２Ｃ１９

Research Integrity and Research Security in Open Science Infrastructure, Policies, and Operation & Management: Enhancing the effectiveness of collaborative research across nations and academic disciplines

○Takehito Kamata (Sophia University)
takehitokamata@sophia.ac.jp

1. Research Integrity and Research Security

Policymakers have refined policies on research integrity and security in their countries; however, organizational commitments and responsibilities at the institutional level are more complicated because of technology and digital communication platforms established and advanced within and beyond national borders. Academies and international organizations actively discussed and published statements, policies, and reports to maintain integrity in research and assure security in research [1, 2, 3, 4]. Their policies have been the foundation of the development of policies and programs on research integrity and research security at the international, national, institutional levels around the world. In current interconnected international and interdisciplinary research communities, researchers and stakeholders alike should be aware of research integrity and security complications from the perspectives of academic rank-specific focuses, disciplines, institutions, and nations.

In this paper, I outline and discuss five topics: (a) emerging challenges; (b) policies and practices; (c) three concepts; (d) methods; and (e) findings, discussion, and conclusion. I crafted this prioritized agenda to reconsider the policies and practices to promote research integrity and security at the institutional, national, and international levels based on my recent discussions with leading scholars, professionals, and policymakers at four academic and professional conferences (8th World Conference on Research Integrity, 48th Annual AAAS Science & Technology Policy Forum, International Studies Association 2024 Virtual Conference, and the Science of Team Science 2024 Virtual Annual Conference).

2. Emerging Challenges in Research Integrity and Research Security

Researchers and stakeholders confront emerging challenges in various fields. These challenges are not directly linked to all individual researchers; however, research support professionals need to recognize their institutional responsibility to promote research at the individual and institutional levels. This section outlines three emerging challenges: preserving digital scholarly journals, the rising costs of digital scholarly publications, and developing digital scholarship profiles.

Currently, research outcomes could include presenting research at conferences, publishing scholarly journal articles or books, acquiring patents, and others. One study indicates the challenges in preserving digital publications. Researchers examined the digital object identifiers (DOI) of approximately seven million digital scholarly journals, finding that these journals have not been properly preserved and that 58.38% of digital journals were preserved in only one archive, and 27.64% were not preserved at all [5]. To maintain past and current scholarly publications by developing the DOI registration and enforcing preservation standards across institutions, industries, agencies, and nations, stakeholders need to be aware of the cost.

In addition to the cost of preserving digital scholarly publications, researchers and their affiliated institutions need to be aware of the rising cost of article processing. Haustein et al. (2024) analyzed article processing charges of six major publishers such as Elsevier, Frontiers, MDPI, PLOS, Springer Nature, and Wiley for open access publishing between 2019 and 2023, and they estimated that the annual costs of article processing has tripled from $910.3 million in 2019 to $2.538 billion in 2023 [6]. According to their study, researchers, institutions, and funders should consider the cost of research publications and request decision-making transparency on publication fees. For instance, article submitters have the option to request accelerated review and production time by paying rapid

service fees.

Focusing on scholarly research citations has led researchers into wrong behaviors. Some researchers are eager to pursue research achievements through developing their digital scholarship profile. Researchers have used ChatGPT to create a fictional profile of a researcher with a fictional affiliated institution in Google Scholar. This fictional researcher's outcomes were introduced and listed as the 36th most-cited research in a discipline [7]. There are researchers who do not even reference the original statement in the main test and add the citation to the reference list. This case indicates that some researchers used this technique to manipulate excessive self-citations and purchasing citations to boost their research results. In this case, Google Scholar as the platform provider should recognize this issue and act to prevent fraudulent practices and identity suspicious citation patterns.

3. Policies and Practices on Research Integrity and Security

Policymakers and national leaders have analyzed emerging challenges, identified potential threats to research communities around the world, and maintained a discussion on research integrity and security. In May 2023, the G7 Science and Technology Ministers' Communiqué (2023) discussed the significance of upcoming international initiatives and leadership to promote safe, secure, and open international research collaborations and innovations. The ministers shared current challenges and agreed to promote international collaboration through promoting safe and sustainable use of space, analyzing global climate changes and functions of the seas, strengthening the physical and digital functions of research infrastructures, and identifying and minimizing barriers to research and mobility in accordance with national laws and regulations [8]. The leaders acknowledged current global challenges and agreed to collectively advance interconnected research infrastructures.

