The Multilateral Integration of Blockchain, Ethical Packet Sniffing and AI for Cybersecurity in BRICS

Blessing Mbalaka
Independent Researcher
bjmbalaka@gmail.com

Executive Summary

This policy brief proposes that the BRICS (Brazil, Russia, India and South Africa) should plan and coordinate on ways to mitigate cybersecurity risks on a multilateral level. The BRICS countries are ideal for such a meta-governance mechanism which could coordinate toward the circumvention of some cyber risks. This Policy brief proposes that there should be an integration of blockchain technologies, packet sniffing technologies and AI detection tools to help mitigate emerging cybersecurity risks. The policy brief outlines the risks and challenges prevalent in this current climate, whilst also proposing potential remedies sourced from rigorous academic studies. The precise amendments include the synthesised mechanism of blockchain-based internet registries, packet sniffing technologies AI verification tools and capacity building to aid in the mitigation of cybersecurity risks. In 2007, a cyber-attack in Brazil plunged more than 3 million people into darkness.[1] Cyberattacks collectively cost the BRICS countries $50.3bn in 2013.[2] These funds could have been reinvested into the economy. BRICS needs the rapid technological integration of cyber-crime mitigation tools, tools which this policy brief will outline.

Introduction

Current Cybersecurity risks and challenges

As the world becomes more digitized, the risks of cyberattacks are becoming an increasing concern for society. Disruptive technologies are being birthed in a digital warzone encompassing of malicious actors looking to capitalise on cyber-security vulnerabilities. Cybercrimes in this emerging and rapidly changing world evolved to encompass new techniques which challenge policymakers. Some instances of cybercrime can be noted from the stolen data saga, in which the data of 1 billion citizens in China was stolen, in 2022.[3] This same source states that the Shanghai police department was hacked by a hacker claiming to have attained personal information from the Chinese police department. The perpetrator of the pre-noted hack, 'Chinadan', demanded 10 bitcoins, an amount of $200000 for the data on the dark web. The dataset included ID records, personal addresses and birth records.[4] These stolen records can be used to conduct fraudulent activities. The world is in a battle against cybersecurity, and it is important to be cognizant of these risks which include botnets, ransomware, digital extortion, online scams and work email hacks.[5]

[1] Brenner, J.F. 2013. Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the atomic scientists*, 69(5):15-20.

[2] Norton. 2013. Norton Report 2013. Accessed at: 2013 Norton Report | NortonLifeLock. Date (Accessed 2023/05/14)

[3] The Guardian. 2022. Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens._4 July 2022. [Online]. Available at: https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens [Accessed 2023/05/14].

[4] Business Day. 2022. 'ChinaDan' offers Hacked Police Records on Chinese Citizens for 10 Bitcoin., 6 July 2022. [Online]. Available at: https://www.businesslive.co.za/bd/world/asia/2022-07-06-chinadan-offers-hacked-police-records-on-chinese-citizens-for-10-bitcoin/

[5] INTERPOL (2021) Interpol. 2021. INTERPOL report identifies top cyberthreats for Africa. Accessed from: https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in Africa#:~:text=The%20INTERPOL%20

Raconteur, cited by the world Economic Forum, found that $6.6 million had been lost from the public sector in 2017 due to cyberattacks. This figure grew by 20% in 2018.[6] The report cited findings from Raconteur which found that cybercrime had been caused by malicious insiders.

The policy brief aims to frame the numerous cybersecurity risks which are prevalent in the increasing digital landscape. The policy brief explores the geopolitically induced state sponsored cyber-attacks. This section looks to emphasize the risks posed by the echoing of geopolitical conflicts on the internet. BRICS countries, as all countries are at risk from pre-existing cyber-attacks and the weaponization of numerous innovations such as AI (artificial intelligence) enhanced cyberattacks.

These concerns were highlighted by a 2013 study by the international antivirus company Norton.[7] Norton conducted a study into 24 countries, and from that study it found that globally, 61% of adults had experienced a form of cybercrime. This figure was 73% in South Africa, with an average cost of $233 per victim. The figure below depicts the cost incurred on BRICS countries due to cybercrime.

