Old Dominion University

ODU Digital Commons

Community & Environmental Health Faculty Publications | School of Community & Environmental Health

2023

# Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations

Issah Samori
*minoHealth AI Labs*

Gbadebo Odularu
*Old Dominion University*, godul001@odu.edu

Lucas Potter
*Biosview*, lpott005@odu.edu

Xavier-Lewis Palmer
*Old Dominion University*, xpalmer@odu.edu

Follow this and additional works at: https://digitalcommons.odu.edu/commhealth_fac_pubs

 Part of the Electrical and Computer Engineering Commons, and the International Public Health Commons

## Original Publication Citation

Samori, I., Odularu, G., Potter, L., & Palmer, X.-L. (2023). Biocybersecurity and deterrence: Hypothetical Rwandan considerations. In R. L. Wilson & B. Curran (Eds.), *Proceedings of the 18th International Conference on Cyber Warfare and Security (pp. 348-354)*. Academic Conferences International Limited. https://doi.org/10.34190/iccws.18.1.1012

This Article is brought to you for free and open access by the School of Community & Environmental Health at ODU Digital Commons. It has been accepted for inclusion in Community & Environmental Health Faculty Publications by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

# Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations

**Issah Abubakari Samori[1], Gbadebo Odularu[2], Lucas Potter[3] and Xavier-Lewis Palmer[1-3]**
[1]minoHealth AI Labs, Accra, Ghana
[2]Old Dominion University, Norfolk, USA
[3]BiosView, Oswego, USA

issahsamori@gmail.com
godul001@odu.edu
lpott005@odu.edu
xpalm001@odu.edu

**Abstract**: Digitalization and sustainability are popular words within modern disciplines as practitioners each look toward the future of their respective fields. Specifically for the African continent, which is making great strides in developmental targets, those two terms are central to core aspects of policy initiatives that may foster cooperation across its varied lands and nations. One of the underlying challenges that confront Africa is a lack of strong regional integration across socioeconomic and political programs; there is value in African regions having more regional connectedness. We assess the rate of regional integration and development in Africa and discuss how to alleviate development crises that could be accelerated by deploying a sustainable cybersecurity strategy, which increasingly includes the bioeconomy and its components. This can be done through the application of Fourth Industrial Revolution (4IR) technologies such as Artificial Intelligence (AI) and modern biotechnology. This work suggests that political and socio-economic activities associated with regional integration must be seen as an all-encompassing task that transcends beyond national boundaries towards a cyber biodefense fortification and increases in 4IR technological integration. This has the aim of thereby encompassing efforts to persuade leaders to fast-track policies that seek to promote geospatial cyberinfrastructure, integrative cybersecurity considerations, cross-border digitalization programs, and increased need for cybersecurity research and education, with mindfulness towards education and further integration of mindful automation. In conclusion, a model of integrative security is proposed for Africa.

**Keywords:** Africa, Cybersecurity, Machine Learning, Cyberbiosecurity, Biocybersecurity, Public Health

## 1. Introduction

Cybersecurity policies or notional counterparts are commonplace in both the Global North (GN) and Global South (GS). Sub-policies hoping to deter cybercrime may not be found explicitly in national cybersecurity plans like that of Rwanda. However, there is a need for clearer and more comprehensive policy language that can allow deeper discussion into the contexts in which they may be enacted or pursued. Some policies, extending from emergent trends in technology development cannot emerge easily, especially when they are of hybrid fields that depend on infrastructure that is believed to belong to different domains. Herein exists the problem of biocybersecurity (BCS) and cyberbiosecurity (CBS). These describe the bridge between biosecurity, cybersecurity, and cyber-physical security and are especially relevant within the bioeconomy wherein ample cyber-physical interfaces in critical infrastructure exist; Vulnerabilities here carry national security implications as the tools to exploit them are increasingly easier to access (Murch et al. 2018; George 2019). Threats that can occur at this intersection concern the weaponization of linked biological and digital information and products that can critically derail bio-economies and the populations that depend on them (Duncan et al, 2019; Richardson et al.,2019). Attacks from their weaponization can stall development in GS countries and prevent the bridging of development gaps. To anticipate and counter BCS/CBS threats require high levels of specialization in biosecurity and cybersecurity. As biological and cyber systems further intertwine, the attacks by malicious actors at this intersection could appear and grow, accompanying the growing wave of GS cybercrime. Further, attacks through methods such as epigenetic logic bombs, medical device-driven person DDOS-ing, intra-implant surveillance, and multiplication of attack vectors via drones, mosquitoes, or other means, may allow for novel horrific means of civil disruption (Millett and dos Santos, 2019; Turner, 2019; Vinatzer et al., 2019: George, 2019; Richardson et al.,2019; Potter, 2020). The types of attacks, from the biological end, can be expanded by the complexity of the biology that is exploited since aspects of biology can serve as unique interlocks in system vulnerabilities.

