




DOI: 10.22363/2313-0660-2022-22-2-288-302

Research article / Научная статья

Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity

Konstantin A. Pantserev  

St. Petersburg State University, Saint Petersburg, Russian Federation

 pantserev@yandex.ru

Abstract. For almost two decades, Sub-Saharan African countries have been making significant efforts to ensure the rapid development of industries related to information and communication technology (ICTs) in the region. At present, all leading nations are placing greater emphasis on the development of hybrid intelligent systems capable of solving extremely complicated tasks. This includes Sub-Saharan African countries, which consider the development of advanced technologies to be an effective instrument for ensuring sustainable social and economic growth and solving a great number of the continent's problems. It has become evident, however, that all technological novelties that should simplify our lives can be used for malicious purposes. The present study examines existing practices and risks of malicious use of artificial intelligence (MUAI) in Sub-Saharan African countries. At the end of the study, the author comes to the conclusion that the problem of ensuring information, psychological, and cybersecurity is common to all African countries, which creates a serious obstacle for their further sustainable social and economic development. Over the past decade, Sub-Saharan Africa has made significant efforts to elaborate a joint vision for counteracting cybercrimes and the malicious use of advanced technologies. But all the attempts to establish effective supranational instruments that would regulate the fight against cyberattacks at the Pan-African level and take into account the interests of the vast majority of African countries in this area have failed. This demonstrates the presence of serious contradictions among African countries, which, taken together, prevent the establishment of mutually beneficial cooperation even in such an important field as cybersecurity. However, until such cooperation is established, it seems unlikely that African countries will even come close to solving this problem, which means that their information space will continue to be subjected to large-scale cyber-attacks that pose a serious threat not only to the security of individuals, but also to national and Pan-African security.

Key words: artificial intelligence, strategic communication, psychological warfare, information security, cybersecurity, Sub-Saharan African countries


Acknowledgements: This research was supported by the St. Petersburg State University, project No. 93024916 “Artificial Intelligence and Data Science: Theory, Technology, Sectoral and Interdisciplinary Researches and Applications”.



For citation: Pantserev, K. A. (2022). Malicious use of artificial intelligence in Sub-Saharan Africa: Challenges for Pan-African cybersecurity. *Vestnik RUDN. International Relations*, 22(2), 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности

К.А. Панцеров  

Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация
 pantserev@yandex.ru

Аннотация. На протяжении двух десятилетий страны Африки южнее Сахары прилагают значительные усилия, направленные на быстрое развитие информационно-коммуникационных технологий. В настоящее время все ведущие мировые державы уделяют повышенное внимание созданию гибридных интеллектуальных систем, способных решать наиболее сложные задачи. Страны Африки южнее Сахары не остались в стороне от этого процесса. Их правительства убеждены, что передовые технологии являются наиболее эффективным инструментом, способным обеспечить устойчивый социально-экономический рост и решить наиболее насущные проблемы. Однако любые технологические новации, которые призваны упростить нашу жизнь, могут быть использованы и в злонамеренных целях. Настоящее исследование показывает возможные риски злонамеренного использования технологий искусственного интеллекта в странах Африки, расположенных южнее Сахары. Некоторые из этих рисков уже стали реальностью. Автор приходит к выводу, что проблема обеспечения информационно-психологической и кибербезопасности является общей для всех африканских стран. Именно она встает на пути обеспечения дальнейшего устойчивого социально-экономического роста государств рассматриваемого региона. На протяжении последнего десятилетия страны Африки южнее Сахары старались выработать совместное видение борьбы с киберпреступлениями и злонамеренным применением передовых технологий. Однако все их попытки создать действенные наднациональные институты, которые регулировали бы борьбу с кибератаками на panaфриканском уровне и учитывали бы интересы подавляющего большинства африканских стран, провалились. Данное обстоятельство демонстрирует наличие серьезных противоречий среди африканских государств, которые препятствуют установлению взаимовыгодного сотрудничества даже в такой важной сфере, какой является проблема обеспечения кибербезопасности. Тем не менее пока подобное сотрудничество не будет налажено, представляется маловероятным, что африканские страны хотя бы приблизятся к решению данной проблемы, что означает, что они и в дальнейшем будут подвергаться масштабным кибератакам, которые создают серьезную угрозу для личной, национальной и panaфриканской безопасности.

Ключевые слова: искусственный интеллект, стратегическая коммуникация, информационно-психологическое противоборство, информационная безопасность, кибербезопасность, страны Африки южнее Сахары

Благодарности: Статья выполнена при финансовой поддержке СПбГУ, проект № 93024916 «Искусственный интеллект и наука о данных: теория, технология, отраслевые и междисциплинарные исследования и приложения».

Для цитирования: Панцеров К. А. Злонамеренное использование технологий искусственного интеллекта в странах Африки южнее Сахары: вызовы panaфриканской кибербезопасности // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 288—302. <https://doi.org/10.22363/2313-0660-2022-22-2-288-302>

Introduction

Sub-Saharan African countries have become a subject “of global interest with

regards to technological development, leapfrogging and foreign investment, despite the lag in socio-economic development in

comparison with other regions” (Haula & Agbozo, 2020). All leading powers are currently paying increasing attention to research aimed at the creation of hybrid intelligent systems that can solve very complicated tasks. Thus includes the nations of Sub-Saharan Africa, which consider the development of advanced technologies to be an effective instrument for ensuring sustainable social and economic growth and solving many of the problems in the region. It has become evident, however, that all technological novelties that should simplify daily life can be used for malicious intent.

The use of artificial intelligence (AI)-based technologies opens a wide range of possibilities for hackers and provides the possibility for them to go through any cyber defense. Thanks to advanced technologies, hackers can:

- hide malicious codes in official, secure applications;
- affect voice or visual authentication;
- put devices under their control through the use of private keys;
- organize intelligent attacks over systems or networks;
- simulate reliable system components.