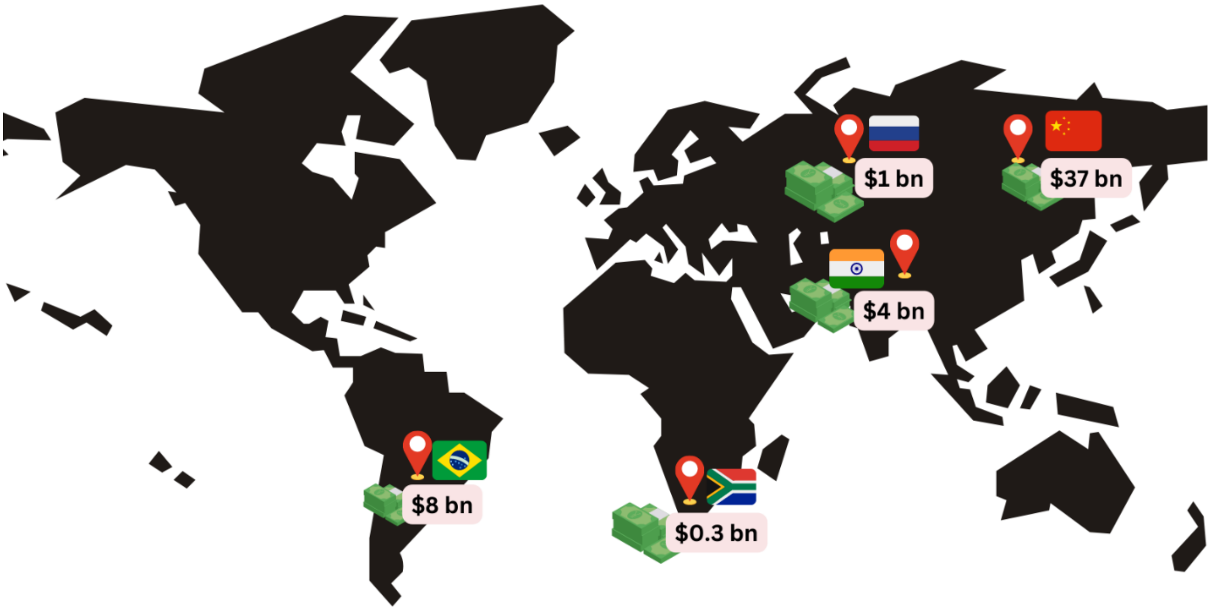

Figure 1: Cost of Cybercrime in BRICS countries

Adapted by the Author from Norton (2013)

The Impacts of Geopolitical Conflicts and State Sponsored cyber-Attacks

The global interconnectedness of the internet has led to geopolitical conflicts being echoed in the cyber space (online). The global interconnectedness of the internet has been integral to the improvements in global telecommunications. However, Akoto states that there is an infamous aspect from these innovations.[8] The global geopolitical conflicts prevalent in the quest for hegemonic status are hyper-competitive, which leads to the issue of state-sponsored cyber-attacks.[9] State-sponsored

report%20identifies%20the%20most%20prominent%20threats,trick%20individuals%20into%20revealing%20personal%20or%20financial%20information%3B

[6] World Economic Forum. 2019. This Is the Crippling Cost of Cybercrime on Corporations. Accessed at: This is the true cost of cybercrime, according to experts | World Economic Forum (weforum.org)

[7] ???

[8] Albahar, M. 2019. Cyber attacks and terrorism: A twenty-first century conundrum. *Science and engineering ethics*, (*25*): 993-1006.

[9] Nguyen, D. 2015. State sponsored cyber hacking and espionage. *Infosec Writers*.[online] Available at: State Sponsored Cyber Hacking and Espionage (infosecwriters.com)

attacks comprise computational attacks on digitally run infrastructure.[10] These include espionage, financial gain and terrorism. Akoto,[11] cited above, expresses these sentiments by highlighting how trade secrets attained through cyber-espionage could lead to economic growth by boosting domestic production.

Risk of AI Weaponization

The recent disruptions in the field of AI with the generative pre-trained AI Chat GPT has opened a pandora's box in which code and the ability to generate programmes can now be generated with a simple text search. This technology, if it is made without safety parameters could lead to the emergence of AI tools for espionage. This risk needs to be closely monitored.