What this means for nations that possess high biodiversity, such as those in Africa, is that they sit uniquely in terms of potentially weaponizable aspects of biology through consideration of pathogen storehouses in diverse environments (Samori et al, 2023). This prompts us to consider a new age of MAD in the context of Synbio and Cyber, provided that threat actors become more competent with both (Samori et al, 2023; Corlett et al., 2020;

Edwards and Revill, 2016; Gronvall, 2019). The means of deterring these types of exploits would be beneficial to develop nations within the African Union; therefore, a policy of BCS/CBS deterrence is offered for consideration. Ideally, one could suggest alternatives to BCS/CBS deterrence, but no alternatives exist. Academically, the concept of BCS, CBS, digital biosecurity, and or any variant has only existed with a degree of clustered rigor in the past decade and attempts to address BCS/CBS is quite new (Peccoud et al 2018; Murch and DiEuliis 2019). It is common to hear military, intelligence, and even politicians speak of cybersecurity, but "cyberbiosecurity" is yet to be treated with equal importance even in the Global North. This potentially highlights an issue of how much of a head start the Global North has in targeting unique GS holdings with respect to the value of their flora and fauna. A deep question exists in how holistic a country can examine itself, but that requires unity and a strong command of resources. In this work, the AU is used as an example of a partial GS commentary. Further, it is focused on the African continent with an emphasis on the continent's unique challenges regarding the Central African Nation of Rwanda as a partial study. Based on this background, the article discusses BCS/CBS and specific BCS/CBS deterrence policy for Africa.

## 2. The Greater AU and On Rwanda's Experience in Cyber-Deterrence

The creation and growth of the internet have brought forth great wealth and development to all parts of the world, albeit unevenly. As such, each economic sector, in each country, has used it to improve marketing and distribution. Governments have used it to both implement policy and monitor, to bring security to their nations. This has led to the increasing popularity and necessity for securing the use of the internet and protecting those who use it. At times the control of the internet has been used to prevent insurrections, stop improper exchanges of data or resources, and monitor malicious actors, especially nation-states as is evident in recent times has occurred, but a careful in-between has been preferred leading to the discussion of alternate means (Gohdes, 2020; Marchant and Stremlau, 2020). This is doable, as the options are many but necessary to ponder, as Cybersecurity is a vast domain, with implications affecting both national and international security.

Despite boasting more than 1.2 billion individuals, the 54 nations of the continent of Africa have by large been minimized in conversations surrounding cybersecurity much of this can be ascribed to comparative or uneven gaps in economic or military development, a shortage in professionals, low-penetrance, and more, in addition to historical prejudices and colonial hegemonies (Adomako et al 2018). Even with strides in development and innovations fostered among emigrants and individuals within that have initiated revolutions in technology abroad, it is still common for individuals in developed nations to ignore the evident progress, but instead, let their biases rule their judgment (Gewald et al 2012; Endong and Obi, 2020; Olubela 2018; Williams, 2020). Regardless of these biases, these young African nations are pressing on and aiming to catch up to many of these older and developed nations despite the hurdles that exist. This resolve is necessary as much cyber infrastructure remains underdeveloped and cybercrime persists in ways that can undermine cyberspace autonomy in many areas of the continent, which poses risks for development (Abrahams, L., & Mbanaso 2017). These concerns can be countered through strengthening intra-continental policies in cybersecurity, such as deterrence, as their growth is without doubt linked to their ability to cement their grasp on this important and explosively growing field. Especially in the case of fast-developing countries like Rwanda, the protection of government-administered services and private stakeholders is paramount (Nkusi, 2017). As of 2016, just about half of the continent's countries have enacted laws against cybercrime, penetration exists at slightly less than a third of the continent's population, and cybercrimes cost the continent over a billion, annually (Adomako et al 2018). This will need to change as Rwanda and other African countries continue to develop. Rwanda was chosen for this paper. It is an example of a young African country that has experienced not only rapid growth and development but while landlocked and emerging from a relatively recent civil war. Their progress has lessons for other GS nations to study, imperfections considered. This paper briefly examines part of its National Cyber Deterrence Policy, based on its 2015 National Cybersecurity Policy (Republic of Rwanda, 2015).

