 7(2) BRICS Law Journal 66–93 (2020).

Table of Contents

Introduction

BRICS is currently the most influential association of states created on an economic basis. The unification of Brazil, India, China, Russia, and South Africa was made possible thanks to the promising economic indicators and economic growth rates of these countries. In the economic sphere, the BRICS member nations are integrated and mutually complementary. Russia is the largest exporter of energy resources, the agricultural industry is developed in Brazil, China is the leader in human capital and information technology, industry and services are developed in India, and South Africa has experience in the "green industry," tourism is developing, and the country is rich in minerals. Experts say that

> South Africa is the most prolific producer of patents in the African continent.[1]

[1] Xolani Makhoba & Anastassios Pouris, *A Patentometric Assessment of Selected R&D Priority Areas in South Africa: A Comparison with Other BRICS Countries*, 56 World Patent Information 20, 20 (2019).

Each of the BRICS member nations has a number of inherent characteristics that make it attractive to other members of the association.

China occupies a special role in the BRICS format. There is no doubt that the People's Republic of China has become a center of power, having the largest population worldwide, a permanent seat on the U.N. Security Council, the official status of a nuclear power, and being second in the world in terms of gross domestic product. In addition to all this, Chinese researchers use the concept of "total national power," which they calculate by comparing quantitative and qualitative assessments of the territory, natural resources, military potential, economic development parameters, diplomatic influence, international prestige, national cohesion, cultural impact on other countries, etc. The role of China is also increasing in the accumulation of "intellectual capital." As W. Cheng notes,

> As China becomes the second largest economy in the world, there have been increasing domestic demands requesting China to engage with the global governance of various issues more closely. In intellectual property (IP), China has recently engaged with global IP governance both responsively and actively.

This paper answers the questions (a) how did China respond to the global IP up-ratchet which sets higher IP standards; and (b) how did China actively promote its agenda for the global IP governance. This paper argues that China has a clearer and more consistent position in its responsive engagement than in active engagement. In other words, China is more affirmative in making defensive coalitions opposing TRIPS-plus standards proposed by developed countries than promoting its own IP initiatives regionally or plurilaterally. China's positions in these defensive coalitions are the classic pro-development, developing country positions. Its active IP engagement is more diversified. Specifically, China keeps a low profile and does not attempt to take the lead in IP negotiations at the Regional Compressive Economic Partnership. By contrast, China has emerged as a model exporter, focusing on IP capacity building in its IP arrangements in the Belt and Road Initiative (BRI) and BRICS.[2]

What unites these countries, which are so different at first glance? All BRICS member nations have a strong and not unreasonable conviction that the "collective" West, led by the United States, is not only not interested in the rapid growth of their economy and, especially, in its diversification and modernization, but also deliberately prevents it, seeks to keep these countries relatively lagging behind the western level.

The policy of the BRICS nations is aimed at playing a significant role as regional leaders in their region. The same with certain specifics can be said about the policy

---

[2] Wenting Cheng, *China Engages with the Global Intellectual Property Governance: The Recent Trend*, 22(3-4) Journal of World Intellectual Property 146 (2019).

of China in East and Central Asia, the policy of India in South Asia, which would like to neighbor friendly countries. Brazil does not see anything reprehensible in striving to play the role of a regional leader in South America. Finally, South Africa hardly has the resources to be the leader of the entire African continent, given the presence of such countries as Nigeria, however, it is not only striving for the leading country in the southern part of the continent, but already is.

However, the BRICS association is gradually going beyond the scope of only economic cooperation and acquiring the features of institutionalization of supranational education. The logic of the stages of the unification of the BRICS member nations demonstrates rapprochement in various areas of interstate cooperation. Foreign authors recognize the growing influence of the BRICS member nations in solving global problems. F. Petrone, in relation to the climate problem, notes that if the BRICS stand out as leaders on these issues, and inspire changes that allow the world to obtain out of the gridlock, they will also gain more importance in terms of soft power and more credibility internationally. It is a difficult challenge, but the 'decline' of the West could open these paths up to them. This process is under way, either because the BRICS are already starting to expand their economic power, or because they have the need to act as models.[3]

Other scientists using sociological research methods write the following:

> Based on literature review and interviews with journalists, we argue that the BRICS member nations are constructing a collective vision, guided by logics of recognition and of transformation. The production of discourse reaches its high point during the BRICS leaders' summits. To go beyond analysis of the discourse revealed in the media, this article examines projects, thereby aiming to qualify and label the justificatory discourses, in order to develop an understanding of intentions. The BRICS member nations have become a reference point as the press increasingly makes comparisons between these countries. The notion of recognition present in the political elites also appears as a part of the public imagination and in the press. The leaders too seek transformation. The first official multilateral institution founded by the BRICS member nations was the New Development Bank. Current efforts indicate the development of common scientific and technological research initiatives and official support for the establishment of an innovative BRICS Network University. Initiatives will appear as these countries try to consolidate their position.[4]

---

[3] Francesco Petrone, *BRICS, Soft Power and Climate Change: New Challenges in Global Governance?*, 12(2) Ethics & Global Politics 19, 27 (2019).

[4] Tom Dwyer & Olivier Arifon, *Recognition and Transformation: Beyond Media Discourses on the BRICS*, 15(1) Global Media and Communication 27, 27–28 (2019).

These points of view indicate that the cooperation of the BRICS member nations has gone beyond the framework of the economy and is rapidly developing in other areas of cooperation.

1. Directions and Forms of Joint Activities of the BRICS Member Nations in Law Enforcement

These countries are playing an increasingly important role in building a multipolar world and solving problems, including ensuring the external and internal security of these countries. P. Røren and P. Beaumont note:

> An impressive portfolio of case-study research has now demonstrated how and through what means the BRICS (Brazil, Russia, India, China, South Africa) countries have sought higher social status.[5]

The governments of the BRICS member nations have developed a joint vision of the goals and principles of activity in the field of not only the economy, but also in the field of ensuring security and combating crime. Therefore, the need has ripened for closer cooperation in law enforcement. Successful experience in the cooperation of the BRICS member nations in the economic sphere with the same approaches and principles allows us to count on success in international cooperation in the field of security. A study of the final documents of the BRICS summits allows us to formulate the following areas of cooperation in ensuring security:

1. Countering international terrorism. Terrorism in itself as a negative social phenomenon carries an increased social danger. Also the unstable environment in the field of public safety affects the economic performance of the BRICS member nations. As M. Balcilar, M. Bonato, R. Demirer and R. Guptab note:

> Noting that geopolitical shocks and in particular terrorist incidents are largely unanticipated, our findings underscore the importance of a strong financial sector that can help return the market to stability and an open economy that allows local investors to diversify country-specific risks in their portfolios.[6]

In modern conditions, the BRICS act as a group of economic cooperation and their interaction of these countries in the fight against international terrorism represents a significant consolidating factor for the effective counteraction to terrorism at

---

[5] Pel Røren & Paul Beaumont, *Grading Greatness: Evaluating the Status Performance of the BRICS*, 40(3) Third World Quarterly 429, 429 (2019).