Extortion via deepfakes can be used for ransom attacks, and manipulation of key state actors for critical information.[12] Information coerced from the targeted individuals could jeopardise national security and critical infrastructure. Deepfake (AI generated face-swapping technology) attacks can be embarrassing and humiliating tools for coercing compliance from political elites or individuals. Targeted individuals could be coerced into making decisions which expose security vulnerabilities of the state. This weaponization can be addressed by the mainstreaming of deepfake detection tools. However, once one is exonerated from the published deepfake, humiliation still remains. in the current Indian election season is an event which is warned to contribute to catastrophic implications which challenge the very integrity of the elections through the use of weaponised deepfakes.[13] The BRICS countries need to share a strong unified front and propose for algorithmic augmentation which incorporates deepfake detection tools. Some detection approaches, which are showing signs of early promise are camera fingerprints and biological signal-based schemes.[14] There is no clear way to directly link deepfakes with election outcomes without calculating precise public sentiments, sentiments which cannot be validated objectively. but this is a correlation worth investigating in future studies. Similar malicious use has been depicted in South Africa by Marwala.[15] These challenges, synonymous to Marwala's earlier accounts has contributed to the unilateral prohibition of deepfake use during the election season.[16]

Policy propositions

Cybercrime has nuances which require a multi-pronged approach to mitigate some cyber-crime concerns. The following section proposes an integration of Blockchain technology[17], packet sniffing technology and AI technology to aid in the circumvention some cybercrime.

[10] Akoto, W. 2021. International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, 58(5):1083-1097.

[11] Norton., 2013. 2013 Norton Report. Accessed at: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/norton-report-2013-sa.pdf

[12] Zeng, C. and Olivera-Cintrón, R. 2019. Preparing for the world of a perfect deepfake. *Dostopno na*: https://czeng. org/classes/6805/ Final. pdf *(18. 6. 2020).*

[13] George, A.S., 2023. Regulating Deepfakes to Protect Indian Elections. *Partners Universal Innovative Research Publication*, *1*(2), pp.75-92.

[14] Yu, P., Xia, Z., Fei, J. and Lu, Y., 2021. A survey on deepfake video detection. *Iet Biometrics*, *10*(6), pp.607-624.

[15] Maree, A., 2021. South Africa: Leaks and Deepfakes Shaping the Race for ANC Presidency. The African Report.

[16] Tardáguila, C., 2024. New Analysis Reveals Scope of 'Fake News' Referencing or Produced by AI in Brazil; Little Related to Elections or Democracy, For Now. Tech Policy.

[17] Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R. 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2):147-156.

[12.] Yu, P., Xia, Z., Fei, J. and Lu, Y., 2021. A survey on deepfake video detection. *Iet Biometrics*, *10*(6), pp.607-624.

Multilateral Internet Regulation Agreements and Regulations Across BRICS countries

The BRICS countries could form a centralized BRICS ISP and internet regulatory body which exchanges in skills and innovations surrounding ISP regulation best practices. The body could be a hub for knowledge transfers which helps bolster the cybersecurity readiness across BRICS nations. The body would integrate the various cyber security strategies in the BRICS countries and propose amendments. The committee would strategize on means to mitigate state sponsored approaches. A similar case of national cooperativeness was prevalent between INTERPOL, China, private sector actors, Malaysia, Indonesia, Myanmar, Singapore, Thailand, Vietnam and the Philippines came together to work cooperatively toward addressing and identifying malicious actors and websites containing malware (software designed for malicious intent). A similar public-private partnership could be used in the BRICS countries to collaboratively mitigate cybercrime concerns.

The Multilateral Integration of Blockchain, AI and Packet Sniffing Technologies

Luca Belli, depiction of the emerging need for data-protection infrastructure and digital sovereignty in the data-driven societies 'scramble for data' suggests that there is a need to establish protective digital infrastructure to mitigate unscrupulous cybersecurity risks. Luca Belli further states that the BRICS countries need to improve readiness by ensuring that their laws are well adept to the rapidly evolving technological climate.[18]

Currently, there is an array of cybersecurity and data protection laws, however, the malicious use of AI has made it necessary to consider an array of mitigation tools which address the issues associated with the incoming and present cybersecurity risks. These laws include:

- The protection of personal information act in South Africa[19]
- The Cybercrimes Act of 2019 in South Africa[20]
- The Information Technology (IT) Act of 2000[21]
- China's cyber security law[22]
- The worrying increase of cybercrime in Russia[23] and the subsequent "Federal Law of 26 July 2017 No. 187-FZ On Security of Critical Informational Infrastructure of the Russian Federation ("the Law")".