With this in mind, the following hypothesis is proposed: any AI technologies can be applied either usefully or maliciously, and it is just a matter of time before all types of criminals become familiar with them. While states should support the development of advanced technologies, they should also ensure that governmental bodies, society, and individuals are not harmed by the misuse of such technologies.

Two main methods are used in this paper: case studies of the level of development in advanced technologies in different Sub-Saharan African countries and critical discourse analysis of different national strategies, road maps, and so on, devoted to the further development and implementation of AI technologies in Africa and ensuring the

cybersecurity of African countries. This method was chosen because critical discourse analysis, as a method, “shows how language works in sociocultural and political contexts, focusing on power relations and ideological perspectives reflected in discourse texts, and their wider implications for the society” (Chiluwa, 2019b). It therefore helps in identifying “social problems expressed or reflected in texts (such as political power abuse, racial discrimination, xenophobia, or terror threats) as one of its main objectives and the possibility of finding solutions to them” (Chiluwa, 2019b).

Using analyses of the existing AI technology initiatives in Sub-Saharan Africa, the paper reveals the most obvious prospective threats. Three questions form the core of the research: What is the current level of development of AI technologies in Africa? Has AI already been used maliciously in Sub-Saharan Africa? What measures should Sub-Saharan African countries undertake to stop the further malicious use of advanced technologies? The author concludes by suggesting the measures necessary for strengthening the information and psychological security of Sub-Saharan African countries.

Literature Review

The current scientific discourse includes a wide range of articles on different aspects of AI,¹ some of which focus on its malicious use

¹ See: Chandler S. Deepfakes 2.0: The Terrifying Future of AI and Fake News // Daily Dot. October 5, 2018. URL: <https://www.dailydot.com/debug/deepfakes-ai-clones-fake-news> (accessed: 04.07.2021); Chesney R., Citron D. Deepfakes and the New Disinformation War: The Coming Age of Post Truth Geopolitics // Foreign Affairs. January/February 2019. URL: <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> (accessed: 04.07.2021); Fillion R. M. Fighting the Reality of Deepfakes // Nieman Lab. 2019. URL: <https://www.niemanlab.org/2018/12/fighting-the-reality-of-deepfakes> (accessed: 30.07.2021).

(e.g., Brundage et al., 2018; Chesney & Citron, 2018; Antinori, 2019; Bazarkina & Pashentsev, 2019; Dack, 2019), while other are devoted to different issues involved in psychological warfare in general and the manipulation of information in particular (e.g., Jeangène Vilmer et al., 2018; Pashentsev, 2019; Bazarkina, Pashentsev & Simons, 2020). There is a lack of research on the development of AI in Sub-Saharan Africa, including the extent to which countries in the region are protected from potential and actual malevolent application of such advanced technologies. The present article intends to fill this gap.

Advanced Technologies in Sub-Saharan Africa: Myth or Reality

The necessity of the development of advanced technologies is considering as the essential condition for the ensuring of the world leadership in the contemporary world. According to Haula and Agbozo (2020), at first glance it appears that African countries face a large number of non-technical problems, such as “civil unrest, corrupt governance, low educational enrolment levels, poor healthcare delivery, a wide digital divide, as well as lacking infrastructure to meet present day global socio-economic demands.” It would seem that the need for AI development must inevitably take a back seat; however, this is not quite true: “Within the past decade, there have been massive shifts in the realization of the role of technology and innovation in contributing to the alleviation of the woes of the sub-region” (Haula & Agbozo, 2020).

African countries see the development of breakthrough technologies as a certain guarantee of their technological sovereignty and are convinced that AI technologies could solve many of the continent’s traditional problems, among others (Artificial Intelligence for Africa..., 2018).

Thus, in agriculture AI technologies could be used to improve productivity and increase

the efficiency of agricultural work. The unmanned aerial vehicles equipped with hybrid intelligence systems could be widely applied in Africa. These drones could be used not only for fertilizing agricultural plantations, but also be equipped with precise sensors that would help in aerial monitoring to detect signs of pests and crop diseases, as well as assess the extent of soil aridity and weed damage. The images obtained from the drones would then be automatically checked and analyzed together with other available data and provide farmers with valuable information about the health of their crops without the need for additional laboratory studies.²

AI technologies could also provide significant assistance in the modernization of the health-care systems of African countries, making medicine in the region more high-tech. One of the main problems of African medical institutions is the lack of qualified medical personnel, and AI technologies could partially solve this problem by providing primary medical diagnostics, and collecting and processing data about the patients and their medical history. The doctor would then be able to receive more patients in one shift. Advanced technologies could also increase the level of medical diagnostics and detect dangerous diseases at an earlier stage, which increase the chance of full recovery. AI would also be useful in providing remote diagnostics to rural areas via chatbots and computer vision, thus providing access to millions of Africans who would not otherwise be able to access medical care. Thus, chatbots, for example, “may minimize hospital visits and assist with triaging before medical consultation. Specially designed AI mobile applications requiring little skills can help in diagnosing birth asphyxia and malaria in the rural areas of Africa where there is a shortage

² Oduma E. How AI Can Transform Kenyan Industries // Ai Kenya. January 21, 2019. URL: <https://kenya.ai/how-ai-can-transform-kenyan-industries> (accessed: 28.07.2021).

of skilled health workers and medical equipment” (Owoyemi et. al., 2020).

AI could also be widely used by African governments and significantly reduce paperwork, improve public sector the efficiency, and speed of public service delivery. This would allow the heads of governmental bodies to solve the problem of resource allocation by redirecting staff where they would be most useful. The predictive capabilities of AI may be of particular importance, as these would allow government officials and policymakers to respond more quickly to societal needs: from preventive intervention by social services to help children and other socially vulnerable segments of the population in difficult life situations, to crime prevention and rapid response in emergencies. Finally, AI-based algorithms could provide citizens with new platforms for assessing the quality, adequacy, and effectiveness of public services, which would provide more effective feedback to the population.

