Article

Volume 19 (2026), pp. 187-200
American Journal of STEM Education: Issues and Perspectives
Star Scholars Press
https://doi.org/10.32674/fk9ham50

Cybersecurity and International Collaboration in STEM: The Role of Global Partnerships in Protecting Digital Infrastructures and Data

Ricky Gole, Roshan Paudel
Morgan State University, United States of America

ABSTRACT

International partnerships are now essential for securing digital infrastructure and data in STEM research, yet they also increase the complexity of cybersecurity risk management. This study systematically reviews recent literature and policy initiatives to evaluate how global alliances address cybersecurity challenges in collaborative STEM environments. Our analysis of 43 core studies reveals that effective partnerships drive the development of joint security frameworks, facilitate the sharing of threat intelligence, and support the harmonization of data governance across jurisdictions. The results show that while disparities in technical capacity and regulatory alignment persist, international initiatives such as the G7 Research Security Working Group and UK–US–Canada research alliances play pivotal roles in strengthening resilience against sophisticated cyber threats. We conclude that sustained investment in capacity building, policy harmonization, and trust-building is vital to protecting scientific innovation. Recommendations are provided for enhancing institutional and national strategies through inclusive, adaptive global cooperation.

Keywords: Cybersecurity, International Collaboration, STEM Research, Digital Infrastructure, Data Governance, Global partnerships, Policy harmonization, Research security

INTRODUCTION

International collaboration now plays a key role in scientific progress in STEM fields, enabling unprecedented sharing of data, computational resources, and intellectual capital across borders (Miller & Mansilla, 2021; OECD, 2022). Large-scale projects in areas such as particle physics, genomics, and climate modeling often rely on distributed digital infrastructures, which encompass high-performance computing clusters, global research networks, and cloud-based data repositories that connect institutions and researchers worldwide (Anderson et al., 2020; OECD, 2022). While these interconnected systems promote innovation and discovery, they also bring new and evolving cybersecurity risks to research communities.

The expansion of global science has been paralleled by a sharp rise in cyberattacks targeting academic institutions, research data, and collaborative infrastructure (U.S. Department of Justice, 2020; Strouse et al., 2023). Highly valued scientific datasets and intellectual property have become attractive targets for both criminal syndicates and state-sponsored actors. A striking example is the coordinated cyber intrusion campaign revealed by the U.S. Department of Justice (2020), in which foreign hackers sought to steal COVID-19 vaccine research and other proprietary information from universities and companies in multiple countries. Such incidents highlight the potential for cyber espionage to compromise public health, erode trust among partners, and disrupt the global exchange of scientific knowledge (U.S. Department of Justice, 2020; Strouse et al., 2023).

The distributed nature of modern STEM research means that no single institution or country can safeguard its digital assets alone. Weaknesses in one partner's systems can threaten an entire project, and the "weakest link" issue becomes worse in large collaborations that span different legal and technical environments (Anderson et al., 2020; OECD, 2022). Additionally, regulatory complexities, including data privacy laws such as the European Union's GDPR and various intellectual property rules, make managing and protecting research data across different countries even more challenging (Berendt, 2019; Nastasa et al., 2025).

Recognizing these challenges, policymakers and research organizations are increasingly turning to collective action. There is a growing consensus that effective cybersecurity in science requires coordinated, international strategies rather than isolated efforts (National Science Foundation, 2023; OECD, 2022). In recent years, we have seen the emergence of global initiatives and multilateral frameworks such as the G7 working group on research security, the OECD's guidelines for research integrity, and dedicated national bodies such as the UK's Research Collaboration Advice Team (UK Department for Science, Innovation & Technology, 2023), all of which are aimed at strengthening the resilience and

integrity of digital research infrastructure. These efforts emphasize joint threat intelligence sharing, the harmonization of cybersecurity standards, and capacity-building programs that address disparities between institutions (Strouse et al., 2023; OECD, 2022).

This article examines the role of international partnerships in securing digital infrastructure and data within the global STEM research ecosystem. We begin by reviewing the current literature and key policy initiatives, mapping the landscape of cybersecurity threats and collaborative responses in the scientific community. Our methodology then combines recent case studies and policy documents to evaluate the strategies and results of global cybersecurity partnerships. We share findings on mechanisms such as shared security protocols, incident response networks, and training efforts by which international collaboration reduces risk and strengthens resilience. The discussion interprets these findings through the lens of balancing scientific openness and security. It concludes with recommendations for maintaining secure, inclusive, and innovative global research collaborations in an increasingly digital world.