These laws are cognizant of the need for data protection measures, however, the issue of AI and cybercrime is a new problem which requires solutions.

AI mainstreaming poses a serious challenge to the limitations of these legislative approaches. These acts are cognizant of conventional cybercrimes such as fraud, denial of service attacks and phishing scams. However, the emergence of AI and deepfake technology poses a serious challenge for regulators. Malicious AI use for cybercrime and hacks is a serious threat to state digital infrastructure

[18] Belli, L. ed., 2021. *CyberBRICS: Cybersecurity regulations in the BRICS countries.* Springer Nature.

[19] Parliament of South Africa.,2013. Protection of Personal Information Act No. 4 of 2013.

[20] Parliament of South Africa., 2019. Cybercrimes Act of 2019.

[21] PWC.,2024. A comparison of cybersecurity regulations: India. Accessed at: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html

[22] KPMG., 2017. Overview of China's Cybersecurity Law. Accessed at: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

[23] Ortner, D., 2015. Cybercrime and punishment: The Russian Mafia and Russian responsibility to exercise due diligence to prevent trans-boundary cybercrime. *BYU L. Rev.*, p.177.

and to the people. The states must adopt iterative adoption of strategies to help adapt in this rapidly changing technological landscape.

There is a huge policy gap absent in BRICS countries and this is the multilateral integration of Blockchain, AI and packet sniffing technologies for cybersecurity prevention. China is the only country which incorporated packet sniffing technologies in the "Great Fire Wall of China" whilst also nullifying web activity from numerous dark web websites.[24] Ethical Packet sniffing enables the internet service provider a way to scan and identify unscrupulous activity on the dark web. There is a plethora of cybersecurity concerns which require expert consultation from ethical hackers who are well trained on issues such as packet injections, malicious packet sniffing within the intranet, weak encryption on government websites.[25] Ethical hackers are well trained in identifying security vulnerabilities on websites.[26] These ethical hackers could be tasked with rigorously testing the government infrastructure across the BRICS nations by assessing areas worth strengthening with Blockchain technology, packet sniffing technology and AI tools.

Lesson from the Great Fire Wall of China, Ethical Packet sniffing and AI

The Laws today need to be adjusted to cater for the emerging threats. Implementing harsh policies may lack parliamentary support and may lead to a free internet which is at risk of malicious exploitative uses. China has been subject to public scrutiny following its firm approach to internet regulation.[27] However, replicating the gains from the Chinese approach poses a serious challenge in the realm of liberal democratic ideals. The liberal democratic ideals advocate against censorship and promote ideas such as freedom of speech and access to information.[28]

China has found a way to mitigate tor dark web access and mitigate malicious website entry. The approach of a targeted firewall which mitigates specific malware and screens information on the country's internet is a potential solution to cyber-attacks. The software can be decentralised to a non-state actor that monitors the traffic using packet sniffing technology. Packet sniffing technology could be integrated with a screening AI algorithm to search for malicious websites.

There is a technique which is called 'ARP Cache Poisoning'. This technique enables a middleman, to monitor the internet activity to monitor websites which are not encrypted by security protocols such as SSL. This could help to monitor websites which do not have such protections identify their IP addresses and disconnect them from the internet.

However, the levels of tolerance for censorship vary from state to state. The liberal democratic ideals make compliance with totalitarian policies difficult and may lead to a rejection of extreme censorship approaches. Despite the loosening grip of liberal democracy,[29] the ideals may remain determinants of policy directions. South Africa, much like most of BRICS are subject to an array of laws which protect data and govern the proper use of the internet, however, there are always around the law, and these loopholes, such as dark web access pose a serious challenge for policymakers. The

[24] Ensafi, R., Fifield, D., Winter, P., Feamster, N., Weaver, N. and Paxson, V. 2015, October. Examining how the great firewall discovers hidden circumvention servers. In *Proceedings of the 2015 Internet Measurement Conference*. (2015): 445-458.