Hybrid intelligence systems could also be used in education to automate the assessments, which would allow teachers to free up time for other important tasks, including additional counseling for students on the subjects studied, preparing for classes, or improving their own skills. AI could also provide additional support to students and offer help with automated tutors and curators to create an individual learning trajectory based on the abilities of each individual student. AI could also be used to monitor student performance and alert teachers of possible academic performance issues, providing useful feedback on course effectiveness.

In this respect, AI is a powerful potential tool to help African countries tackle the continent’s most significant challenges and ensure their sustainable socio-economic growth and transition to an innovation economy. And African countries themselves are striving to conduct their own scientific research in the

field. Thus, a number of startups using technical solutions in the field of AI are already being implemented.

In South Africa, for example, a special data management service called MySmartFarm was launched on 1 June 2012, “which simplifies technology for farmers frustrated by the collection and interpretation of information from multiple sources. It automatically collects all kinds of data and aggregates it with easy-to-use farm management tools’ data, in order to present usable information, advice and predictions for each field on easy to use dashboards and mobile Apps.”³ This start-up quickly became in great demand among South Africans and in 2013 has won IBM’s South Africa SmartCamp award, which supposed support and mentorship from IBM.⁴

Another start-up, the *DroneClouds*, was launched in South Africa in 2015. It “helps farmers increase yield by giving them to-the-point, actionable crop insights using drones, satellite, mobile, the cloud and agro experts.”⁵

In Ghana the start-up *SyeComp* “focuses on enhancing agriculture through ICT and advanced geospatial solutions, research and knowledge management. It specializes in the acquisition, processing, analysis and synthesis of geospatial data from satellites and multispectral drone sensors for various applications using geographic information systems (GIS) and remote sensing (RS) technology. *SyeComp* provides support for various actors across and along the value chains in new dynamics of gathering multispectral and hyperspectral image data and

³ MySmartFarm // Solar Impulse Foundation. URL: <https://solarimpulse.com/companies/mysmartfarm> (accessed: 18.08.2021).

⁴ Sanchez D. MySmartFarm Ag Solution Wins IBM SmartCamp Award // The Moguldom Nation. October 11, 2013. URL: <https://moguldom.com/24914/mysmartfarm-app-wins-ibm-south-africa-award> (accessed: 01.02.2022).

⁵ Lourie G. 7 South African Drone Firms to Keep an Eye on // TFS Media. September 12, 2017. URL: <https://www.techfinancials.co.za/2017/09/12/httpstalkiot-co-za201709117-south-african-drone-firms-to-keep-an-eye-on> (accessed: 01.02.2022).

disseminating information through multiple channels to gain relevant insights” (Artificial Intelligence for Africa..., 2018, p. 19).

Kenya also started implementing two startups based on AI-algorithms. One of them, called *FarmDrive*, represents a technological platform, that provides financial institutions with a model, based on a large amount of data, relevant to the agricultural industry, necessary for risk assessment when issuing loans and developing targeted loan products that would meet the needs of small farmers.⁶ Another start-up supposes integration into social networks and messengers of a specialized chatbot named *Sophie*.⁷ This free chatbot, equipped with a convenient voice interface, represents a platform on which any user can ask questions in the intimate sphere, including in the field of reproductive medicine, and get an exhaustive answer. This service is available in several popular social media platforms, such as Messenger and Twitter.

Nigeria is also actively implementing AI technologies into people’s daily life. The most successful example is the technological platform *Kudi.ai* (“kudi” means money in the Hausa language). It was launched in 2017 and represents a chatbot functioning on AI algorithms; its main task is to provide assistance in the financial sphere, including transferring money and paying bills. Also, as in the case chatbot of Sophie, Kudi is integrated into most popular messaging apps and social networks, in particular, Facebook (On March 21, 2022, the Tverskoy District Court of Moscow satisfied the claim of the Prosecutor General’s Office of the Russian Federation and recognized the activities of the social networks Instagram and Facebook, owned by Meta, as extremist, banning their work in Russia. — *Editor’s note*).⁸ Another chatbot, called *Lara*,

launched on March 5, 2017, is an intelligent system that helps users get from one point to another by providing detailed text, step-by-step instructions, and determining the exact fare in advance.⁹

Nigeria’s banking sector is also starting to use AI-technologies. Thus, located in Nigeria, *Zenith Bank* “launched several new solutions that enable more convenient, safe and quick customer transactions. These include the bank’s Scan to Pay App which can be used by Zenith and non-zenith customers to make online and in-store payments in seconds through quick response code scanning on any internet enabled phone. The bank’s mobile app also offers enhanced functionalities such as instant account opening for new customer” (Artificial Intelligence for Africa..., 2018, p. 14).

And in May 2017 another Nigerian Bank — the Wema Bank — launched the first African fully digital Bank called the ALAT. It gives the opportunity for customers to “open an account via mobile phone or Internet in under five minutes and debit cards are delivered anywhere in Nigeria within two to three days, free of charge” (Artificial Intelligence for Africa..., 2018, p. 14).

In Uganda there has been launched the *Awamo* — “a digital banking platform and credit bureau that uses AI to reduce fraud when signing up customers and businesses to its platform. The platform helps digitise business procedures, credit information sharing, and many other services using mobile devices” (Butcher, Wilson-Strydom & Baijnath, 2021, p. 48).

Based on all these examples, we can conclude that African countries are beginning to use AI technology in the creation of various services aimed at meeting the needs of their

⁶ FarmDrive. URL: <https://farmdrive.co.ke> (accessed: 18.08.2021).