[6] Mehmet Balcilar et al., *Geopolitical Risks and Stock Market Dynamics of the BRICS*, 42(2) Economic Systems 295, 295–296 (2018).

the global and regional levels. At present, Russia, China, Brazil, South Africa, and India have not been able to create an effective system of joint counter-terrorism activities, therefore, there are reserves for improving the regulatory, organizational, and other components of cooperation in countering international terrorism. These reserves are seen in an increase in the forms of international cooperation in the fight against terrorism, which should correspond to modern forms of domestic counter-terrorism activities. Here are some of the possible forms of joint activities of the BRICS member nations in the field of combating terrorism: conducting joint counter-terrorism operations; considering the issues of operational compatibility of the forces conducting counter-terrorism operations; conducting agreed preventive measures; cooperating in eliminating the consequences of terrorist attacks and emergency situations and minimizing damage from them; organizing and conducting joint anti-terrorism exercises, training, the exchange of positive experience law enforcement activities and information on combating terrorism, separatism and extremism; conducting joint scientific research in this area; cooperation in the field of armaments; border control; preventing the financing of terrorism; illegal trafficking in weapons and explosives;

2. Combating smuggling and illegal migration. The organization of interaction between the BRICS member nations in the direction of countering smuggling is becoming increasingly relevant. This is due to circumstances such as relative transparency of borders, weak customs control over the movement of goods, and inconsistency between the laws in force in different countries that regulate the rules for the movement of goods and foreign economic activity. The measures taken to combat smuggling are clearly insufficient and inadequate in the current situation, and international agreements aimed at combating smuggling are far from being fully implemented in practice. In the desire of states to create a tough mechanism for controlling the movement of goods there was no coordination to lead to the simultaneous operation of many international and domestic regulatory legal acts. This significantly impeded the functioning of the entire system of international regulation of counteraction. In addition, a number of provisions of existing international agreements are objectively outdated. Separately, it should be noted the problem of illegal movement across the state borders of the BRICS member nations of items restricted and prohibited in free civil circulation (drugs, weapons, etc.), while the rapid growth of illegal drug trafficking and crimes against public safety has become a serious problem for some countries.

The need to concentrate efforts in the field of countering smuggling on strengthening border lines is obvious, therefore we consider it necessary to conclude special agreements with the BRICS nations on cooperation between law enforcement agencies of the border regions. This circumstance is also due to the fact that three countries (Russia, India, China) from the five BRICS member nations have common borders.

As for the problems of illegal migration, not only the BRICS member nations, but countries around the world suffer from it. International cooperation on border security is diverse and includes measures to facilitate the legal movement of goods, stop crime, maintain security around borders and protect natural resources. All these operations are vital and necessary, however, at present, three areas are of particular concern to the BRICS member nations: the fight against terrorism, illegal drug control and illegal migration. Effective counteraction to these illegal phenomena is possible with the optimal organization of flight routes over the border for monitoring and opens up new possibilities for both military and civilian purposes, such as border monitoring and remote sensing.

Many systems have been developed to provide border authorities with more effective oversight and robust decision support. Such systems differ in the technology used, the accuracy, the types of events that can be detected and the continuity of monitoring. The article by a group of scientists entitled "Assessing the Effectiveness of Flying Ad Hoc Networks for International Border Surveillance" explores the technical capabilities of existing and new surveillance technologies used for international border monitoring. The efficiency of these systems is described, as well as the technological infrastructure necessary for their implementation. Particular attention is paid to identifying the strengths and weaknesses of these systems and their ability to solve current and future tasks. It notes that

> flying ad hoc networks can be used to deliver a rapidly deployable, self-configurable, flexible and relatively small operating cost network for border surveillance.[7]

3. Combating organized crime, which includes the most dangerous types of illegal activities (drug trafficking, human trafficking, arms trafficking, etc.). A particular problem is the illegal distribution of drugs due to the negative impact on the health of the population. In this regard, the BRICS member nations should take a tougher stance on this issue. This is emphasized in the foreign press.[8]

Modern organized crime is characterized by a high level of professionalism and the ability to control the financial systems of states. It is a new globalized criminal system that takes full advantage of the most modern information technologies. Already, organized criminal groups have the ability to operate with huge amounts of money, in fact they threaten the ability of the BRICS member nations to exercise financial control over their economies. Ultimately, organized crime groups will have the opportunity to buy up state institutions, control revenue-generating sectors of the economy and trade

---

[7] Fayez Al Fayez et al., *Assessing the Effectiveness of Flying Ad Hoc Networks for International Border Surveillance*, 15(7) International Journal of Distributed Sensor Networks 7, 7–8 (2019).

[8] Khalid Tinasti & Isabela Barbosa, *The Influence of Global Players on the Drug Control System: An Analysis of the Role of the Russian Federation*, 17(2) Drugs and Alcohol Today 124 (2017).

zones, undermine existing financial markets, acquire weapons, ammunition, explosive devices (including nuclear devices). It is no secret that obtaining nuclear weapons is an integral part of the strategy of all major international terrorist organizations. This is necessary for them to obtain effective means to intimidate the population and influence on the decision-making of public authorities of various countries. It is clear that the integration of criminal groups should be opposed to even stronger integration of law enforcement agencies of various states;

4. Anti-corruption. The relevance of this problem in the BRICS member nations is emphasized in the modern scientific research, in particular by Indian scientists:

> incidents of corruption enhance environmental degradation by reducing the positive impact of renewable energy consumption on environmental quality, and increasing the negative impact of fossil fuel consumption. This study has also divulged that the corruptive practices are more prone in case of the countries, where the development is mature and institutionalization is more stringent.[9]

The problem of corruption in the BRICS member nations is also noted by other scientists:

> Corruption is a global challenge which may impact negatively on economic growth and sustainable development of the BRICS member nations (Brazil, Russia, India, China and South Africa). All of these five countries have been held back by corruption in varying ways, but their rising importance to the global economic system ensures the spotlight now shines brighter than ever on them. Yet some of the BRICS member nations have handled the issue better than others. According to Transparency International's Corruption Perception Index (2017), in the BRICS bloc of major emerging economies, South Africa is ranked the best (71st), followed by China (77th) and India (81st), with Brazil is 96th and Russia 135th out of 180 countries. These five nations support the strengthening of international cooperation against corruption, including through the BRICS Anti-Corruption Working Group, as well as on matters related to asset recovery and persons sought for corruption.[10]

5. Ensuring information security of the BRICS member nations. In recent years, there has been an alarming increase in the number of cyberattacks on the infrastructure of various countries of the world. An important area of cooperation is ensuring

---

[9] Avik Sinha et al., *Impact of Corruption in Public Sector on Environmental Quality: Implications for Sustainability in BRICS and Next 11 Countries*, 232 Journal of Cleaner Production 1379 (2019).

[10] Alexey Kurakin & Alexander Sukharenko, *Anti-Corruption in the BRICS Countries*, 5(1) BRICS Law Journal 56, 56–59 (2018).

cybersecurity of the BRICS member nations. Given the current unstable socio-political situation and the massive increase in terrorist attacks, it is imperative that BRICS law enforcement agencies recognize the possibility of terrorist organizations using cyberspace to disrupt a normal lifestyle. The level of the threat of cyber terrorism is higher than ever today and this creates many problems, spreads uncertainty and fear among citizens. It is unlikely that this problem can be effectively resolved without cooperation between the BRICS member nations.