The policy in question is that of deterrence, within the scope of cybersecurity. The policy was developed by Rwanda, to outline and establish a national cybersecurity policy. It is part of a trend by other developing nations to catch up to development in policy with that of others (Adomako et al 2018, Lewis, 2014; Nkusi, 2017; Republic of Rwanda, 2015). In terms of how the policy is applied, insufficient information is given, owing to scant literature in the core document, the field, and from the government; the document itself referred to broad means of establishing capacity (Makanda et al 2017; Republic of Rwanda, 2015). However, there is a spectrum of potential ideas, which could prove useful. For example, from the positive and relatively inexpensive end, nations could make use of "cumulative deterrence" (Tor, 2017). Within, nations diplomatically pool resources to monitor and discourage acts. This is attractive as it allows funds normally appropriated for solo deterrence to be diverted

elsewhere in areas that possess a more dire need. However, this may require concessions within the nation of Burundi, with whom it split, that could cost Kagame popularity and thus internal power; careful steps are needed to avoid inflaming tensions that still exist (Ndayisaba, 2020). Further, a policy of cumulative deterrence might also require further learning on its other adjacent neighbors, but this might collectively achieve the same burden, but this remains to be seen as Rwanda develops its deterrence capacity. Crosston (2011) noted that many experts believed that even the "advanced" modern powers were unprepared for sophisticated, nation-state sponsored cyber-attacks and suggested that perhaps a mutually assured debilitation would be the best hope. For much of the African continent, this remains challenging in a conventional sense since considerably more of its internet penetration has been linked to the use of mobile phones versus that of fibre cables or the like (Makanda et al 2017). For example, in a study on Malawi, utilizing data from Malawi's 2015-2020 Strategic Plan, Makanda et al (2017) found that it is common for phone use across the content far outstrips the fixed broadband lines that exist. While this has allowed for mobile banking revolutions that have spread worldwide like that of the M-PESA system in Kenya and similar, also highlights an exploitable vulnerability and option in offensive capacity for Rwanda to pursue (Gewald et al 2012; Mas and Radcliffe 2010). This is an option that would require building an offensive capacity to dent mobile networks across the continent, which could backfire as no weapon remains unnoticed for long and could trigger an arms race in an offensive mobile capacity that could spread internationally (Dunham, 2008; Lakhdhar et al 2017). This could also damage Rwanda's image, internationally, reducing its ability to obtain assistance, utilize its soft power, and eventually threaten its pace of development, as with the case of North Korea, which has received scorn for not just its nuclear power development but also its capacity in offensive cyber operations (Boo, 2017; Haggard and Lindsay, 2015). However, some offensive capacity could prove helpful in countering the growing capacities of other nations. A dynamic balance could be in its best interest, for which some scholars like Iasiello (2014) may concur. His work noted the transience of many cyber-deterrence policies and how the field of cybersecurity is not static and requires adaptable and dynamic plans (Iasiello, 2014). Rwanda would be wise to tread carefully in the implementation of the deterrence policy.