⁷ SophieBot. URL: <https://web.archive.org/web/20161104205907/http://www.sophiebot.tk/> (accessed: 18.08.2021).

⁸ Akinwamide N. Kudi AI is Putting a Human Feel to Online Payments in Nigeria // Techpoint Africa. February

8, 2017. URL: <https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria> (accessed: 29.07.2021).

⁹ Ndiomewese I. Startup Profile: Lara — Get Step-By-Step Public Transportation Directions to Any Destination // Techpoint Africa. April 17, 2017. URL: <https://techpoint.africa/2017/04/17/lara-profile> (accessed: 29.07.2021).

citizens. But at the same time, it must be remembered that all these technologies can be used maliciously. That's why it seems extremely important to examine existing practices and risks of malicious use of artificial intelligence (MUAI) in Africa.

Risks of Malicious Use of AI in Sub-Saharan Africa

Sub-Saharan African countries are already suffering cyberattacks of a different kind, such as phishing, DDoS-attacks, and data theft (Interpol, 2020). The last point leads us to the conclusion that when developing the ICT sector in a particular country, it is necessary to think about ensuring the information security of the whole country and its citizens.

According to official data in 2017, the total loss due to cybercrime across Africa amounted to 3.5 billion USD. The largest amount of damage, 649 million USD, was caused to Nigeria, Kenya keeps the second place, with 210 million USD, and South Africa rounds out the top three with a total of 157 million USD in damages.¹⁰ Undoubtedly these impressive figures underscore the fact that African governments must do something to strengthen information security in their countries. A further analysis of the statistics indicates that African banks are most vulnerable to cyberattacks, as they are the focus of 23% of attacks, followed by government bodies at different levels (19%), ecommerce (16%), mobile-based transactions (13%) and telecommunication (11%).¹¹

The problem is complicated by the fact that Africa's digital infrastructure is rather ill-equipped to manage the continent's growing

cybersecurity risk, and more than 60% of African enterprises have not trained their staff in the field of cybersecurity. More than 90% of big African companies spend less than 10,000 USD on different cybersecurity issues and are operating below the cybersecurity poverty level.¹² Thus, African countries are very attractive to any kind of cybercriminal. A 2013 report on whether Africa is a safe harbor for cybercriminals highlights two key circumstances that contribute to the growth of cybercrime in Africa: mass access to the fiber-optic broadband communication system, which contributes to a rapid increase in the number of Internet users, and the lack of developed legislation in the field of cybersecurity (Kharouni, 2013). At the same time, although a number of African countries have adopted laws aimed at protecting personal data and combating cybercrime in recent years, there have been no positive changes in this area, and, indeed, a sharp increase in the number of cybercrimes in Africa poses a serious threat to personal, national, and even international psychological security.

Although Sub-Saharan African countries have an increased focus on advanced technology, "they seldom have national strategies to support future plans. At present, high levels of corruption in public institutions and weak data infrastructure that is susceptible to data leaks pose a threat to data privacy and successful AI implementation" (Butcher, Wilson-Strydom & Bajinath, 2021, p. 62).

The vast majority of cybercrime offences committed in Africa are financial in nature and target individuals for theft. According to Interpol's African Cyberthreat Assessment Report, the following major cyberthreats can be highlighted for Africa: online scams, digital extortion, business e-mail compromise, botnets, and ransomware.¹³

¹² Ibid.

¹³ Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/>

¹⁰ Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line // Serianu. 2017. URL: <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf> (accessed: 05.07.2021).

¹¹ Isiavwe D. Cybersecurity Threat Evolution: Perspectives from Africa // The Information Security Society of Africa — Nigeria. February 15, 2020. URL: <https://www.issan.org.ng/download/cyber-security-threat-evolution> (accessed: 05.07.2021).

The situation is simplified by the fact that mass digitalization has created a great number of different databases with personal details for a huge number of ordinary people. In Africa, such databases have very poor cyber-defense and can quite often fall into the hands of intruders who use the information maliciously to get something of value from their victims.

One of the largest cyberattacks in Africa is the leakage of personal data from residents of the Republic of South Africa, which occurred in 2017.¹⁴ Files containing personal information of millions of South Africans, both living and deceased, became freely available on the Internet, including their national identity numbers, information about marital status, income, information about work and the current position, and information about their property. It is noteworthy, that this data leak cannot be called a hacker attack in the full sense, because all of this information about users was posted on the website of the data processing company Dracore Data Sciences without any additional protection.¹⁵ It is quite obvious that it was only a matter of time before this information would fall into the hands of hackers, who can now dispose of it at their discretion.

In addition to such cases, which have all the signs of criminal negligence, African countries regularly face massive cyberattacks, some of which actively use the possibilities of AI and attack critical infrastructure in Africa. Thus, *Life Healthcare*, the second largest

operator of private hospitals in South Africa responsible for the supply of digital services in hospitals throughout South Africa, faced a large-scale cyberattack in June 2020 that put its reception systems, business processing systems, and email servers out of service. This led to a month of downtime and caused fatal consequences in the midst of the coronavirus pandemic.

In October 2020, two other cyberattacks occurred in South Africa that took key social and emergency services in Johannesburg out of service: “Analysis of the attack identified not only the exploitation of a vulnerability, but also that after employing lateral movement techniques the threat actors deliberately deployed their ransomware to coincide with the end of the month payment cycle — in an effort to further coerce South African authorities to pay the cryptocurrency ransom.”¹⁶ In July 2021, the state-owned South African company Transnet faced an unprecedented cyberattack, as a result of which container operations in both major South African ports — Cape Town and Durban — were disrupted. On July 22, 2021, the official Transnet website went down and only showed an error message. The company, which operates the major ports in South Africa, as well as a huge railway network transporting minerals and other goods for export, officially confirmed that its IT infrastructure experienced failures. The Institute for Security Studies (ISS) highlighted that, for the “first time the integrity of South Africa’s critical maritime infrastructure has been severely disrupted” with an attack on the port able to delay or shut down a critical trade route and disrupt vital trade services.”¹⁷ Thus “most of the copper and cobalt mined in the Democratic Republic of Congo and Zambia, where miners such as Glencore and Barrick

News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa (accessed: 11.07.2021).