As noted by Z. Mitrovic and C. Thakur from Durban University of Technology (Durban, South Africa):

> a number of reports in the last two years revealed that the BRICS economies (Brazil, Russia, India, China and South Africa) were found to be amongst the largest victims of cybercrimes. The recent BRICS summit, held in Xiamen, China, had as one of the main themes of global security, including cybersecurity. Consequently, The BRICS leaders called for a coordinated strategic action in these areas, driven by the requirements and priorities.[11]

Cybersecurity in the area of big data should also be given increased attention. When committing a computer offense, law enforcement agencies need to conduct digital forensics, collect digital evidence, determine the place of the offense, detect intent on its commission and calculate possible negative consequences. All these issues have not been given a definite solution in different countries, and therefore there should be interaction between the BRICS member nations on general principles and legal grounds in this area. These problems are actively dealt with by Chinese scientists who note:

> As a new research area, Digital Forensics is a subject in a rapidly developing society …
>
> The Smart City technique is making use of ICT (information communications technology) to collecting, detecting, analysing and integrating the key information data of core systems in running the cities. Meantime, the control is making intelligent responses to different requirements that include daily livelihood, PII (Personally identifiable information) security, environmental protection, public safety, industrial and commercial activities and city services. The Smart City data are Big Data, collected and gathered by the IoT (Internet of Things).

---

[11] Zoran Mitrovic & Colin Thakur, *Positioning South Africa in the BRICS Cybersecurity Context: A Strategic Perspective*, Conference Paper, 14th International Conference on Cyber Warfare and Security ICCWS 2019, Stellenbosch, South Africa, 28 February – 1 March 2019 (Mar. 20, 2020), available at https://www.researchgate.net/profile/Zoran_Mitrovic3/publication/331438637_Positioning_South_Africa_in_the_BRICS_cybersecurity_context_a_strategic_perspective/links/5c865423458515831f9b5a02/Positioning-South-Africa-in-the-BRICS-cybersecurity-context-a-strategic-perspective.pdf.

> This paper has summerised our review on the trends of Digital Forensics served for Big Data. The evidence acquisition challenge is discussed. A case study of a Smart City project with the IoT collected services Big data which are stored at the cloud computing environment is represented. The techniques can be generalised to other Big Data in the Cloud environment.[12]

6. Providing legal assistance and ensuring the safety of tourists. Tourism between the BRICS member nations is important from the point of view of developing the economic potential of these countries. A study by U.J. Banday and S. Ismail highlights that

> tourism has been a new dimension in economics of international trade in the recent years for developing countries. It contributes to the economic growth by contribution to the foreign exchange for many nations. The present study is an attempt to examine the relationship between tourism revenue, economic growth and its implications for the environment. Panel data approach for the period of 1995–2013 has been applied to the BRICS countries to investigate the interrelationship among variable using ARDL co-integration model. The result validates "tourism led-growth hypothesis" for BRICS countries which implies that the growth of tourism in BRICS nations has a positive impact on economic growth. The study further reveals that the growth in tourism leads to both positive and negative effects on the economy over time. The study used renamed Environmental Kuznets Curve to reveal that not all environmental controlling measures improve but only pollution controlling measures helps improving income. The study concludes that growth in tourism generates negative externalities in the form of pollution, which needs to be addressed by the government to enhance sustainability in economic growth and development in BRICS nations.[13]

7. Legal support and ensuring the security of high-tech and business activities in the BRICS member nations, including with the use of information technologies. As noted in studies:

> there is no single path of technology upgrading. Instead, we find several unique paths with different trade-offs between intensity, structural change and the nature of the global interaction. All BRICS economies display increased

---

[12] Xiahua Feng & Yuping Zhao, *Digital Forensics Challenges to Big Data in the Cloud* (Mar. 20, 2020), available at https://core.ac.uk/download/pdf/82971343.pdf.

[13] Umer J. Banday & Saba Ismail, *Does Tourism Development Lead Positive or Negative Impact on Economic Growth and Environment in BRICS Countries? a Panel Data Analysis*, 37(1) Economics Bulletin 553, 553–560 (2017).

> generation of frontier technological activities, while China and Russia have also increased the intensity of behind frontier technological activities. China has also diversified its technology knowledge base and entered into dynamic frontier areas. With increasing intensity of frontier technology activities of the BRICS, the relative, but not absolute, the importance of foreign actors and international collaboration has declined. However, BRICS economies seem to lack the organisational and complementary capabilities to match the extent technology sourcing from abroad, observed in high-income countries. Our result represents the application of a new conceptual framework and contributes to assessing the sustainability of innovation-based growth among BRICS.[14]

The forms of joint activities in these areas are diverse:

1. The creation of a joint legal information base of regulatory legal acts of the BRICS member nations;

2. The use of joint technological developments and attracting international cooperation for the implementation of activities in the field of combating crime and ensuring the security of citizens of the BRICS member nations;

3. The development of a joint infrastructure and material base of security systems for the BRICS member nations;

4. The exchange of knowledge and successful experience in law enforcement and the fight against crime. States face common challenges in ensuring the security of citizens, therefore, the exchange of experience benefits the BRICS member nations and makes it possible to share best practices in law enforcement and to unify security standards in the future. Since it is obvious that cooperation of one type of system is more productive;

5. Maintaining working relations between law enforcement agencies in the BRICS member nations through the mutual exchange of law enforcement officials abroad to assist in the disclosure and investigation of all types of transnational crime, including crimes in the field of terrorism;

6. The creation of an effective and safe system for supporting business activities in the BRICS member nations;

7. The creation of management and monitoring systems based on information and communication technologies in the fields of ensuring public safety.

Of course, the list of areas and forms of joint activity is not exhaustive and is constantly expanding; more obvious is the need for coordination of law enforcement activities of the BRICS member nations based on modern information technologies. Moreover, many specialists talk about areas of joint technological interaction:

---

[14] Iciar Dominguez Lacasa et al., *Paths of Technology Upgrading in the BRICS Economies*, 48(1) Research Policy 262 (2019) (Mar. 20, 2020), available at https://www.eco.unicamp.br/Neit/images/destaque/TEXTO_12.03_2019_Lacasa_Jindrab_Radosevic_Shubbak.pdf.

All BRICS economies display increased generation of frontier technological activities, while China and Russia have also increased the intensity of behind frontier technological activities. China has also diversified its technology knowledge base and entered into dynamic frontier areas. With increasing intensity of frontier technology activities of the BRICS, the relative, but not absolute, the importance of foreign actors and international collaboration has declined. However, BRICS economies seem to lack the organisational and complementary capabilities to match the extent of technology sourcing from abroad, observed in high-income countries.[15]

2. Digitalization of the Joint Activities of the BRICS Member Nations

Digitalization is becoming a key factor in the progressive development of both for individual states and for alliances of states. The global economy is in transition period from the simple introduction of digital technology to the integrated construction of a digital system on the scale of all civilized countries. The digitalization of all spheres of human activity is primarily aimed at ensuring the full and effective use of information for the optimal solution of the tasks of this activity. Jurisprudence in general, and law enforcement, in particular, cannot remain indifferent about this innovative historical process. If they do, the gap between innovative and traditional spheres of human activity will widen, damaging the security of the BRICS member nations.