In terms of how the policy fits into national/international policy/strategy, one can answer that it does well. According to its 2015 policy, it is in the process of building and strengthening its capacity, which may show remarkable progress by the release of its next edition (Republic of Rwanda, 2015). While scepticism in meaningful policy implementation may exist due to a shortage of professionals as noted by Adomako et al (2018), there is a long-running optimism as noted by Goodman (2010) who believes that deterrence is easier in practice than is theorized when grounded in the physical realities that shape any idealized plan. However, to make good on such optimism, there will need to be an upsurge in expertise to match cybersecurity, broadly, and internally. These concerns have future and ecological implications as well. Mueller (2020) notes in Cyberbiosecurity, expertise is difficult to come by which may pose difficulties on the biological end. This especially deserves mention as Central Africa boasts high biodiversity as Fa et al (2014) note, and countries like Rwanda may find value in leaning on sustaining that aspect when considering dividends that it may play in its bioeconomy. Numerous authors such as Peccoud et al (2018), George (2019), and Turner (2019) have commented on how the bioeconomy is linked to cybersecurity through cyber-physical workflows present in bioprocessing and how it inextricably poses national security, and thus international security implications.

## 3. An Overview of Regional Actors and Processes

In terms of the policy overview, and how it serves to resolve the existing problem, the issue is both simple and complex, in that no broad policy exists. Through proposing a policy, we address an emerging problem whose worst threats to human safety are in the future. With regards to BCS/CBS, interdisciplinary experts with some technical knowledge have been working to propose strategies that take best practices from biosecurity, cybersecurity, human factors, and related, but these proposals ultimately yet to find their way to the ear of governing authorities and much-less lawmakers. This context finds difficulty in that a sufficiently educated lay population, legal base, and governing base are needed for effective communication, the passage of law concerning, and the implementation of helpful policy. This problem is exacerbated by the fact that a comprehensive cybersecurity policy agreement itself has not been enacted in cybersecurity for the AU (Turianskyi, 2020). Further, the AU, much less than the EU, or the Global North is ready for a comprehensive BCS/CBS deterrence policy. At the same time, experts such as George (2019) have already pointed out and indicated that BCS/CBS possesses national implications, which also leads to international implications. The Global South is targeted for such a proposal instead of the Global North in that countries in each are interlinked through trade and history. What is allowed in the less prosperous areas, can eventually filter upward, much like increasing cybercrime that is spreading throughout GS, in part due to weak policy and enforcement, coupled

with economic situations that push individuals within more easily to crime (Baylon and Antwi-Boasiako, 2016). That said, consideration of the least equipped party is also important in the international scope as it eventually engages the most equipped parties. Everyone is eventually affected and is an actor. Next exists the question of how to bind actors. The AU is far from finishing the process of adopting a continent-wide cybersecurity agreement, the Convention on Cyber Security and Personal Data Protection (Turianskyi, 2020). It is difficult to imagine that they would be able to string together a BCS/CBS agreement at this point, with that in mind. Upon the day that they can consider their unique eco-biology, they should consider how each country's diverse flora and fauna can be exploited and protected in light of BCS/CBS. Within, they possess deep strategic resources that could be better protected through similar legislation. Such could also bolster conservation efforts across the continent that have been battered due to poaching and sacrifices of biodiversity for their economies.

## 4. Potential Impact of AI on Biocybersecurity

Artificial intelligence (AI) has seen remarkable progress over the past decade. This could be attributed to the rise in data generated and the amount of computing power available (Xu et al., 2021). Generative AI models, like Generative Pre-trained Transformers (GPT) (Brown et al., 2021) and DALL-E (Ramesh et al., 2022), are able to generate convincing images and text that are indistinguishable from what humans could generate. Some large language models (LLMs) are able to generate coherent convincing texts on subjects that seem like they were written by experts. This becomes worrisome when dealing with biological data. As more biological data (be it a newly discovered toxin or the latest variant of an infectious pathogen) is discovered, these generative models can get a better understanding of the makeup of these toxins and infectious pathogens and the underlying mechanisms based on which they operate. A system with such an understanding of biology can be used to generate lethal bioweapons that could have little to no weaknesses. This is alarming given that Africa is home to diverse biological species, which is good for an AI system when learning. AI can assist in accelerating crimes against biosecurity and cyberbiosecurity.