¹⁴ Mohapi T. What We Know So Far about South Africa’s Largest Ever Data Breach // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210122034431/https://iafrikan.com/2017/10/17/south-africas-govault-hacked-over-30-million-personal-records-leaked/> (accessed: 11.07.2021).

¹⁵ Mohapi T. Is Dracore Data Sciences Responsible for South Africa’s Largest Ever Data Leak? // iAfrikan. October 18, 2017. URL: <https://web.archive.org/web/20210404225144/https://www.iafrikan.com/2017/10/18/dracore-data-sciences/> (accessed: 11.07.2021).

¹⁶ Cyberthreat Assessment Report: Interpol’s Key Insight into Cybercrime in Africa // Interpol. October 21, 2021. URL: <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa> (accessed: 11.07.2021).

¹⁷ Ibid.

Gold operate, use Durban to ship cargo out of Africa.”¹⁸ This last example clearly demonstrates how advanced technologies can be used maliciously to disable critical infrastructure in African countries. The true reason for the cyberattack on the Transnet computer systems has also not been established, but there some concern that it could be related to the riots and violence that had swept through some parts of the country earlier in the year.

From time to time Ethiopia has also faced large-scaled cyberattacks on its critical infrastructure. The Nile River’s Grand Ethiopian Renaissance Dam is widely known to be a source of tension between Ethiopia and Egypt, and in June 2020, the Egypt-based actor known as the Cyber Horus Group hatched plans for a big cyberattack to create “significant economic, psychological, and political pressure on Ethiopia over the filling of the Nile River’s Grand Ethiopian Renaissance Dam (GERD).”¹⁹ The group managed to hack a number of government websites and spread messages threatening war if Ethiopia began filling the dam.

The last example illustrates that sometimes advanced technologies are used in Africa to manipulate public opinion and increase social tension. The most suitable technology for this is the creation of fake video and audio. By itself, this technology, also called ‘deepfakes,’ represents a synthesis of images using appropriate AI algorithms, that results in the apparent clone of a real person who moves and speaks just like the template. This technology opens a wide range of opportunities for malicious use and poses a

serious threat to personal, national, and international security, because it allows a hacker or a potential terrorist to make any politician or well-known person appear to say and do whatever the hacker wants, and this false video can be posted on social media platforms (on fake profiles) or on a fake website for well-known media. The fake video can quickly spread all over the web and end political careers or even cause deep political crises between nations. It is noteworthy that “convincing deepfakes can be made by pretty much anyone with the right hardware and software and a few hours to kill. The results can wreak havoc on individual livelihoods and reputations, but more frighteningly, can be used to manipulate en masse.”²⁰

One of the most revealing examples of the use of advanced technologies to incite mass discontent and tension in relations between different African countries is the active use of deepfakes during the wave of riots and violence that swept through South Africa in 2019 on the basis of xenophobic sentiments, after truck drivers staged a strike in protest against the employment of foreigners. During the mass pogroms of foreign-owned enterprises in Johannesburg in early September 2019 twelve people were killed. Although nobody from Nigeria has actually been suffered (among those killed ten were South African citizens and two were Zimbabweans), a number of fake videos and images that allegedly depicted attacks and murders of Nigerians or their mass deportation rapidly appeared on social media.²¹ To further incite mass discontent, a video taken out of context also appeared on online that claims to depict a

¹⁸ Shabalala Z., Heiberg T. Cyber Attack Disrupts Major South African Port Operations // Reuters. July 22, 2021. URL: <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/> (accessed: 29.09.2021).

¹⁹ Allen N. Africa’s Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

²⁰ Neille D. Manipulating Reality: The Rise of Deepfakes and How to Spot Them // Daily Maverick. May 05, 2021. URL: <https://www.dailymaverick.co.za/article/2021-05-05-manipulating-reality-the-rise-of-deepfakes-and-how-to-spot-them> (accessed: 18.09.2021).

²¹ Faife C. In Africa, Fear of State Violence Informs Deepfake Threat // WITNESS. December 9, 2019. URL: <https://blog.witness.org/2019/12/africa-fear-state-violence-informs-deepfake-threat> (accessed: 18.07.2021).

burning building in South Africa, although the fire was actually located in India in the state of Gujarat.²² As a result of these deepfakes, Nigeria withdrew a delegation from a big international conference held in South Africa and announced the evacuation of its citizens from that country. This forced South Africa to make an official apology to Nigeria for the xenophobic attacks that caused a surge in tension between two countries, and to assure its Nigerian partners that all cases of mass pogroms of Nigerian-owned enterprises would be thoroughly investigated.²³ This type of malicious use of advanced technologies to incite conflict between two countries in a region where many countries have unresolved disputes and claims against each other poses a very serious threat to international information and psychological security, because any such clash could escalate into another full-scale armed conflict.

