JAD Call for Special Issue:

Cyber Frontiers, and Building Economies Back Better in a Digital Age

Summary

Today, and more frequently, most internet users in our global community are potentially under attack. As these online or web-related threats evolve, attacks become more polymorphic, and cybercriminals continue to become more sophisticated in these big data and technologies-driven digital age. By implication, the rapidly shifting cyber landscape is requiring prompt and proactive risk mitigation interventions that are more than mere prevention or a one-size-fits-all solutions.

Since 2005, thirty-four countries are suspected of sponsoring cyber operations, while there was a total of seventy-six operations, most being acts of espionage (Council Foreign Relations (CFR)'s Cyber Operations Tracker, 2020). Relevant interventions aimed at overcoming cybersecurity challenges include *inter alia:* biometrics, business management or database administration, crime investigation, connectivity infrastructure, information systems, programming, systems engineering, critical information infrastructure assurance, defense operations, cryptography, data science, digital and multimedia forensics, information technology, network management, systems security, etc. Consequently, most OECD nations or developed countries continue to explore diversely digital, legislative, and cyber-strategies in salvaging collapsing businesses, reducing systemic shocks, and enhancing post-pandemic socioeconomic trajectories.

Even though cybersecurity remains one of the fundamental drivers of bringing economies back better, and about seventy-six countries publicly boast of national cybersecurity strategies, the post-pandemic capacities are seemingly transcending beyond mere participation in cybersecurity to encompass strategic information superhighway involvement, contribution, and inclusion in the globally standardized cyber frontiers (Goel, 2020; ITU, 2018). For instance, with the meteoric expansion in the digitalization and virtualization of education, workforce, supply chain, e-government, e-health, e-trade, e-agriculture etc amidst less robust security measures in place, many enterprises experienced cybersecurity risks such as intelligence theft, digital fraud, public infrastructure sabotage, net neutrality, illicit financial flows, cyber espionage, hacktivism, internet censorship and national security breaches (CSEA, 2021; Barrinha & Renard, 2017). In other words, cybercriminals are taking advantage of the pandemic situation and unprecedented cyberattacks are being experienced across trade-in-services sub-sectors and over (digital) national borders (Goel, 2020). In view of this, cyber-frontiers, digitalization, and socioeconomic transformation nexus preparedness policies will help businesses overcome unprecedented hurdles, make prompt decisions to enable remote work scaling, deliver virtual care, maintain businesses continuity, and enhance global realization of the UN SDGs (Calderaro & Craig, 2020; Manantan, 2021). Enterprises and governments are seemingly becoming more fortified by bypassing internet and directly accessing cloud connection via major cloud providers such as Amazon Web Services, Microsoft Azure and Google Cloud Platform.

Addressing cyber-related challenges could include measures such as cyber capacity building, cyber-physical power system (CPPS), cyber-diplomacy, cyberwarfare, election security, fortifying energy infrastructure, establish an income tax credit for investment in qualified businesses that develop cybersecurity and artificial intelligence (AI), cyber investment incentive tax credit program, invest resources in digital literacy and cyber safety of public websites, creates the of cyberterrorism, establish school district cyber-crime prevention services program, establish civilian cyber security reserve forces, creates cybersecurity enhancement fund to be used for upgrading cyber security in local governments, cyber initiatives to encourage economic development in cybersecurity fields, calculate damages caused by computer tampering, regulating cyber-laws in industries like insurance, protect privacy, safeguard sensitive information, enable public officials to detect, investigate, respond to and prevent cyberattacks that threaten public health and safety, preserve business confidentiality, incentivizing cyber training, and finally setting up formal policies, standards and practices (Willers, 2021; Wu, Li & Li, 2020; Journal of Self-Governance and Management Economics, 2020; Lancelot, 2020).

The International Telecommunication Union (ITU) June 2021 Global Cybersecurity Index (GCI) reveals that Africa's commitment as well as its legal, technical, organizational and cooperation capacities to respond to cybersecurity threats are comparatively lower across other continents (ITU, 2020). However, a few countries such as Tanzania, Mauritius and Rwanda exhibit better cybersecurity index for digital rights and cross-border collaborations on the continent. As Africa benefits from the exponential expansion of digital revolution, this ongoing trajectory can enhance the Africa's realization of a cyber frontier agenda, as well as the realization of the UN SDGs and African Union 2063 agenda at a record time. Thus, cybersecurity best practices are required to stay abreast of cybersecurity policies, strengthen capacities for cyber research, build stronger cyber-related educational programs, as well as to keep information and information systems more secure as workers connect to potentially unsecured home networks while accessing company resources from personal devices.

One of the essential and resilient roads to macroeconomic shock recoveries is to deploy socio-cyber-physical systems for brining businesses back better as well as fostering socioeconomic transformation (Rijswijk et al, 2021, Odularu and Adekunle, 2020). Based on this background, the broad research objective of this JAD's special call is to critically assess and recommend tools, that informs businesses and government's post-pandemic hyperspace responses towards leveraging ICTs' confidence, security, and trust in achieving safer and more sustainable development targets. Leveraging on the ITU Guide to Developing National Cybersecurity Strategy, as well as the challenges and opportunities confronting Africa, this JAD's special call for papers will analyze socioeconomic shocks being faced by businesses and countries with specific focus on digitalization and cyber interventions. More specifically, this JAD's special call for articles will address, but not limited the following potential cyber interventions topics:

- Cyber frontiers policy implications of socioeconomic preparedness, cross border trade, regional cooperation, and illicit financial flows in the post-pandemic era.
- Collaborative cyber interventions and platform economics for cyber-vulnerable households, (minority) micro, small, and medium enterprise (MSMEs) towards enhancing supply chains, data governance and inter-sectoral socioeconomic recovery programs.