## 5. Implementation

Implementation ideally should be carried out by all African countries, and this would be strengthened with the increase in signatories by each additional country. Implementation would require stronger cybersecurity practices across the continent, in pace with its rapid connectivity, but also stronger biosecurity investments with appropriate mirror investments in infrastructure and practices. An easy benefit is that it can strengthen the growing efforts in combating epidemics from country to country, and more efficiently help contain epidemics.

Massive investments, unity, and anti-corruption measures would be required. Not all countries of the Global South are stable and possess the financial capacity to undertake endeavours to strengthen their cyberbiosecurity. As a result, incremental steps such as regional partnerships and foreign aid might be a way forward as each country finds its path. Each country will need to consider its unique, vulnerable resources to protect. That will require a means of increased scouting, public learning, and accounting beyond mere conservatorships of wildlife preserves and zoos.

This endeavour would be costly for any country considering the costs of current biotechnology. DIY efforts have shown that some costs in scouting can be reduced and distributed among citizens; this especially goes for tasks such as scouting biological resources and education, which are among the heaviest work (Bello et al., 2020; Sarpong et al., 2020; Kosaki, 2020; Wamuchiru and Moulaert, 2018; Kong and Bakker, 2018; Gruber, 2019). Even for advanced economies, there are not enough specialists to go around. Consequently, GS policy successes could entail benefits for the Global North. Community Bio groups have shown that biotechnology access does not need to be hyper-specialized, and education costs can be lowered as well, increasing access (Bello et al, 2020; Tylecote, 2019).

Communities in the Global South can identify, and catalogue unique aspects of their country's life forms, especially guided by local experts. AI can be adapted to sort through and categorize data. While intensive, this is important as such work affects everyone allowing for the improved mapping of both beneficial resources and pathogens among both humans and their environments. This has been addressed by Samori et al, 2023. With more biological resources mapped and improved education surrounding it, from the bottom-up, comprehensive biosecurity and thus BCS/CBS policy can more easily enter the mind of politicians to craft as citizens press politically from their increased appreciation and stake in their resources (Castro and New; 2016; Falzon et al, 2020).

## 6. Limitation and Conclusion

To summarize, Rwanda, like many other developing nations, has begun taking cybersecurity seriously and is developing both its infrastructure and means of bringing its cybersecurity policy up with international and intercontinental standards. In terms of deterrence, it has many directions in which it can go, but the direction in which it treads must be done at a speed that allows it to stem cybercrime and provocations by neighbouring and faraway nation-states. Further, its policy must carefully balance neighbourly burdens without cost to internal stability which could arise due to too many concessions or over-investment. In the absence of sufficient detail from their 2015 policy, international voices were added to this work in order to aid the discussion of the broader framework of cyber-deterrence concerning the case of Rwanda.

Adding BCS/CBS considerations to a national deterrence policy or Defend Forward initiative seems to be the most practiced deterrence policy at this time. (Deeks, 2020; Palmer et al, 2021). As such, a country can divert military funds to its initiative and gradually sharpen such a policy to expand with allies (Smeets; 2020). In general, BCS/CBS deterrence policies will need to be developed in the future as biology increasingly finds its way into conversations and arsenals of cybersecurity. For security, countries need to have adequate BCS/CBS infrastructure and policy in place before the biological equivalent of Metasploit becomes commonplace. Pursuing this policy appears preferable and may be the only one that reasonably exists.

## References


Abrahams, L., & Mbanaso, U. (2017). State of Internet security and policy in Africa. The International Institute of Tropical Agriculture (IITA) Resort, Ibadan, Oyo Nigeria 2-4 May, 2017

Adams, R. (2022). 'AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent. https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018, March). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. TPRC.

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science. 3–21. https://doi.org/10.1007/978-3-030-22475-2_1

Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics.

Asongu, S. A., Efobi, U. R., Tanankem, B. V., & Osabuohien, E. S. (2020). Globalisation and female economic participation in Sub-Saharan Africa. Gender Issues, 37(1), 61-89.

Austin, G. (2010). African economic development and colonial legacies (Vol. 1, No. 1, pp. 11-32). Institut de hautes études internationales et du développement.