[25] Patil, S., Jangra, A., Bhale, M., Raina, A. and Kulkarni, P. 2017, September. Ethical hacking: The need for cyber security. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*:1602-1606.

[26] Palmer, C.C. 2001. Ethical hacking. *IBM Systems Journal*, 40(3):769-780.

[27] Zheng, H., 2013. Regulating the internet: China's law and practice. *Beijing L. Rev.*, *4*, p.37.

[28] Busch, A., Theiner, P. and Breindl, Y., 2018. Internet censorship in liberal democracies: Learning from autocracies?. *Managing democracy in the digital age: Internet regulation, social media use, and online civic engagement*, pp.11-28.

[29] Habets, I., 2015. Liberal democracy: The threat of counter-narratives. *European View*, *14*(2), pp.145-154.

Chinese approach is a firm remedy that can mitigate a lot of problems, but it is a contradiction to the right to the internet which much of BRICS will raise.

Blockchain for Cyber Security

Blockchain technology has the potential to transform cybersecurity by creating securitized state and digital infrastructure which operates on blockchain technology. The technology is beneficial because it is immutable because it can be altered with the 51% node consensus attack.[30] The cost, resources and computational power required makes this attack unlikely.[31] The decentralised network would be difficult for hackers to compromise nor attain the encrypted data. However, blockchain is very energy intensive and this may present unintended environmental impacts. Furthermore, the energy crisis in South Africa may make the processing of blockchain problematic.

ISP (Internet Service provider) Monitoring and Blockchain Integration

The BRICS countries, despite their relations maintain their own internal-state sovereignty. This implies that each of the countries in BRICS have their own guidelines and practices which govern these states respectively. These bodies include Brazil's National Telecommunications Agency; Russia's Federal Service for Supervision of Communication, Information technology; The Indian Telecom Regulatory Authority of India and the Chinese Ministry of Industry and information Technology and the South African Independent Communications Authority of South Africa. These bodies respectively monitor and regulate the practices of ISPs in the countries. These bodies could be bolstered with the capacity to form a blockchain based website registry. The integration of blockchain technology into a website registry, a globally verified website registry that only allows access to websites registered to be permissible for ISP providers could help prevent the access of fly by night websites which look to expose security vulnerabilities. The website would verify the websites, similarly to how websites are verified on the bitcoin transaction ledger. This would help to mitigate fly by night scams such as colleges, and online stores.

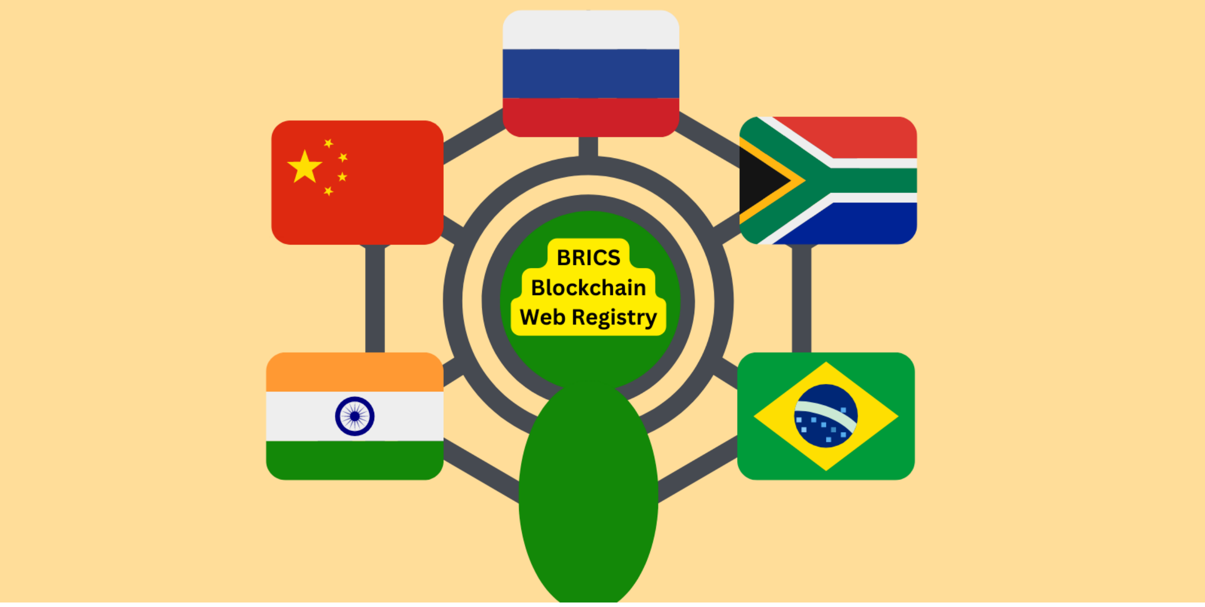

Figure 2: BRICS Blockchain Web Registry, Author (2023).