In 2024, the G7 Security and Integrity of Global Research Ecosystem Working Group stated two primary risks as "undue influence, interference, misappropriation of research, and other clandestine activities and behaviors" (p. 4) in research security, and national leaders and policy makers recognize these risks and emerging challenges in collaborative research across nations [9]. The working group also emphasized sharing responsibilities among the key stakeholders such as governments, research funders, research institutions, and individual researchers to assure research security and integrity efforts.

In the field of international relations and diplomacy, policymakers and leaders recommend enhancing research security to better serve national and regional interests. In Europe, the Council of the European Union published its recommendation on enhancing research security in May 2024. This recommendation outlines the recommendations such as promoting responsible internationalization, detailed roles of funding organizations, and specifying support actions for research performing organizations for the member states and the comprehensive leadership and coordination for the European Commission to enhance research security [10].

Challenges and issues related to research security also arise at the national or federal level. The United States has actively discussed and advanced policies and programs to examine research security issues in federal agencies. The guidance for implementing National Security Presidential Memorandum 33 (NSPM-33) has been the foundation of the development of research security in the United States [11]. This document outlines the responsibilities and roles of the federal agencies and organizations to enhance research security while advancing open and collaborative research communication across nations. In addition, the Guidelines for Research Security Programs at Covered Institutions, published in July 2024, outlines federal guidelines to implement research security programs at institutions receiving significant federal research and development funding [12]. The latter states the significance of balancing security and collaborations by ensuring non-discrimination during the research security implementation procedures and outlining four mandatory security elements: cybersecurity, foreign travel security, research security training, and export control training [13].

Based on these guidelines, federal agencies developed and published their own programs, policies, and procedures to implement research security programs. The National Science Foundation (NSF) announced launching a new Research Security Program in July 2023. The NSF intends with this program to understand and enhance research security [14]. The National Institutes of Health

created and published the NIH Decision Matrix for assessing potential foreign interference and the process for allegations related to foreign interference. These are useful resources for researchers and institutions in handling allegations of foreign interference [15]. The Department of Energy has also recognized that there are governments that aggressively seek access to science and technology advancements and intellectual property through threatening research security. The department has introduced policies on foreign engagement with national laboratories, foreign national access programs, the risk matrix, and other related subjects [16].

Policymakers and government leaders must examine many emerging challenges and refine policies to promote integrity and assure security in international research collaborations. In accordance with the latest policies and regulations, all stakeholders must be aware of gaps in national or institutional policies in conducting international collaborative research.

4. Three Concepts (Research Infrastructure, Policies, and Operation and Management)

To assure research integrity and security, I define three significant concepts in this study that support all research stakeholders within and across nations. First, each nation's research infrastructure is the primary platform to establish and advance research communities. Second, research operation and management play important roles in efficient conduct and support of research practices. Third, research policies help all stakeholders to understand basic jurisdiction at the national and organizational levels.

5. Methods

I intend to analyze the relations among the three influencing factors (research infrastructure, research policies, and research operation and management) and the responsibilities of stakeholders in responding to research integrity and security issues in international research collaborations. I examine the three factors and their influences on the stakeholders' responsibilities of research integrity and security in international research collaborations. This research comes from a comparative qualitative policy analysis of previous or ongoing research policies. The research question driving the analysis in this study is the following: In what ways do research infrastructure, research policies, and research operation and management influence responsibilities of research integrity and security in international research collaborations? I examine stakeholders' responsibilities in terms of research integrity and security policies and stakeholders' responses.

6. Findings, Discussion, and Conclusion

Research integrity issues include data management (storing and sharing), legal issues and agreements, research ethics education, research misconduct (fabrication, falsification, and plagiarism), and others. Research security issues include maintenance and advancement of research led by national governments, government agencies, and research communities within and across nations. Policymakers consider artificial intelligence, cybersecurity, export and import controls, generative artificial intelligence, intellectual property, and other related topics that could be potential threats to national security.