Balogun, J. A. (2020). Commentary: Lessons from the USA delayed response to the COVID-19 pandemic. African journal of reproductive health, 24(1), 14-21.

Bangura, A. K. (2019). The "Arab Spring": An Epitome of Western Political Machinations.

Baylon, C., & Antwi-Boasiako, A. (2016). CHAPTER SIX: INCREASING INTERNET

Barabanov, O. N., & Maslova, E. A. (2019). The Concept of Global Commons as a Factor of Global Instability. Mirovaia ekonomika i mezhdunarodnye otnosheniia, 63(8), 55-63.CONNECTIVITY WHILE COMBATTING. Cyber Security in a Volatile World, 77.

Bello, Ganiyu, et al. "Biology Education and Bio Entrepreneur Opportunities in Nigeria." Nigerian Online Journal of Educational Sciences and Technology 1.2 (2020): 1-17.

Boo, H. W. (2017). An assessment of North Korean cyber threats. The Journal of East Asian Affairs, 97-117.

Botvinick, M., Ritter, S., Wang, J. X., Kurth-Nelson, Z., Blundell, C., & Hassabis, D. (2019). Reinforcement Learning, Fast and Slow. Trends in Cognitive Sciences, 23(5), 408–422. https://doi.org/10.1016/J.TICS.2019.02.006

Bredtmann, J., Martínez Flores, F., & Otten, S. (2019). Remittances and the brain drain: Evidence from microdata for Sub-Saharan Africa. The Journal of Development Studies, 55(7), 1455-1476.

Brown, S., Korea, -Suny, & Korea, S. (2021). ARTIFICIAL INTELLIGENCE IN THE GLOBAL SOUTH (AI4D): POTENTIAL AND RISKS. https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf

Castro, D., & New, J. (2016). The promise of artificial intelligence. Center for Data Innovation, 1-48.

Cherif, R., & Hasanov, F. (2019). The Leap of the Tiger: Escaping the Middle-income Trap to the Technological Frontier. Global Policy, 10(4), 497-511.

Chukwu, M. O. (2020). Projects of Economic and Social Development in the Global South: The 20th and 21st-century developmental trends and their impacts.

Corlett, R.T., Primack, R.B., Devictor, V., Maas, B., Goswami, V.R., Bates, A.E., Koh, L.P., Regan, T.J., Loyola, R., Pakeman, R.J. and Cumming, G.S., 2020. Impacts of the coronavirus pandemic on biodiversity conservation. *Biological conservation*, *246*, p.108571.

Crosston, M. D. (2011). World gone cyber MAD: How "mutually assured debilitation" is the best hope for cyber deterrence. Strategic studies quarterly, 5(1), 100-116.