It might also intensify the activity of different terrorist groups on the continent, such as Boko Haram in Nigeria, Ansar al-Din in Mali, Movement for Unity and Jihad in West Africa, and Al-Shabaab in Somalia. These groups could start using advanced technologies to improve communications between fighters, spread propaganda their views throughout Africa, and recruit new supporters: “Because the Internet combines the advantages of speed, cheapness, accessibility, and anonymity, it offers terrorists a variety of media options to sell their extremist ideology and message and attempt to radicalize other Internet users who may have sympathy for them” (Chiluwa, 2019c, p. 208). The Internet in general — and

social media in particular — should be considered as a very dangerous instrument for terrorist propaganda and recruitment (Chiluwa, 2019a, p. 522). As Ishengoma has argued, “The prominence of Internet communications in contemporary social life and the application of the Internet and ICT to advance terrorist activities have given rise to the concept of ‘Terrorism 2.0,’ where terrorist groups have extensively adopted web 2.0 applications and semantic technology tools to propagate their activities” (Ishengoma, 2013).

It is just a matter of time before terrorists become familiar enough with AI and start using its possibilities to organize high-tech terroristic attacks. Boko Haram, for example, is actively using surveillance drones, which are “reportedly more sophisticated than those used by the government.”²⁴ Al-Shabaab “already has been accused of ‘twitter terrorism,’ and hate-speech warranting the shutting down of their Twitter accounts at different times” (Chiluwa, Chimunya & Ajiboye, 2020). African countries should therefore focus all their efforts on strengthening their information, psychological, and cyber security and prevent further malicious use of AI-based technologies.

Ensuring Psychological Security in Sub-Saharan Africa: Challenges and Prospects

The issue of information, cyber and psychological security remains one of the key issues hindering the further sustainable socio-economic development of sub-Saharan Africa. According to Allen, “the continent faces a growing 100,000-person gap in certified cybersecurity professionals.”²⁵ Many organizations, businesses, and agencies lack basic cyber awareness and fail

²² Burning Building Video from India, Not from Xenophobic Violence in South Africa // Africa Check. September 19, 2019. URL: <https://africacheck.org/fact-checks/fbchecks/burning-building-video-india-not-xenophobic-violence-south-africa> (accessed: 18.07.2021).

²³ South Africa Offers ‘Profuse’ Apologies to Nigeria After Attacks // Al Jazeera. September 16, 2019. URL: <https://www.aljazeera.com/news/2019/9/16/south-africa-offers-profuse-apologies-to-nigeria-after-attacks> (accessed: 18.07.2021).

²⁴ Allen N. Africa’s Evolving Cyber Threats // Africa Center for Strategic Studies. January 19, 2021. URL: <https://africacenter.org/spotlight/Africa-evolving-cyber-threats> (accessed: 29.09.2021).

²⁵ Ibid.

to implement rudimentary cybersecurity measures. Governments frequently fail to monitor threats, collect digital forensic evidence, and prosecute computer-based crime. 96% of cyber security incidents go unreported or unresolved, meaning that cyber threats in Africa are likely much worse than recognized.²⁶ A number of African countries are, however, working hard on this issue and have initiated the significant modernization of relevant national legislature, because “for states with weaker cyber security capacities, a strong legal and normative framework is an essential element affording protection from foreign interference and cyber threats.”²⁷ According to data provided by the International Telecommunication Union (ITU), about 40 African countries have cybercriminal legislation and cybersecurity regulations in place. Moreover, eleven countries — South Africa, Botswana, Uganda, Zambia, Burkina Faso, Tanzania, Cameroon, Nigeria, Benin, Ghana and Côte d’Ivoire — have developed complex commitments and engage in cybersecurity programs and initiatives.²⁸

Rwanda, Kenya, and Uganda, for example, have undertaken a number of measures to counteract cyberthreats and protect data in cyberspace. These measures should be recognized as effective, but they are not sufficient for a comprehensive solution to the problem. Rwanda, for example, has elaborated a National Policy on the field of cyber security, which supported the creation of the National Center of Computer Security and Response

²⁶ Van der Waag-Cowling N. Living Below the Cyber Poverty Line: Strategic Challenges for Africa // Humanitarian Law and Policy. June 11, 2020. URL: <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa> (accessed: 18.08.2021).

²⁷ Ibid.

²⁸ Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union, 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf (accessed: 18.08.2021).

focused on the identification and prevention of cyberthreats. The National Cyberspace Emergency Plan to counteract cyber crises has also been elaborated. Finally, a law on ICT in Rwanda was adopted in 2016 that contains a number of articles devoted to the malicious use of information technologies for the purpose of committing crimes which imposes criminal liability for unauthorized access to data.²⁹

Kenya elaborated its own National Cyber Security Strategy in 2014.³⁰ Following this strategy, amendments have been adopted to the law on ICT aimed at the criminalization of illegal access to information. The National Kenya Computer Incident Response Team — Coordination Centre (National KE-CIRT/CC) has also been created, which is supported by the ITU to coordinate responses to cybersecurity matters at the national level in collaboration with relevant actors both locally and internationally.³¹

Uganda also has a more or less well developed legislative base for ensuring cybersecurity. The country has adopted a special law on the malicious use of computers, which ensures the protection of wire transactions and makes it possible to monitor and intercept suspicious messages. A special National Cyberspace Emergency Response Team and a specialized National Information

²⁹ Rwanda: 2016 Law Governing Information and Communication Technologies // ARTICLE 19. May 2018. URL: <https://www.article19.org/wp-content/uploads/2018/05/Analysis-Rwanda-ICT-Law-April-2018.pdf> (accessed: 18.08.2021).

³⁰ National Cybersecurity Strategy of Kenya // Ministry of Information Communications and Technology of Kenya. February 2014. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf (accessed: 18.08.2021).

³¹ Digital Trends in Africa: Information and Communication Technology Trends and Developments in the Africa Region, 2017—2020 // International Telecommunication Union. 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf (accessed: 18.08.2021).

Advisory and Technology Body have also been created, whose tasks include providing technical support and training in the field of cybersecurity.

It is impossible to solve all of the challenges facing African countries in this area only through the introduction of various prohibitive measures at the national level. The problem of ensuring cyber and psychological security is complicated, and a comprehensive solution is possible only through the involvement of all stakeholders, which include representatives of various governmental bodies, top managers of big companies, representatives of the financial sector, and civil society.