The potential of modern information technologies is becoming a new factor in the national power of states along with traditional indicators such as territory, population, level of economic development, and combat readiness of the armed forces. Informatization is moving into a new role – from an object of legal regulation into a subject. Previously, states regulated public relations in the field of informatization, but now informatization has an impact on the state itself and the system of regulation of public relations by this state. This was made possible thanks to the introduction of information systems united under the name of "artificial intelligence" in the sphere of regulation of public relations and human activity management.

The introduction of information technology in the traditional spheres of human activity contributes to the positive development of these areas, which means the progress of society as a whole. For example, information and communication technologies have a significant impact on the development of traditional industries. In Russia, the volume of sales of goods and services to Russians using the Internet in 2015 reached the equivalent of 2.3 percent of gross domestic product and has a tendency to increase.

The basis of management in any area of human activity is the information received. The correct organization of human activity (whether it is on state management,

[15] Dominguez Lacasa et al. 2019.

interaction between states, ensuring security or planning a tourist trip) is based on the analysis of the necessary information. The main problem is that sometimes it's hard to obtain complete, high-quality, and reliable information to make any decision at any level.

In our opinion, the informatization of public authorities and citizens at this stage has the following disadvantages:

1. Limited circle of users of existing information systems. Each state and law enforcement agency has its own closed information system to improve the efficiency of its own activities, which is designed to work for a limited circle of users. Moreover, there is no need to talk about cooperation within the framework of different states;

2. Incompatible software and hardware. In existing information systems, the information technologies and technical means used are poorly compatible with each other within the framework of one state, and there is no question of coordinating this software and hardware in different countries;

3. The large number of information resources. In Russia, a large number of state and commercial information and reference systems have been created, which contain information of varying completeness and reliability based on which it is difficult to make the best decision;

4. Traditional statistical methods usually employed to analyze information and based on which decisions are usually made cannot efficiently process a continuous flow of information because of the volume. A large amount of such information, including information received on-line from devices connected to the network, fundamentally changes the approaches to processing such information;

5. The low level of information provided. Sites and portals often do not meet modern requirements for the quality and convenience of providing services on the Internet, use information that duplicates each other, unrelated navigation systems, various visual and graphic designs and models for presenting information, do not comply with regulatory acts regulating this area of activity;

6. Lack of modern information technology in individual countries. In the strategy for the development of the information society in Russia for 2017–2030 (approved by Decree of the President of the Russian Federation of 5 December 2017 No. 203) it is noted: states whose sectors of the economy are based on technologies for analyzing large amounts of data have a competitive advantage on the world market. Such technologies are actively used in Russia, but they are based on foreign developments. Domestic analogues are currently absent. The widespread introduction of foreign information and communication technologies, including those at critical information infrastructure facilities, complicates the solution of the problem of protecting the interests of citizens and the state in the information sphere. With the use of the Internet, computer attacks are increasingly being made on public and private information resources and on critical information infrastructure objects.

However, the leader in modern information technologies is China, including in terms of ensuring security using artificial intelligence technologies. As C.C. Demchak notes:

> China is chasing dominance in emerging artificial intelligence (AI) technologies in both the private and military sectors, as a central part of its effort to be the leading global cyber power. The rise of AI – a subset of cyber as are machine learning, quantum computing, and other new technologies – does not herald a new arms race equivalent to that of the Cold War. Rather, the concern should be on the profound disruption to the existing westernized global order. This piece reviews how the 1990s westernized national creation called cyberspace created so many ubiquitous, embedded vulnerabilities whose easy exploitation directly accelerated the rise of an otherwise impoverished authoritarian and aggressive China. Today no single democracy has the scale and sufficient resources to alone match the foreknowledge and strategic coherence of the newly confident and assertive China. To change current global trends, the small group of consolidated democratic civil societies needs a collective approach to counter China's growing dominance across all fields of cyberspace. The piece ends describing the Cyber Operational Resilience Alliance (CORA) to provide the public and private scale and collective strategic coherence required to ensure the future wellbeing and security of democracy in an overwhelmingly authoritarian, post-western, cybered world.[16]

7. International legal mechanisms to defend the sovereign right of states to regulate the information space, including in the national segment of the Internet, have not been established. Most states are forced to "adapt" state regulation of information and information technology to new circumstances.

All these shortcomings and limitations of existing information systems necessitate the creation of a unified information system based on common approaches and principles. A common (uniform) information system should be open, i.e. ensure the integration of available computing resources with the possibility of further expansion, improvement, and logical integration with similar systems. Therefore, it is necessary to streamline the algorithms for data processing and access to such data. The system must contain quality information, i.e. special requirements must be presented to its openness, efficiency, reliability, and completeness.

Ensuring effective cooperation in the field of ensuring public safety is becoming one of the main tasks of the BRICS member nations and its implementation is difficult without creating a Unified Digital Environment for Law Enforcement Services of

---

[16] Chris C. Demchak, *China: Determined to Dominate Cyberspace and AI*, 75(3) Bulletin of the Atomic Scientists 99, 99–104 (2019).

the BRICS member nations. The creation of a Unified Digital Environment for Law Enforcement Services in the BRICS member nations will have a positive impact on the interaction and cooperation of these nations, and will more effectively achieve the goals that determined the creation of this interstate association, including the intensification of trade and economic cooperation. The Unified Digital Environment should become an effective infrastructure for ensuring multilateral interaction between officials and citizens in the sphere of law enforcement. The conceived functionality of the Unified Digital Environment is that it should create mechanisms for developing comprehensive cooperation among the BRICS member nations, supporting joint law enforcement projects, and creating tools to ensure the security of entrepreneurial activity, thereby help strengthen economic relations between the BRICS member nations.

What should be the BRICS Unified Digital Law Enforcement Environment? There is a certain set of interconnected components of which it consists, providing system integration of growing volumes of information and information technologies in law enforcement activities in order to optimally ensure the security of the BRICS member nations and manage this process. Additionally, this Unified Digital Environment of law enforcement services of the BRICS member nations should also become the optimal management resource in this area.

3. Structure of the BRICS Unified Digital Law Enforcement Environment

As a system, the Unified Digital Law Enforcement Environment of the BRICS member nations should logically combine the following components:

1. Technical and methodological component, which includes: a) modern methods of information processing and b) technical and software environment;

2. User component that includes interested participants in the specified environment;

3. Resource component – opportunities provided to users of the environment.

3.1. Technical and Methodological Component of the BRICS Unified Digital Law Enforcement Environment

Let us consider the first technical and methodological component of the BRICS Unified Digital Environment. The unified information environment should utilize modern methods of information processing which are successfully applied in various fields of human activity, but are not widely used in ensuring security and law enforcement. All these methods can conditionally be attributed to the tools of "artificial intelligence." Among the techniques for the information environment that will allow it to perform its tasks, the following are relevant: "Big data," "Deep learning," "Data Mining," "LegalTech."