Specific empirical studies have revealed the role that renewed government attention in cyber, diagnostics, and appropriate research information may play as key preparedness strategies towards overcoming the current and future challenges associated with the diseases outbreak and socioeconomic shocks. In view of this, this JAD's special call will provide deeper understanding on the relationship between strategic businesses, national economic priorities, and cyber frontiers agenda as enterprises and governments are continuing to reach tipping points and 'bleeding' edge regarding the volume and dynamics of the threats they face in an increasingly digitalized but vulnerable world.

Keywords: **Threats, safety, cyber-frontiers, capacity building, trust, digital divide, security, intellectual property, cyber vulnerabilities, socio-cyber-physical system, Africa.**

Special Issue Timeline

October 1, 2021 – Launch of the JAD call for special issue
October 25, 2021 – Paper abstracts due to special issue editors
October 31, 2021 – Authors of accepted abstracts notified
December 31, 2021 – Draft full papers due to editors
February 5, 2022 – Reviews and revision requests back to authors
March 5, 2022 – Second drafts due to editors
March 15, 2022 – Final edit suggestions to authors and publication decision.
March 30, 2022 – Final papers due to editors
April 2022 – Technical edit and formatting
May 2022 – Full special issue publication

Abstract Submission
To have your manuscript considered for this special issue, please email an abstract of 300 words to godularu@bau.edu. The abstract should describe the overall theme or topic of the manuscript. Accepted articles will be based on conceptual, empirical, case studies, and methodological research studies. Manuscripts should normally be between 6,000 and 15,000 words, including all notes, table, visualizations, and references.

Other Information
Special Issue Editors: **Professor Gbadebo Odularu (godularu@bau.edu) and copy Professor Sahin (sebnem.sahin@undp.org).**

Full papers for accepted abstract must be submitted through the JAD online by December 31, 2021. All papers will go through a double-bliend peer review process and be available online. All submissions will need to follow the JAD submission guidelines at: Editorial Manager® If you have questions about the special issue, please email the special issue editors.

References

- Andrea Calderaro & Anthony J. S. Craig .2020. Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building, Third World Quarterly, 41:6, 917-938, DOI: 10.1080/01436597.2020.1729729
- Barrinha, A. & T. Renard .2017. Cyber-diplomacy: the making of an international society in the digital age, Global Affairs, 3:4-5, 353-364, DOI: 10.1080/23340460.2017.1414924
- CSEA. (2021). *Are African countries doing enough to ensure cybersecurity and Internet safety?* Www.itu.int. https://www.itu.int/en/myitu/News/2021/09/01/06/54/Are-African-countries-doing-enough-to-ensure-cybersecurity-and-Internet-safety
- CFR's Cyber Operations Tracker, 2020. *Tracking State-Sponsored Cyberattacks Around the World.* Council on Foreign Relations. https://www.cfr.org/cyber-operations/
- Goel, S. .2020.. National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections, 19*(1), 73-86. Retrieved September 5, 2021, from https://www.jstor.org/stable/26934537
- ITU, 2021. *Global Cybersecurity Index 2020*. Www.itu.int. https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020
- International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity.
- Journal of Self-Governance and Management Economics. 2020. Industrial Artificial Intelligence, Business Process Optimization, and Big Data-driven Decision-Making Processes in Cyber-Physical System-based Smart Factories. (2020). *Journal of Self-Governance and Management Economics*, *8*(2), 28–34. https://www.ceeol.com/search/article-detail?id=877667
- Lancelot, J. F. .2020. Cyber-diplomacy: cyberwarfare and the rules of engagement, Journal of Cyber Security Technology, 4:4, 240-254, DOI: 10.1080/23742917.2020.1798155
- Manantan, Mark Bryan F. .2021. Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, Australian Journal of International Affairs, 75:4, 432-459, DOI: 10.1080/10357718.2021.1926423
- Odularu, G., & Adekunle, B. .2020. Understanding Digitalization in the African Context. *Journal of African Development, 21*(1), 1-13. doi:10.5325/jafrideve.21.1.0001
- Rijswijk, K., Klerkx, L., Bacco, M., Bartolini, F., Bulten, E., Debruyne, L., Dessein, J., Scotti, I., & Brunori, G. (2021). Digital transformation of agriculture and rural areas: A socio-cyber-physical system framework to support responsibilisation. *Journal of Rural Studies*, *85*, 79–90. https://doi.org/10.1016/j.jrurstud.2021.05.003
- Willers, J. O. (2021). Seeding the cloud: Consultancy services in the nascent field of cyber capacity building. *Public Administration*. https://doi.org/10.1111/padm.12773
- G. Wu, M. Li and Z. S. Li,. 2020. "Resilience-Based Optimal Recovery Strategy for Cyber–Physical Power Systems Considering Component Multistate Failures," in IEEE Transactions on Reliability, doi: 10.1109/TR.2020.3025179.