[30] Sayeed, S. and Marco-Gisbert, H. 2019. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied sciences*, 9(9): 1788.

[31] Eyal, I. and Sirer, E.G. 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7): 95-102.

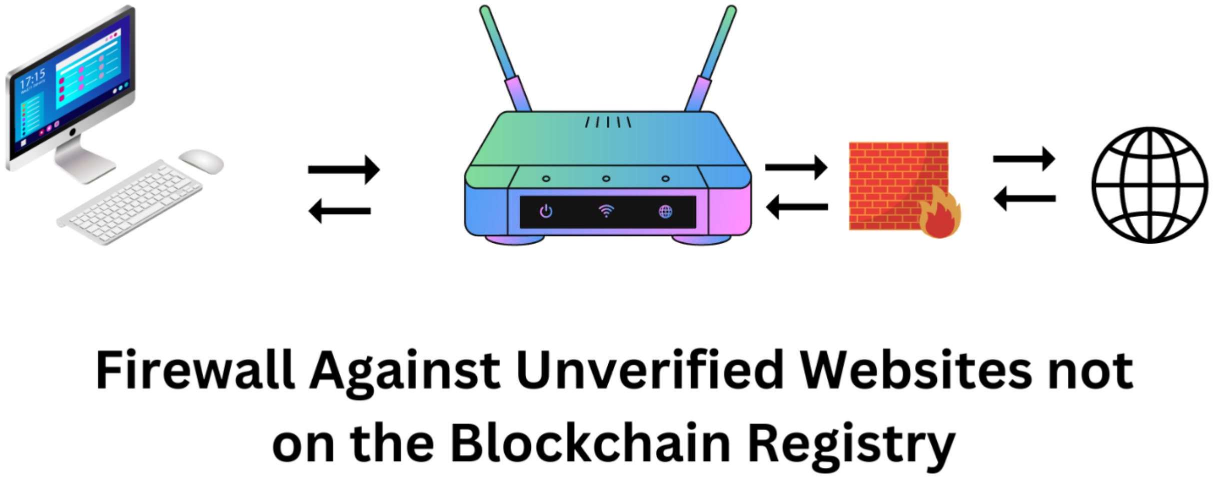
Firewall Against Unverified Websites not on the Blockchain Registry

Figure 3: Firewall for BRICS web Registry, Author (2023).

Mandatory Cyber security Training

The training of staff on cyber-security awareness and mitigation needs to be a mandatory practice for all personnel involved in state infrastructure. In some instances, hacking can be done by merely sharing an email with an encrypted virus, and phishing or smishing deception.[32] Challenges in coordinating training, financing and adapting the training may need to be addressed.[33]

Free AI content screening mechanisms and Free, open-source Anti-virus software

The use of AI website monitoring tools could be made mandatory for all websites registered to the website registry. The AI would be a content-scanning apparatus which monitors websites for cybercrime.[34] Although, it is important to be cognizant of the challenge posed by malicious actors who could weaponise AI to beat these safety nets. State-sponsored hacks and other instances of weaponised AI programmes create a dilemma for policymakers who seek to regulate the use of AI online. This contradiction may be a ceaseless dilemma which may require a perpetual dialogue surrounding the implementation of iterative adaptive strategies.[35]

The utilisation of open-source free anti-virus software could help to mitigate the issue of cost and improve cybersecurity for employees in the office and in their homes. The poverty in South Africa and around the world may make access to such software challenging. A state-sponsored software could help resolve the issue of cost.

[32] Yeboah-Boateng, E.O. and Amanor, P.M., 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4):297-307.

[33] Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3):73.