The "Big data" information technique consists in processing huge amounts of data to obtain human-perceived results, in the face of a continuous increase in these

data. This technology can be used in the law enforcement activities of the BRICS member nations, for example, the prevention of criminal activity on the Internet, the identification of banking and other economic crimes, the suppression of illegal trafficking in prohibited items, countering illegal migration, etc. Abroad, the Big Data information processing technology is promoted by such authors as T. Hoeren,[17] R. Smolan and J. Erwit,[18] S. Raschka.[19]

An example of the use of modern information technologies for processing big data to determine the level of crime in a given area is a technology developed by American scientists. Their article notes:

> Crime is one of the most important social problems in the country, affecting public safety, children development, and adult socioeconomic status. Understanding what factors cause higher crime rate is critical for policy makers in their efforts to reduce crime and increase citizens' life quality. We tackle a fundamental problem in our paper: crime rate inference at the neighborhood level. Traditional approaches have used demographics and geographical influences to estimate crime rates in a region. With the fast development of positioning technology and prevalence of mobile devices, a large amount of modern urban data have been collected and such big data can provide new perspectives for understanding crime. In this paper, we use large-scale Point-Of-Interest data and taxi flow in the city of Chicago, IL in the USA. We observe significantly improved performance in crime rate inference compared to using traditional features. Such an improvement is consistent over multiple years. We also show that these new features are significant in the feature importance analysis. The correlations between crime and various observed features are not constant over the whole city. In order to address this geospatial non-stationary property, we further employ the geographically weighted regression on top of negative binomial model (GWNBR). Experiments have shown that GWNBR outperforms the negative binomial model.[20]

As noted above, for making optimal decisions, the system must contain high-quality information. In times of "fake news," separating truth from lies can be problematic. It becomes possible to obtain reliable information with the help of modern information

---

[17] Thomas Hoeren, *Big Data and the Legal Framework for Data Quality*, 25(1) International Journal of Law and Information Technology 26 (2017).

[18] Rick Smolan & Jennifer Erwit, *The Human Face of Big Data* 224 (Sausalito, CA: Against All Odds Productions, 2012).

[19] Sebastian Raschka, *Python Machine Learning* 1–17 (Birmingham: Packt Publishing, 2016).

[20] Hongjian Wang et al., *Non-Stationary Model for Crime Rate Inference Using Modern Urban Data*, 5(2) IEEE Transactions on Big Data 180 (2019).

technologies and the following model developed on their basis. The study of the researchers notes:

> In an era of big data, explosive growth of online posts makes the judgment of their qualities harder while more important. In many cases, people want to quickly identify those most informative posts, which contain details, insights or in-depth criticisms, to help them make better decisions. To meet this demand, a three-stage model is proposed. First, a super-network model is introduced to accommodate the multidimensional attributes of online posts, including keywords, user ID, emotions and the related event. Second, a corpus updating mechanism is introduced to generate event specific corpora, which help to discriminate the informative quality of posts in the next stage. Third, machine learning algorithms are applied, where the posts are first filtered by a linear discriminant classifier and then assessed by a multilayer perceptron neural network. To test the model, we chose six online public opinion events that fell into two categories: major public safety crisis and online controversies about public policies. Experimental results showed the effectiveness of the proposed model, where majority of errors are less than 0.05, on a 0-1 measuring scale. In the future, this model may also be adapted to areas including evaluation of informative quality of websites, product reviews and answers in question and answer communities.[21]

In addition, decisions should be made on the basis of the analysis of "fresh" information, preferably received in real time. Traditional research is mainly based on statistical identification. This is insufficient to find or make the most optimal format of behavior, since with a constantly changing situation and continuous accumulation of information, decisions have to be made based on already outdated data. But at the same time, such problems as the dynamic increase in big data, the relationship between human behavior in micro-vision and public control in macro-vision, as well as the relationship between the perception of data in the real world and the reaction scenario to it, are ignored. Therefore, the provision of public safety and public administration based on real-time big data analysis is becoming a separate area of scientific research in China. As noted in a study by Chinese researchers:

> Real-time big data driven public safety scenario deduction system framework is proposed to find the most optimal emergency decision plan. ACP approach based public safety emergency decision method is proposed to apply the game theory in real. Two specific safety scenarios are chosen to study from evacuation in streets and park, chemical gas leak in ports and chemical

[21] Yuxue Chi et al., *A Supernetwork-Based Online Post Informative Quality Evaluation Model*, 168 Knowledge-Based Systems 10 (2019).

> industrial area. The computational experiments are designed according to the requirements of public safety scenario to apply real-time big data. The main work can be summarized as following: big data collection from internet of things for public safety, multi-paradigm modeling based urban population distribution modeling by big data integration, computational experiments of crowd in specific situations, the applications of emergency decision analysis is for public management. Based on iterations of interactions between micro and macro views, real world and virtual systems, the research can be used to solve the problems in real public management application.[22]

The Unified Digital Environment would obtain additional features thanks to the Deep Learning methodology.[23] Deep learning is a set of machine learning methods based on learning representations using artificial neural networks which make it possible to solve a wide range of problems, for example, in computer vision, machine translation, and speech recognition. The prospects for using these technologies in law enforcement are diverse. For example, searching for persons hiding from law enforcement agencies by monitoring social networks and video recording systems of violations, providing assistance in legal support of entrepreneurial activities, etc.

Due to recent successes in machine learning, especially in the field of statistical training based on big data, the interest of the scientific community, industry, and the public in this area is growing. Industry is investing heavily in AI, and spin-offs and start-ups are appearing at an unprecedented rate. Scientists predict favorable trends in the field of artificial intelligence in general and machine learning in particular:

> For the future, we envision a fruitful marriage between classic logical approaches (ontologies) with statistical approaches which may lead to context-adaptive systems (stochastic ontologies) that might work similarly as the human brain.[24]

The next technology applicable in the unified information environment is Data Mining. The applicability of Data Mining in law enforcement comes down to information sifting, data mining, data extraction, as well as data analysis, i.e. programs

---

[22] Bin Chen et al., *A Public Safety Deduction Framework Based on Real-Time Big Data* in *Theory, Methodology, Tools and Applications for Modeling and Simulation of Complex Systems: 16th Asia Simulation Conference and SCS Autumn Simulation Multi-Conference, AsiaSim/SCS AutumnSim 2016, Beijing, China, October 8–11, 2016, Proceedings, Part III* 547, 574–584 (L. Zhang et al. (eds.), Singapore: Springer, 2016).

[23] Li Deng & Dong Yu, *Deep Learning: Methods and Applications*, 7(3-4) Foundations and Trends in Signal Processing 197 (2014).

[24] Andreas Holzinger et al., *Current Advances, Trends and Challenges of Machine Learning and Knowledge Extraction: From Machine Learning to Explainable AI* in *Machine Learning and Knowledge Extraction: Second IFIP TC 5, TC 8/WG 8.4, 8.9, TC 12/WG 12.9 International Cross-Domain Conference, CD-MAKE 2018, Hamburg, Germany, August 27–30, 2018, Proceedings* 1 (A. Holzinger et al. (eds.), Cham: Springer, 2018).

detecting relevant information in databases to solve specific problems. One of the most important purposes of Data Mining methods is to visualize the results of calculations, especially using geographic information systems. Such visualizations, for example, the location of a particular person, can be used as visual evidence in criminal cases or in the search for missing tourists. These technologies are being studied by such scientists as D. Hand, H. Mannila and P. Smyth.[25]

The Unified Digital Environment should use the technology "LegalTech," which specialize in information technology services for professional legal activities.[26] These technologies allow us to automatically prepare decisions and documents for certain categories of legal issues, analyze judicial decisions, and evaluate the prospects of a legal case. Undoubtedly, the introduction of such technologies will increase the legitimacy and effectiveness of law enforcement agencies, the availability and provision of legal assistance, and the ease of interaction between business entities of the BRICS member nations in solving legal problems.