Cumming, G. S. (2020). Impacts of the coronavirus pandemic on biodive ity conservation. Biological Conservation, 246, 108571.
CUNNINGHAM, M. A. (2020). A National Strategy for Synthetic Biology. Strategic Studies Quarterly, 14(3).
Deeks, A., 2020. Defend forward and cyber countermeasures. *Ashley Deeks, Defend Forward and Cyber Countermeasures, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper*, (2004).
Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., ... & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting us food and agricultural system. Frontiers in bioengineering and biotechnology, 7, 63.
Dunham, K. (2008). Mobile malware attacks and defense. Syngress.
Dyer, O. (2020). Trump claims public health warnings on covid-19 are a conspiracy against him. bmj, 368, m941.
Edwards, B., & Revill, J. (2016). Decade of Synthetic Biology in the Context of the Biological and Toxin Weapon Convention and the Chemical Weapon Convention.
Endong, F. P. C., & Obi, P. (2020). "We Are Anything but a 'Shithole'Country!": Exploring Nigerian Online Journalists' Reception of Donald Trump's Insult Politics. In Deconstructing Images of the Global South Through Media Representations and Communication (pp. 273-294). IGI Global.
Englebert, P. (1997). Feature review The contemporary African state: Neither African nor state. Third World Quarterly, 18(4), 767-776.
Fa, J.E., Olivero, J., Farfán, M.Á., Márquez, A.L., Vargas, J.M., Real, R. and Nasi, R., 2014. Integrating sustainable hunting in biodiversity protection in Central Africa: hot spots, weak spots, and strong spots. *PLoS One*, *9*(11), p.e112367.
Falzon, G., Lawson, C., Cheung, K. W., Vernes, K., Ballard, G. A., Fleming, P. J., ... & Meek, P. D. (2020). ClassifyMe: a field-scouting software for the identification of wildlife in camera trap images. Animals, 10(1), 58. Bioengineering and Biotechnology, 7, 51.
Gehl Sampath, P. (2021). Governing Artificial Intelligence in an Age of Inequality. Global Policy, 12(S6), 21–31. https://doi.org/10.1111/1758-5899.12940
George, A.M., 2019. The national security implications of cyberbiosecurity. *Frontiers in bioengineering and biotechnology*, *7*, p.51.
Gewald, J.B., Leliveld, A. and Peša, I. eds., 2012. *Transforming innovations in Africa: Explorative studies on appropriation in African societies* (Vol. 11). Brill.
Gohdes, A.R. (2020), Repression Technology: Internet Accessibility and State Violence. American Journal of Political Science, 64: 488-503. https://doi.org/10.1111/ajps.12509
Goodman, W., 2010. Cyber deterrence: Tougher in theory than in practice?. *Strategic Studies Quarterly*, *4*(3), pp.102-135.
Gronvall, G. K. (2019). Synthetic Biology: Biosecurity and Biosafety Implications. In Defense Against Biological Attacks (pp. 225-232). Springer, Cham.
Gruber, K. (2019). Biohackers: A growing number of amateurs join the do-it-yourself molecular biology movement outside academic laboratories. EMBO reports 20(6), e48397.
Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence: Https://Doi.Org/10.1177/0008125619864925, 61(4), 5–14. https://doi.org/10.1177/0008125619864925
Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace.
Harnischfeger, J. (2019). Biafra and secessionism in Nigeria: An instrument of political bargaining. In Secessionism in African Politics (pp. 329-359). Palgrave Macmillan, Cham.
Hernandez, L. (2021). How Rwanda's AI policy helps to shape the evolving AI ecosystem. https://digicenter.rw/how-rwandas-ai-policy-helps-to-shape-the-evolving-ai-ecosystem/
Iasiello, E. (2014). Is cyber deterrence an illusory course of action?. Journal of Strategic Security, 7(1), 54-67.
Imperiale, M., Boyle, P., Carr, P. A., Densmore, D., DiEuliis, D., & Ellington, A. (2018). Biodefense in the Age of Synthetic Biology.
Kong, D. S., & Bakker, N. (2018, August). Community driven design of living technologies. In Proceedings of the 15th Participatory Design Conference: Short Papers, Situated Actions, Workshops and Tutorial-Volume 2 (pp. 1-3).
Kosaki, T., Lal, R., & Reyes Sánchez, L. B. (2020, May). " Soil Education Manual-Toolbox for DIY program at your classroom" by International Union of Soil Sciences (IUSS). In EGU General Assembly Conference Abstracts (p. 21359).
Lakhdhar, Y., Rekhis, S., & Boudriga, N. (2017, December). Proactive damage assessment of cyber attacks using mobile observer agents. In Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia (pp. 29-38).
Lewis, J. A. (2014). National perceptions of cyber threats. Strategic Analysis, 38(4), 566-576.
Marchant, E., & Stremlau, N. (2020). The Changing Landscape of Internet Shutdown in Africa| A Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa. International Journal of Communication, 14, 18.
Makanda, K., Vallent, T. F., & Kim, H. (2017) Remarks on National Cyber Security for under Developed and Developing Countries: focused on Malawi.
Mas, I., & Radcliffe, D. (2010). Mobile payments go viral: M-PESA in Kenya.May, J. F., & Rotenberg, S. (2020). A Call for Better Integrated Policies to Accelerate the Fertility Decline in Sub-Saharan Africa. Studies in Family Planning, 51(2), 193-204.
MILLETT, K. K., dos Santos, E., & MILLETT, P. D. (2019). Cyber-Biosecurity Risk Perceptions in the Biotech Sector.
Ministry of Information Technology and Communication, 2017. ICT Sector Strategic Plan (2018-2024) - "Towards digital-enabled economy". Rwanda: MITEC.