At the same time, special emphasis should be placed on the need to intensify cooperation in this area among all African countries. For this purpose, the African Information Security Association (AISA) was created in 2006 as the result of the *International Conference on Computer Security and Cybercrime in Africa*.³² AISA's mission is to develop information security in Africa, and any stakeholder concerned about ensuring information security — including individuals, organizations, and various governmental bodies — can join the association. According to the information provided on the website, AISA's main activity is aimed at sharing world best practices in the field of information, computer, and Internet security and organizing campaigns to combat cybercrime in Africa, primarily by organizing and holding seminars and conferences, publishing books, and magazines, and maintaining websites and blogs, as well as developing various security guidelines and consultations.³³ The annual monitoring of the level of information security in Africa is one of AISA's most important activity streams. Despite more

³² African Information Security Association (AISA). URL: <https://web.archive.org/web/20120128191125/http://www.jidaw.com/aisa> (accessed: 18.08.2021).

³³ Ibid.

than a decade of work, we have not been able to find any meaningful results from its activities, and the content of its website remains very poor.

Among other important initiatives demonstrating the attempt of African countries to develop a joint approach to ensuring information security there should be noted the African Union *Convention on Cyber Security and Personal Data Protection*, which was adopted in 2014 in Malabo, Equatorial Guinea.³⁴ The appearance of this document should be considered an important step that proves the desire of African countries to develop joint mechanisms to further combat cybercrime and “provide a framework for cybersecurity in Africa. As part of this, member states are asked to establish national cybersecurity policies as well as legal, regulatory, and institutional frameworks for cybersecurity governance.”³⁵ At the same time, however, the process of signing and subsequent ratification of this document shows the existence of serious contradictions between different African countries in the field of cybersecurity. To date, the *Convention* has been signed by only 14 African countries, and only 13 have ratified it (Angola, Cape Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and Zambia).³⁶ It is noteworthy that

³⁴ African Union Convention on Cyber Security and Personal Data Protection // The Institute for Security Studies. June 27, 2014. URL: <https://issafrica.org/ctafrika/uploads/AU%20Convention%20on%20Cyber%20Security%20and%20Personal%20Data%20Protection.pdf> (accessed: 21.07.2021).

³⁵ Jili B. The Spread of Surveillance Technology in Africa Stirs Security Concerns // Africa Center for Strategic Studies. December 11, 2020. URL: <https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns> (accessed: 05.09.2021).

³⁶ List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection // African Union. March 25, 2022. URL: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (accessed: 01.04.2022).

regional leaders in the field of ICTs, such as Kenya, Nigeria, and South Africa have not signed this document. Indeed, the *Convention* has not yet entered into force, because it must be ratified by at least 15 countries,³⁷ so it can therefore be considered only as another program document trying to regulate one of the most important areas of cooperation related to cybersecurity. But “even with the challenge in ratification, it remains a major step forward towards increasing awareness amongst the ministers and administrators from member states.”³⁸ The *Convention* again shows that supranational institutions and instruments work extremely poorly in African circumstances, perhaps because of the many contradictions among African countries, which, taken together, prevent them from developing common working tools to solve the most significant problems of the continent, including information, psychological and cybersecurity.

In this regard, only the ISSAN has managed to achieve relative success and become a real platform for cooperation and exchange of views between all stakeholders, including banks, telecommunications companies, government agencies, government regulators, IT companies, information security consultants, and lawyers.³⁹ It must be particularly emphasized that ISSAN is a non-profit organization whose objective is to ensure that Nigeria's cyberspace, primarily the banking and public sectors, is protected and the organization solves this task

³⁷ African Union Convention on Cyber Security and Personal Data Protection // African Union. June 27, 2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed: 05.09.2021).

³⁸ Tomlin S. N. Cyberspace Security in Africa — Where Do We Stand? // African Academic Network on Internet Policy. February 12, 2020. URL: <https://aanoip.org/cyberspace-security-in-africa-where-do-we-stand> (accessed: 18.08.2021).

³⁹ Information Security Society of Africa — Nigeria (ISSAN). URL: <https://issan.org.ng> (accessed: 18.08.2021).

by carrying out a set of activities aimed at familiarizing all stakeholders with best practices in this area.

Conclusion

In conclusion, we would like to make a few important points.

Firstly, Sub-Saharan African countries are paying increased attention to the elaboration of different technological solutions based on AI algorithms. The use of unmanned aerial vehicles should be considered as the most promising technology with the great potential in the region. According to Haula and Agbozo (2020), “drone technology has the capacity to improve upon service delivery in the agriculture, health and security sectors of sub-Saharan Africa.” For example, such drones can be used for “monitoring terrorist movements and identifying targets/threats; healthcare delivery; land administration, and cadastral intelligence; fertilizer and irrigation treatments; crop performance improvement; automation of pestilence combating.”

Secondly, all new technologies can be used for malicious intent. The states of Sub-Saharan Africa continue to suffer from cyber-crimes of all kinds, which in the age of rapid development of AI-based technologies are becoming increasingly high-tech. The problem of ensuring information, psychological, and cybersecurity is common to all African countries, which creates a serious obstacle for their further sustainable social and economic development. As Vattapparamban et al. (2016) argue, when an unmanned aerial vehicle goes beyond the line of sight, it can be used as a signal sniffer. Drones also can be used for cyber-attacks, interdiction of other drones, or even GPS spoofing. Such threats should be carefully studied before the use of drones becomes widespread in the region.

Thirdly, over the past decade, Sub-Saharan African countries made significant efforts to develop a shared vision to counter cybercrime and the misuse of advanced technologies.