The technical and software component should include legal decision support systems based on mathematical methods, electronic document management, and interdepartmental interstate electronic interaction capabilities, automated places for users of the Unified Digital Environment, systems of special technical means for automatically recording violations, hardware and software security systems, automated assistants for legal activities and drafting documents.

The Unified Information Environment should be equipped with modern unified intelligent surveillance systems. Recent technological advances have led to the rapid and uncontrolled proliferation of surveillance systems. Under the influence of the urgent requirements of public safety and security, public spaces are equipped with numerous observation systems. However, there are certain disadvantages such as the isolation of these systems, the incompatibility of these systems, and the various owners of these systems. This makes them ineffective in ensuring security and the technological ability to aggregate, control and process multiple video streams from different sources is necessary. To meet these requirements, the and article by the Metropolitan Intelligent Surveillance Systems for Urban Areas by Harnessing IoT and Edge Computing Paradigms combines several approaches and technologies that can be used for the needs of the Unified Digital Law Enforcement Environment. As the authors of this article note:

> To meet these requirements, this paper combines several approaches and technologies, namely the Internet of Things, cloud computing, edge

---

[25] David J. Hand et al., *Principles of Data Mining* 546 (Cambridge, MA: MIT Press, 2001).

[26] Christian Veith et al., *How Legal Technology Will Change the Business of Law*, Boston Consulting Group/Bucerius Law School (January 2016), at 2–13 (Mar. 20, 2020), available at https://issuu.com/jeroenzweers/docs/legal_tech_report_2016.

> computing and big data, into a common framework to enable a unified approach to implementing an ISS at an urban scale, thus paving the way for the metropolitan intelligent surveillance system (MISS). The proposed solution aims to push data management and processing tasks as close to data sources as possible, thus increasing performance and security levels that are usually critical to surveillance systems. To demonstrate the feasibility and the effectiveness of this approach, the paper presents a case study based on a distributed ISS scenario in a crowded urban area, implemented on clustered edge devices that are able to off-load tasks in a "horizontal" manner in the context of the developed MISS framework. As demonstrated by the initial experiments, the MISS prototype is able to obtain face recognition results 8 times faster compared with the traditional off-loading pattern, where processing tasks are pushed "vertically" to the cloud.[27]

To ensure the security and development of the technological component of the Unified Information Environment for Law Enforcement Services of the BRICS member nations, the development of the information infrastructure of the BRICS member nations should be carried out at three levels: a) software; b) information systems and data centers; c) communication networks.

3.2. User Component of the BRICS Unified Digital Law Enforcement Environment

The user component of the Unified Digital Environment should be composed of "functioning zones" for four different user groups:

1. Citizens of the BRICS member nations. The environment should not only facilitate interaction across the entire spectrum of migration problems between countries and BRICS, but also improve the legal framework for cooperation to facilitate the legal contacts of BRICS citizens. For example, in the case of tourist trips, each foreigner will have access to the Unified Digital Environment via login and password with the ability to quickly solve the common issues that tourists usually encounter during their travels abroad. This system should facilitate the communication of citizens with compatriots, legal consultants, law enforcement agencies, and diplomatic representatives of their home countries. In addition, they will gain access to the legal and analytical resources of the system, which will effectively solve every day critical problems in foreign countries.

An interesting experience is informing citizens about emergencies and public order violations through social networks. The widespread introduction of new forms of digital communication platforms provides an opportunity for law enforcement agencies to analyze information from social networks, as well as inform people about

---

[27] Rustem Dautov et al., *Metropolitan Intelligent Surveillance Systems for Urban Areas by Harnessing IoT and Edge Computing Paradigms*, 48(8) Software: Practice & Experience 1475, 1475 (2018).

safe formats of behavior, especially non-standard situations, during mass riots, public events on tourist routes, and measures taken to ensure public order and safety. English scientists conducted a study[28] of public disturbances in England to examine how the police, other organizations and citizens used Twitter in emergencies and what experience they learned from it. This experience can be useful for use in the Unified Digital Law Enforcement Environment of the BRICS member nations;

2. Investors and business entities of the BRICS member nations. Ensuring eco-nomic cooperation is one of the main tasks of uniting the BRICS member nations into one group of states. Of course, this is impossible without the mutual attraction of capital or the creation of a transparent favorable business environment for investors. Access to the relevant resources of the Unified Digital Law Enforcement Services Environment should have a positive effect on creating a favorable investment climate for business entities and creating conditions for the development of electronic interaction between economic activity participants, including financial organizations and government bodies. After all, one of the main tasks of creating this environment is to ensure the security of business, to clarify the legal features of doing business, and to adequately translate the business law of the BRICS member nations;

3. This system will allow law enforcement officials to efficiently and quickly identify, prosecute, and prevent crime, disclose and investigate crimes, and bring those responsible to justice without violating their rights and legitimate interests. In addition, the Unified Digital Environment will improve the quality and efficiency of interaction between law enforcement agencies and units within law enforcement agencies, and will provide access to unified databases and information resources.

In the process of improving the existing mechanisms for cooperation in com-bating cross-border crime, terrorism, and drug trafficking, it is necessary to expand cooperation among law enforcement agencies and work out the issue of creating a single interstate body for cooperation in the field of law and order and security. Looking ahead to the near future, we believe there is a need to create specialized BRICS law enforcement structures analogous to Interpol and Europol. If established, the BRICS police could carry out its activities exclusively in the field of combating common crime, international organized crime, and improving information exchange between national police services. The communications system developed for the exchange of information between the BRICS member countries could become like the Unified Digital Law Enforcement Services Environment, which is based on the most advanced law enforcement information technologies. Having access to the tools of the Unified Digital Environment would allow BRICS law enforcement officials to coordinate joint actions among themselves and conduct joint law enforcement operations, as well as receive the necessary operational information in real time;

---

[28] Rob Procter et al., *Reading the Riots: What Were the Police Doing on Twitter?*, 23(4) Policing & Society 413 (2013).

4. Representatives of government bodies of the BRICS member nations in the field of international relations. For closer cooperation in ensuring the legitimate rights and interests of BRICS citizens, the network of consular posts on a reciprocal basis must be expanded. Solutions to this can arise from the creation of "Electronic Consular Institutions" and the use of the infrastructure of the Unified Digital Environment for the provision of interstate, commercial, and non-commercial services in demand by BRICS citizens electronically.

In addition, information received from users of the environment is also a data processing resource and is intellectually analyzed in the Unified Information Environment to ensure public safety. The collection and analysis of security information from ordinary citizens has become a trend in the era of mobile devices. Involving a wide range of people in solving law enforcement problems on a voluntary basis with the use of information and communication technologies is the dictate of the new times. A sort of informational crowdsourcing using smartphones will make it possible to collect information about public order violations, non-standard situations, and to monitor and evaluate emergencies for preventing and mitigating the effects of natural and public disasters and to ensure public safety. This should be facilitated by the developments of Chinese scientists conducted at Dalian University of Technology (DLUT), consisting in an application urban safety application (application) developed and presented on the Android platform:

> The app acts as a sensor to collect urban data, such as structural acceleration, structural deformation, questionnaires, and images, and implements disaster emergency communications without the use of a network. It then uploads collected data to a website. Subsequently, the urban safety database can be established after the processing of sensed data uploaded by the user. Additionally, verification experiments were carried out at the Dalian University of Technology (DLUT), including displacement monitoring, bridge cable acceleration measurements, and image collection of the DLUT campus buildings. Finally, the experimental results show the feasible and effective use of Urban Safety for safety information monitoring of urban infrastructures.[29]

The Unified Digital Environment of law enforcement services is designed to make interaction between these groups and within them more effective. This should be facilitated by a convenient environment interface programmed for each group, taking into account the specifics of their activities and frequently arising questions and problems, intelligent analysis of user requests, etc. Thus, 16 unique channels of interaction between user groups have to be developed ("citizens" – "entrepreneurs," "citizens" – "law enforcement," etc.).

