Nigerian Journal of Technology (NIJOTECH)
Vol. 43, No. 3, September, 2024
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821

EDITORIAL

While researchers are busy and fixated on their research output, an overwhelming majority is oblivious of potential risk posed by malign actors either operating from the shadows or brazenly attempting to do damage to the research community. Given the high degree of openness that has characterized research activities the world over, cases of exploitation abound. Malign actors which may be individuals with questionable motives, corporate entities, military organizations or government agencies can hide behind the guise of research collaboration to take advantage of unsuspecting researchers which may further translate into collective damage for the researcher's institution. Malign actors engage in a wide range of activities which directly results in intellectual property theft, forced technology transfer and illegal acquisition of sensitive research data.

In order to mitigate against these threats, there have been conversations among stakeholders bordering on Research Security. Research Security is an emerging area which deals with securing research outputs and protecting researchers from exploitation from malign actors. Communities of practice are gradually springing up in various parts of the world including Africa. The African Research Security Consortium is already conducting sensitization workshops in Nigerian universities and intends to extend coverage to other African countries. A couple of governments in North America and Europe are now also taking more than a cursory interest in the subject. Some have already developed policy documents and robust frameworks on research security for researchers, higher education institutions and research producing organisations. Because research collaborations are the indispensable crack in the wall that malign actors exploit, these frameworks and policies dwell on risk assessment and mitigation while at the same time encouraging collaborations. In order to undertake objective risk assessment and activate necessary mitigation measures, researchers and institutions must "know their collaborators". Knowing your collaborators requires that due diligence be done to verify the true identity of the potential collaborator and the risk they pose. Hence, Research Security does not discourage collaborations, but provides guidance for researchers and institutions to (i) know who they are collaborating with, (ii) understand the potential risks of collaborating with certain individuals or organisations and (iii) eliminate risk if possible or minimize them where impossible to totally eliminate. Instead of the dangerously wide open traditional research culture that has fed

exploitation, Research Security introduces a new paradigm that makes research ***"as open as possible but as closed as necessary"***.

Finally, Research Security is a collaborative venture between the government, the institution and the individual researcher and upon this formidable tripod rests the sustainable solution to exploitation by malign actors. But while governments of various countries are still wondering what role to play in this whole new venture, individual researchers are called upon to activate necessary personal protective mechanisms to ward off malign actors. At the institutional levels, the research management offices, the legal units, the intellectual property protection office and the international directorates should work together to develop institution-specific anti-exploitation framework aimed at protecting researchers and the institution from exploitation and the attendant reputational damage. A stitch in time saves nine.

Prof. Chidozie Charles Nnaji
Editor-in-Chief