However, all their attempts to establish effective supranational instruments that would regulate the fight against cyberattacks at the Pan-African level and take into account the interests of the vast majority of African countries in this area have failed. This demonstrates the serious contradictions between African countries, which together hinder mutually beneficial cooperation even in the important area of cybersecurity.

However, until such cooperation emerges, it seems unlikely that African countries will even come close to solving this problem, which means that their information space will continue to be subject to large-scale cyber-attacks, posing a serious threat not only to the security of individuals, but also to national and pan-African security.

Received / Поступила в редакцию: 10.03.2022

Revised / Доработана после рецензирования: 03.04.2022

Accepted / Принята к публикации: 18.04.2022

References

- Antinori, A. (2019). Terrorism and deepfakes: From hybrid warfare to post-truth warfare in a hybrid world. In P. Griffiths & M. Nowshade (Eds.), *Proceedings of the European conference on the impact of artificial intelligence and robotics* (pp. 23—20). Reading, South Oxfordshire, England: Academic Conferences and publishing limited.
- Artificial intelligence for Africa: An opportunity for growth, development, and democratisation. (2018). *Access Partnership*. Retrieved from https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf
- Bazarkina, D. Y., & Pashentsev, E. N. (2019). Artificial intelligence and new threats to international psychological security. *Russia in Global Affairs*, 17(1), 147—170. <https://doi.org/10.31278/1810-6374-2019-17-1-147-170>
- Bazarkina, D. Y., Pashentsev, E. N., & Simons, G. (2020). *Terrorism and advanced technologies in psychological warfare: New risks, new opportunities to counter the terrorist threat*. New York: Nova Science Publishers.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., et al. (2018). The malicious use of artificial intelligence: forecasting, prevention, and mitigation. *Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI*, 1—100. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>
- Butcher, N., Wilson-Strydom, M., & Baijnath, M. (2021). Artificial intelligence capacity in Sub-Saharan Africa. Compendium Report. *International Development Research Centre*. Retrieved from <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/59999/27ea1089-760f-4136-b637-16367161edcc.pdf?sequence=1>
- Chesney, R., & Citron, D. (2018). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(1753), 1753—1820. <https://doi.org/10.15779/Z38RV0D15J>
- Chiluwa, I. E. (2019a). Deception in online terrorist propaganda: A study of ISIS and Boko Haram. In I. E. Chiluwa & S. A. Samoilenko (Eds.), *Handbook of research on deception, fake news, and misinformation online* (pp. 520—537). Hershey, PA: Information Science Reference. <https://doi.org/10.4018/978-1-5225-8535-0.ch028>
- Chiluwa, I. E. (2019b). Discourse analysis and conflict studies. In *SAGE Research Methods Cases*. London: SAGE Publications. <https://dx.doi.org/10.4135/9781526468208>
- Chiluwa, I. E. (2019c). Online activism in Mali: A study of digital discourses of the movement for the liberation of Azawad. In I. E. Chiluwa & G. Bourvier (Eds.), *Activism, campaigning and political discourse on Twitter* (pp. 207—234). New York: Nova Science Publishers.
- Chiluwa, I. E., Chimuanya, L., & Ajiboye, E. (2020). Communicating religious extremism in West Africa. In J. Tarusarira & E. Chitando (Eds.), *Themes in religion and human security in Africa* (pp. 166—179). London: Routledge. <https://doi.org/10.4324/9781003017080-12>
- Dack, S. (2019). Deep fakes, fake news, and what comes next. *The Henry M. Jackson School of International Studies, University of Washington*. Retrieved from <https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next>
- Haula, K., & Agbozo, E. (2020). A systematic review on unmanned aerial vehicles in Sub-Saharan Africa: A socio-technical perspective. *Technology in Society*, 63, 1—7. <https://doi.org/10.1016/j.techsoc.2020.101357>

- Interpol. (2020). Online African organized crime from surface and dark web. *Interpol Analytical Report*. Retrieved from: <https://www.euneighbours.eu/sites/default/files/publications/2020-08/INTERPOL%20report.pdf>
- Ishengoma, F. R. (2013). Online social networks and terrorism 2.0 in developing countries. *International Journal of Computer Science and Network Solutions*, 1(4), 1—12. <https://doi.org/10.48550/arXiv.1410.0531>
- Jeangène Vilmer, J.-B., Escorcía, A., Guillaume, M., & Herrera, J. (2018). Les manipulations de l'information: un défi pour nos démocraties. *Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées*, 1—214. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2_cle04b2b6.pdf
- Kharouni, L. (2013). Africa: A new safe harbor for cybercriminals? *Trend Micro Incorporated Research Paper*, 1—31. Retrieved from <https://web.archive.org/web/20220403192613/https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf>
- Owoyemi, A., Owoyemi, J., Osiyemi, A., & Boyd, A. (2020). Artificial intelligence for healthcare in Africa. *Frontiers in Digital Health*, 2, 1—5. <https://doi.org/10.3389/fdgth.2020.00006>
- Pashentsev, E. (2019). Destabilization of unstable dynamic social equilibriums through high-tech strategic psychological warfare. In N. van der Waag-Cowling & L. Leenen (Eds.), *Proceedings of the 14th International Conference on Cyber Warfare and Security* (pp. 322—328). Reading, South Oxfordshire, England: Academic Conferences and publishing limited.
- Vattapparamban, E., Güvenç, İ, Yurekli, A., Akkaya, K., & Uluğaç S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 216—221). New York: Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/IWCMC.2016.7577060>

About the author: *Pantserev Konstantin Arsenievich* — PhD, Dr. of Sc. (Political Sciences), Professor, Department of Theory and History of International Relations, The Faculty of International Relations, St. Petersburg State University; ORCID: 0000-0002-2164-9525; e-mail: pantserev@yandex.ru