---

[29] Xuefeng Zhao et al., *Urban Infrastructure Safety System Based on Mobile Crowdsensing*, 27 International Journal of Disaster Risk Reduction 427, 427 (2018).

3.3. Resource Component of the BRICS Unified Digital Law Enforcement Environment

The third "resource" component should logically and systematically combine existing and newly created resources:

1. Databases and records of law enforcement agencies. The arrays of operational reference, search, forensic, statistical, archival, scientific, technical and other information used in operational and official activities should be unified and united for the work of all law enforcement agencies.

In our opinion, the experience of Great Britain in the development and implementation of a corporate integrated information data model for the needs of the police deserves special attention. In the UK, the implementation of these relations during the prevention of offenses and their rapid disclosure is provided by the introduction of the latest computer video surveillance, created through to the financing of city administrations and private enterprises. Since 2013, the National Policing Improvement Agency (NPIA) information system has been transferred to the National Crime Agency (NCA) (National Criminal Agency). Access is available to all UK territorial police forces, Police Service of Northern Ireland (PSNI), British Transport Police (BTP), Scottish Police Service, National Identification Service (NIS), National Crime Agency (NCA), Security Service (MI-5) and Secret Intelligence Service (MI-6), Association of Chiefs of Police (ACPO), and others;[30]

2. Reference and search systems combining BRICS regulatory legal acts and other documents of various levels necessary for successful user interaction and economic activity. Database of law enforcement acts, primarily useful court decisions;

3. Useful legal statistics (including victimological ones), convenient for users, drawn up, for example, in the form of road safety maps, public spaces, and public events.

As noted in the studies, ensuring the safety of tourists is a big issue. However, B.M. Barros Feitoza and J.H. Costa note that for Brazil:

> As conclusions of the study, the research pointed out that, in fact, the spaces intended for tourism do not coincide with those in which homicidal violence prevails, and that the city favors certain spaces that, aimed at tourism demand, are targets of investments and public policies whose objective is to equip them with infrastructure and public safety.[31]

Consequently, with the help of information technologies, it is possible to draw up a safety map of public places in large cities and tourist places where the potential

---

[30] National Crime Agency (Mar. 20, 2020), available at

[31] Betânia M. Barros Feitoza & Jean H. Costa, *Violência urbana, insegurança e turismo na 'Cidade do sol' (Natal/Rn/Brasil)* [*Urban Violence, Insecurity and Tourism in "City of the Sun" (Natal, RN, Brazil)*], 25 Turismo y Sociedad 93, 93 (2019).

for becoming a victim of violence is low or tends to zero. Tourists can be informed about such places in an accessible and convenient way via smartphone. Thus, by processing large crime data, a public safety map of the city or locality is created with sectors shaded by the danger levels of being in these places. Individuals will decide how appropriate it is for them to be in a certain place and create the most secure route when planning walks and trips. In this case, the tourist attractiveness of the cities of the BRICS member nations will increase even in the case of a dubious criminal reputation.

Also of note is a development by Chinese scientists, the "city risk map," which contains a methodology for risk assessment in urban areas based on geo-processing of big data. As they note in their article:

> Regional risk assessment for urban major hazards is significant for environment protection and public safety. In practice, repeating geoprocessing steps required in risk mapping process is quite timeconsuming, and it has been a challenge for both researchers and managers. In this study, we designed and implemented a tool for facilitating the process of urban regional risk assessment. Geoprocessing workflow models are built for severity calculation, vulnerability evaluation and risk mapping respectively. We then integrate these models into an automatic GIS tool, and apply it in a typical urban district of north China to demonstrate its functionalities and utility. The risk map successfully obtained shows that it has potential to be a useful decision support tool for guiding emergency management and urban planning. This work offers new insights and valuable demonstration on promoting future risk assessment with the use of emerging GIS geoprocessing technology in the Big Geo-Data age.[32]

To synchronize the resource component of the Unified Digital Law Enforcement Environment, the use of smart city platforms is a possibility. Smart cities combine advances in the field of the Internet of Things, big data, social networks, and cloud computing technologies with the demand for applications in the areas of public interest, such as public safety and mobility. The ultimate goal is to use urban resources to improve the quality of life of their citizens and ensure their safety. However, achieving this goal requires enhanced support for developing and operating applications in a complex and dynamic environment. Middleware platforms can provide an integrated infrastructure that provides solutions for smart cities by combining heterogeneous urban devices and providing unified, high-level tools for developing security applications and law enforcement services.

---

[32] Ming Zhao & Xiang Liu, *Regional Risk Assessment for Urban Major Hazards Based on GIS Geoprocessing to Improve Public Safety*, 87 Safety Science 18, 18 (2016).

China, for example, has a lot to gain by achieving progress in the development of smart cities. As W. Hu, J. An, S. Chen and X. Lv note:

> With the advent and the rapid development of the next generation of the Internet, Internet of things, cloud computing, big data analysis and other information technology, IBM proposed the slogan of constructing "smart city" in 2008. When more and more serious urban diseases occur such as population expansion, resource shortage, serious environmental pollution, traffic congestion and increasing public safety hazards, etc., it will lead to a helpless feeling for everyone while smart city ideas which are based on the new generation of information technology may bring new urban life expectation for the governments and people. It is with this expectation of the city's sustainable and healthy development that the smart city ideas eventually are accepted by the governments and the people. The smart city construction booms in the world. Smart city is a large-scale joint system consisting of multiple intelligent systems from different industries. It can facilitate enterprises, government departments, financial institutions, telecommunication providers, and public sector organizations to provide better services to residents. Simply speaking, smart city is the integration of the latest information technology such as Internet of Things (IoT), cloud computing and big data technologies, as well as various network platforms.
>
> In this chapter, we first introduce the concepts and characteristics of smart city and then elaborated that constructing smart cities in China is a major strategy in economic, developmental transformation, and an important step towards an innovation-oriented country. The chapter describes as well, with full details, the sub-systems and key technologies of the integrated smart city system.[33]

Conclusion

The integration of the five countries of Brazil, India, Russia, China, South Africa is moving towards a multilateral political alliance to solve the global problems of mankind. Already, the BRICS association has become the center of a multipolar geopolitical concept of world order and in the future, the role of world leaders will only increase. The BRICS member nations are not just carrying out joint activities with focus on a common vision of the goals and principles of the organization of economy, but for ensuring security and combating crime. Therefore, the importance of joint cooperation in law enforcement according to uniform standards and using national effective experience in law enforcement in these countries becomes obvious.

---

[33] Weidong Hu et al., *Key Technologies and Applications for Smart Cities in China* in *Breakthroughs in Smart City Implementation* 87, 87 (L.P. Ligthart & R. Prasad (eds.), Gistrup: River Publishers, 2017).