Compromises in research integrity and research security increase distrust of public research, weaken political and social support, and threaten academic autonomy. All stakeholders in research must commit to their collective and relevant responsibilities throughout the affiliated research infrastructure, assure research integrity and research security, and maintain research quality founded on trust and accuracy. They also need to identify overlapping responsibilities among units and individuals at the institutional level.

Individual knowledge and efforts on research integrity and research security should be defined neither by a researcher's institution nor by their level of access to research knowledge and support. Policymakers and higher education leaders are responsible for understanding the latest research integrity and research security policies, refining research support infrastructures, and distributing financial and intellectual resources to individuals based on national and institutional guidelines.

References

[1] Directorate-General for Research and Innovation (European Commission), Tackling R&I foreign interference, European Commission, European Union, (2022).

https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1
[2] Organisation for Economic Co-operation and Development, Integrity and security in the global research ecosystem, OECD Publishing, (2022). https://doi.org/10.1787/1c416f43-en
[3] National Academies of Sciences, Engineering, and Medicine, Fostering integrity in research, Washington, DC: The National Academies Press. (2017). https://doi.org/10.17226/21896
[4] The Royal Society, The Royal Society's research integrity statement, The Royal Society, (2017). https://royalsociety.org/-/media/policy/publications/2017/royal-society-research-integrity-statement-09-10-2017.pdf
[5] M. P. Eve, Digital scholarly journals are poorly preserved: A study of 7 million articles, Journal of Librarianship and Scholarly Communication, 12(1), (2024). https://www.iastatedigitalpress.com/jlsc/article/id/16288/
[6] S. Haustein, E. Schares, J. P. Alperin, M. Hare, L. A. Butler and N. Schönfelder, Estimating global article processing charges paid to six publishers for open access between 2019 and 2023, *arXiv preprint arXiv:2407.16551*, (2024). https://doi.org/10.48550/arXiv.2407.16551
[7] K. Langin, Researchers buy citations to inflate metrics. Science, 383(6685), p. 807, (2024). https://www.science.org/doi/epdf/10.1126/science.ado7761
[8] G7 Science and Technology Ministers' Communique, G7 Science and Technology Ministers' Communique, Cabinet Office, Government of Japan, (2023). https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/230513_g7_communique.pdf
[9] G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, G7 Best practices for secure and open research, G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, (2024). https://science.gc.ca/site/science/sites/default/files/documents/1136-g7-best-practices-for-secure-and-open-research-february-2024.pdf
[10] The Council of the European Union, Council recommendation on enhancing research security, The Council of the European Union, (2024). https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf
[11] National Science and Technology Council, Office of Science and Technology Policy, Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on national security strategy for United States government-supported research and development, National Science and Technology Council, Office of Science and Technology Policy, The White House, (2022). https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
[12] Office of Science and Technology Policy, Guidelines for research security programs at covered institutions, Office of Science and Technology Policy, The White House, (2024). https://www.whitehouse.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf
[13] Council on Governmental Relations, Overview of OSTP guidelines for research security programs at covered institutions, Council on Governmental Relations, (2024). https://www.cogr.edu/sites/default/files/Overview%20of%20OSTP%20Guidelines%20for%20Research%20Security%20Programs%20at%20Covered%20Institution%20clean%20copy%20july%2012%202024%20REVISED.pdf
[14] U.S. National Science Foundation, NSF announces research on research security program, U.S. National Science Foundation, (2023). https://new.nsf.gov/news/nsf-announces-research-research-security-program
[15] M. Lauer, New decision matrix further clarifies NIH processes for handling allegations of foreign interference, National Institutes of Health Extramural Nexus, U.S. Department of Health and Human Services, (2024). https://nexus.od.nih.gov/all/2024/08/15/new-decision-matrix-further-clarifies-nih-processes-for-handling-allegations-of-foreign-interference/
[16] Office of Science of U.S. Department of Energy, Relevant DOE orders and policy, Office of Science Laboratory Policy Research Security, U.S. Department of Energy, (2024). https://www.energy.gov/science/office-science-laboratory-policy-research-security