Mueller, S. (2020). Facing the 2020 Pandemic: What does Cyberbiosecurity want us to know to safeguard the future?. Biosafety and Health.

Murch, R., & DiEuliis, D. (Eds.). (2019). Mapping the cyberbiosecurity enterprise. Frontiers Media SA.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology, 6, 39.

Ndayisaba, A. (2020). Rwanda-Burundi: Political Dialogue as a Method of Achieving Agreement. RUDN Journal of Political Science, 22(1), 105-115.

Nkusi, Fred. "Creating the National Cyber Security Authority Is Vital," April 30, 2017. https://www.newtimes.co.rw/section/read/211603.

Olubela, M. O. (2018). Shithole Countries: An Analysis of News Coverage in the US. Republic of Rwanda, National Cyber Security Strategy (Republic of Rwanda, Kigali, 2015)

Palmer, X. L., & Karahan, S. (2020, March). Defending Forward: An Exploration through the Lens of Biocybersecurity. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (p. 373). Academic Conferences and publishing limited.

Palmer, X., Potter, L.N. and Karahan, S., 2021. COVID-19 and biocybersecurity's increasing role on defending forward. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *11*(3), pp.15-29.

Potter, L., Ayala, O., & Palmer, X. L. (2020). Biocybersecurity--A Converging Threat as an Auxiliary to War. arXiv preprint arXiv:2010.00624.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. Trends in biotechnology, 36(1), 4-7.

Ramesh, A., Dhariwal, P., Nichol, A., Chu, C., & Chen, M. (2022). Hierarchical Text-Conditional Image Generation with CLIP Latents. arXiv. https://doi.org/10.48550/arXiv.2204.06125

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: a call for cooperation in a new threat landscape. Frontiers in bioengineering and biotechnology, 7, 99.

Republic of Rwanda, National Cyber Security Strategy (Republic of Rwanda, Kigali, 2015)

Sarpong, D., Ofosu, G., Botchie, D., & Clear, F. (2020). Do-it-yourself (DiY) science: The proliferation, relevance and concerns. Technological Forecasting and Social Change, 158, 120127.

Samori, I. A., Palmer, X. L., Potter, L., & Karahan, S. (2023). Commentary on Biological Assets Cataloging and AI in the Global South. In Proceedings of SAI Intelligent Systems Conference (pp. 734-744). Springer, Cham.

Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. Intelligence and National Security, 35(3), 444-453.

Tor, U. (2017). 'Cumulative deterrence'as a new paradigm for cyber deterrence. Journal of Strategic Studies, 40(1-2), 92-117.

Turianskyi, Y. (2020). Africa and Europe: Cyber Governance Lessons. South African Institute of International Affairs. https://media.africaportal.org/documents/Policy-Insights-77- turianskyi.pdf

Turner, G. (2019, May). The Growing Need for Cyberbiosecurity. In InSITE 2019: Informing Science+ IT Education Conferences: Jerusalem (pp. 207-215).

Tylecote, A. (2019). Biotechnology as a new techno-economic paradigm that will help drive the world economy and mitigate climate change. Research Policy, 48(4), 858-868.

Vinatzer, B. A., Heath, L. S., Almohri, H. M., Stulberg, M. J., Lowe, C., & Li, S. (2019). Cyberbiosecurity Challenges of Pathogen Genome Databases. Frontiers in bioengineering and biotechnology, 7, 106.

Wamuchiru, E., & Moulaert, F. (2018). Thinking through ALMOLIN: the community bio-centre approach in water and sewerage service provision in Nairobi's informal settlements. Journal of Environmental Planning and Management, 61(12), 2166-2185.

Williams, Q. (2020). 19 Rejoinders from the Shithole. Language in the Trump Era: Scandals and Emergencies, 265.

Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., . . . Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4), 100179. https://doi.org/10.1016/j.xinn.2021.100179