This cooperation should be carried out in the following areas: countering international terrorism, smuggling, illegal migration, organized crime, corruption, and ensuring information security of the BRICS member nations. New level of problems facing the BRICS member nations requires a qualitatively new approach to solving them. It is necessary to recognize the fact that an individual state is not able to independently solve the most difficult problems of combating international crime in the above areas without cooperation and interaction between law enforcement agencies of different countries. Joint activities in these areas are difficult without the use of modern information technologies.

It goes without saying that information and communication technologies have become a part of modern management systems in all sectors of the economy as well as the fields of public administration, national defense, state security, and law enforcement. However, these systems must be unified on the most important issues of international cooperation. It is necessary combine multilateral resources and potentials to counter external challenges, including international terrorism and transnational crime. In the economic sphere, the use of information technologies will make it possible to effectively use the advantages of individual BRICS member nations due to their complimentary relationship, facilitate access to scientific and technological resources, and enhance information security.

The Unified Digital Environment of law enforcement services could become an effective tool for mutual cooperation, combining the resources of the BRICS member nations, users of the BRICS member nations and modern information processing technologies. The key information technologies of this environment should be the methods of processing big data and using the capabilities of artificial intelligence ("Big Data," "Deep learning," "Data Mining," "LegalTech"). Despite the fact that big data processing technologies have become the subject of business research and management research, these methods are not actively used in public administration. In addition, the studies conducted do not determine what capabilities the BRICS member nations have in place to ensure public safety using big data technologies.

The purpose of creating this new technological basis for developing the BRICS member nations' security sphere is to improve the quality of life of BRICS citizens through the widespread use of information and communication technologies aimed at improving the efficiency of law enforcement, stimulating entrepreneurial activity, attracting investment in the production of innovative technologies, and increasing the competitiveness of the BRICS member nations in global markets as well as increasing the tourist attractiveness of Brazil, China, Russia, India, and South Africa.

To create the Unified Digital Environment for Law Enforcement Services in the BRICS member nations, it is necessary to integrate state standards in the field of information and communication technologies into relevant general interstate standards, as well as to ensure the harmonization of interstate and national systems of standards in the field of law enforcement.

The Unified Digital Environment for Law Enforcement Services of the BRICS member nations is, among other things, an electronic system for BRICS economic entities to submit reports to public authorities. It should logically combine the technical and methodological component of information processing and interested participants in this environment and resources, including the information necessary for users to support their decision-making.

The prompt dissemination of reliable information about various aspects of lawful behavior and threats to personal security in a particular location and under specific conditions, including the data of official statistical accounting in a visual form, is the main function of the Unified Digital Law Enforcement Service of the BRICS member nations for their citizens.

The Unified Digital Environment for BRICS law enforcement services does not only involve new information technologies that allow for the transmission of its users' digital communications. It also supports transparency in the adoption of legal decisions, monitoring of compliance with legal procedure while ensuring the rights and legitimate interests of citizens; efficiency in achieving the objectives of law enforcement in the BRICS member nations; reduction of corruption risks in this area; and automation of individual work processes by replacing human resources with software.

References

Al Fayez F. et al. *Assessing the Effectiveness of Flying Ad Hoc Networks for International Border Surveillance*, 15(7) International Journal of Distributed Sensor Networks 7 (2019). https://doi.org/10.1177/1550147719860406

Balcilar M. et al. *Geopolitical Risks and Stock Market Dynamics of the BRICS*, 42(2) Economic Systems 295 (2018). https://doi.org/10.1016/j.ecosys.2017.05.008

Banday U.J. & Ismail S. *Does Tourism Development Lead Positive or Negative Impact on Economic Growth and Environment in BRICS Countries? a Panel Data Analysis*, 37(1) Economics Bulletin 553 (2017).

Cheng W. *China Engages with the Global Intellectual Property Governance: The Recent Trend*, 22(3-4) Journal of World Intellectual Property 146 (2019). https://doi.org/10.1111/jwip.12122

Demchak C.C. *China: Determined to Dominate Cyberspace and AI*, 75(3) Bulletin of the Atomic Scientists 99 (2019). https://doi.org/10.1080/00963402.2019.1604857

Deng L. & Yu D. *Deep Learning: Methods and Applications*, 7(3-4) Foundations and Trends in Signal Processing 197 (2014). https://doi.org/10.1561/2000000039

Dominguez Lacasa I. et al. *Paths of Technology Upgrading in the BRICS Economies*, 48(1) Research Policy 262 (2019). https://doi.org/10.1016/j.respol.2018.08.016

Dwyer T. & Arifon O. *Recognition and Transformation: Beyond Media Discourses on the BRICS*, 15(1) Global Media and Communication 27 (2019). https://doi.org/10.1177/1742766518818858

Hand D.J. et al. *Principles of Data Mining* (Cambridge, MA: MIT Press, 2001).

Hoeren T. *Big Data and the Legal Framework for Data Quality*, 25(1) International Journal of Law and Information Technology 26 (2017). https://doi.org/10.1093/ijlit/eaw014

Hu W. et al. *Key Technologies and Applications for Smart Cities in China* in *Breakthroughs in Smart City Implementation* 87 (L.P. Ligthart & R. Prasad (eds.), Gistrup: River Publishers, 2017).

Kurakin A. & Sukharenko A. *Anti-Corruption in the BRICS Countries*, 5(1) BRICS Law Journal 56 (2018). https://doi.org/10.21684/2412-2343-2017-5-1-56-77

Petrone F. *BRICS, Soft Power and Climate Change: New Challenges in Global Governance?*, 12(2) Ethics & Global Politics 19 (2019). https://doi.org/10.1080/16544951.2019.1611339

Procter R. et al. *Reading the Riots: What Were the Police Doing on Twitter?*, 23(4) Policing & Society 413 (2013). https://doi.org/10.1080/10439463.2013.780223

Raschka S. *Python Machine Learning* (Birmingham: Packt Publishing, 2016).

Røren P. & Beaumont P. *Grading Greatness: Evaluating the Status Performance of the BRICS*, 40(3) Third World Quarterly 429 (2019). https://doi.org/10.1080/01436597.2018.1535892

Smolan R. & Erwit J. *The Human Face of Big Data* (Sausalito, CA: Against All Odds Productions, 2012).

Tinasti K. & Barbosa I. *The Influence of Global Players on the Drug Control System: An Analysis of the Role of the Russian Federation*, 17(2) Drugs and Alcohol Today 124 (2017). https://doi.org/10.1108/dat-12-2016-0031

Zhao M. & Liu X. *Regional Risk Assessment for Urban Major Hazards Based on GIS Geoprocessing to Improve Public Safety*, 87 Safety Science 18 (2016). https://doi.org/10.1016/j.ssci.2016.03.016

Information about the authors

Evgenii Nikitin (Chelyabinsk, Russia) – Associate Professor, Department of Law Enforcement and National Security, South Ural State University (78 Lenina Av., Chelyabinsk, 454082, Russia; e-mail: nikitinev@susu.ru).

Mensah Cocou Marius (Maribor, Slovenia) – Senior Research Associate, Faculty of Law, University of Maribor (9 Mladinska St., Maribor, 2000, Slovenia; e-mail: cocou.mensah@um.si).