[34] Kawaguchi, Y., Yamada, A. and Ozawa, S., 2017. Ai web-contents analyzer for monitoring underground marketplace. In *Neural Information Processing: 24th International Conference, ICONIP 2017, Guangzhou, China, November 14–18, 2017, Proceedings, Part V 24* (pp. 888-896). Springer International Publishing.

[35] Yamin, M.M., Ullah, M., Ullah, H. and Katt, B., 2021. Weaponized AI for cyber attacks. Journal of Information Security and Applications, 57, p.102722.

References

Brenner, J.F. 2013. Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bulletin of the atomic scientists*, 69(5):15-20. https://doi.org/10.1177/0096340213501372

Norton. 2013. Norton Report 2013. Accessed at: 2013 Norton Report | NortonLifeLock. Date (Accessed 2023/05/14)

The Guardian. 2022. Hacker Claims to Have Obtained Data on 1 Billion Chinese Citizens., 4 July 2022. [Online]. Available at: https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens [Accessed 2023/05/14].

Business Day. 2022. 'ChinaDan' offers Hacked Police Records on Chinese Citizens for 10 Bitcoin., 6 July 2022. [Online]. Available at: https://www.businesslive.co.za/bd/world/asia/2022-07-06-chinadan-offers-hacked-police-records-on-chinese-citizens-for-10-bitcoin/

INTERPOL (2021) Interpol. 2021. INTERPOL report identifies top cyberthreats for Africa. Accessed from: https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in Africa#:~:text=The%20INTERPOL%20report%20identifies%20the%20most%20prominent%20threats,trick%20individuals%20into%20revealing%20personal%20or%20financial%20information%3B

World Economic Forum. 2019. This Is the Crippling Cost of Cybercrime on Corporations. Accessed at: This is the true cost of cybercrime, according to experts | World Economic Forum (weforum.org)

Albahar, M. 2019. Cyber attacks and terrorism: A twenty-first century conundrum. *Science and engineering ethics*, (*25)*: 993-1006. https://doi.org/10.1007/s11948-016-9864-0

Nguyen, D. 2015. State sponsored cyber hacking and espionage. *Infosec Writers.*[online] Available at: State Sponsored Cyber Hacking and Espionage (infosecwriters.com)

Akoto, W. 2021. International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, 58(5):1083-1097. https://doi.org/10.1177/0022343320964549

Zeng, C. and Olivera-Cintrón, R. 2019. Preparing for the world of a perfect deepfake. *Dostopno na*: https://czeng. org/classes/6805/Final. pdf *(18. 6. 2020).*

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R. 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2):147-156. https://doi.org/10.1016/j.dcan.2019.01.005

Yu, P., Xia, Z., Fei, J. and Lu, Y., 2021. A survey on deepfake video detection. *Iet Biometrics*, *10*(6), pp.607-624. https://doi.org/10.1049/bme2.12031

Ensafi, R., Fifield, D., Winter, P., Feamster, N., Weaver, N. and Paxson, V. 2015, October. Examining how the great firewall discovers hidden circumvention servers. In *Proceedings of the 2015 Internet Measurement Conference.* (2015): 445-458. https://doi.org/10.1145/2815675.2815690

Patil, S., Jangra, A., Bhale, M., Raina, A. and Kulkarni, P. 2017, September. Ethical hacking: The need for cyber security. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*:1602-1606. https://doi.org/10.1109/ICPCSI.2017.8391982

Palmer, C.C. 2001. Ethical hacking. *IBM Systems Journal*, 40(3):769-780. https://doi.org/10.1147/sj.403.0769

Sayeed, S. and Marco-Gisbert, H. 2019. Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied sciences*, 9(9): 1788. https://doi.org/10.3390/app9091788

Eyal, I. and Sirer, E.G. 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7): 95-102. https://doi.org/10.1145/3212998

Yeboah-Boateng, E.O. and Amanor, P.M., 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4):297-307.

Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3):73. https://doi.org/10.3390/fi11030073

Kawaguchi, Y., Yamada, A. and Ozawa, S., 2017. Ai web-contents analyzer for monitoring underground marketplace. In *Neural Information Processing: 24th International Conference, ICONIP 2017, Guangzhou, China, November 14–18, 2017, Proceedings, Part V 24* (pp. 888-896). Springer International Publishing. https://doi.org/10.1007/978-3-319-70139-4_90