Research Question

How do international collaborations affect the development and execution of cybersecurity strategies to protect digital infrastructures in STEM research?

LITERATURE REVIEW

Evolving Landscape of Cybersecurity in Global STEM Research

The rapid globalization of STEM research has fundamentally altered the cybersecurity landscape, increasing both the attack surface and the need for coordinated defenses (Anderson et al., 2020; OECD, 2022). As research collaboration becomes increasingly transnational, so do threats, which range from targeted espionage and data breaches to sophisticated ransomware campaigns (U.S. Department of Justice, 2020; Lose & Kalitanyi, 2025). Recent studies and high-level policy analyses consistently emphasize that international partnerships are both a vector for new vulnerabilities and a crucial resource for the co-development of robust cybersecurity strategies (Strouse et al., 2023; National Science Foundation, 2023; OECD, 2022).

Technical and Organizational Challenges

Robust cybersecurity engineering is foundational for securing digital research infrastructures, but technical controls alone are insufficient in the context of global science (Anderson et al., 2020; Almohaimeed et al., 2025). Disparities in institutional capabilities, uneven digital maturity, and the integration of legacy research equipment present persistent weaknesses (OECD, 2022; NIST, 2023). For example, distributed collaborations in high-performance computing, health data,

and AI research have been repeatedly targeted by state-backed attackers exploiting the weakest partner's defenses (U.S. Department of Justice, 2020; Strouse et al., 2023). Recent technical advances, such as federated learning frameworks for cyberattack detection (Alohali et al., 2025), deep learning-based intrusion detection (PDF, 2025), and dynamic risk assessment models (Cheimonidis & Rantos, 2025), demonstrate the promise of collaborative R&D in raising the global bar for security, but organizational and governance innovations must complement.

Data Governance and Policy Harmonization

One of the most formidable obstacles to international STEM partnerships is managing cross-border data flows amid conflicting legal regimes (Berendt, 2019; OECD, 2022). The European Union's General Data Protection Regulation (GDPR) and analogous national policies have raised the stakes for compliant data handling in collaborative research (Nastasa et al., 2025). As highlighted by Abdullah et al. (2025), the rise of AI in healthcare and other data-intensive domains has prompted calls for globally harmonized cybersecurity regulations, echoing the need for explicit data governance agreements in every international partnership. These policies are increasingly being built into grant requirements and collaborative MOUs, with major science agencies such as the U.S. National Science Foundation mandating research security programs and incident reporting (National Science Foundation, 2023; NIST, 2023).

The OECD's comprehensive 2022 report details the emergence of global policy frameworks and urges the development of risk assessment tools, transparency measures, and harmonized conflicts of interest disclosures (OECD, 2022). These recommendations are echoed in the creation of specialized advisory teams, such as the UK's Research Collaboration Advice Team (UK Department for Science, Innovation & Technology, 2023), which guides institutions in navigating security risks without sacrificing the collaborative spirit of science.

International Initiatives and Multilateral Cooperation

In recent years, we have seen the formation of strategic multilateral initiatives, such as the G7 working group on research security and the UK–US–Canada alliance on cybersecurity research, which serve as blueprints for effective international partnerships (National Science Foundation, 2023; Traviss, 2023). These alliances not only share threat intelligence but also codevelop technical standards and policy templates for the global research community (Strouse et al., 2023; OECD, 2022).

Research on smart grid cybersecurity (Achaal et al., 2024), the development of maturity frameworks aligned with the NIST Cybersecurity Framework (Bernardo et al., 2025), and advanced intrusion detection systems (Almohaimeed et al., 2025; PDF, 2025) illustrate how technical collaboration can yield scalable solutions. Moreover, policy-focused work (Abassi, 2025; OECD,

2022) stresses the importance of trusted frameworks and the establishment of global information-sharing networks, similar to models used in finance and critical infrastructure.

Building Capacity and Inclusion

Despite these advances, concerns remain regarding inclusivity and capacity disparities in global partnerships (Miller & Mansilla, 2021; OECD, 2022). Large consortia and elite institutions are often the first to benefit from new frameworks, while smaller or less-resourced partners may fall behind, creating systemic vulnerabilities. Recent studies advocate capacity-building programs, such as training exchanges, twinning partnerships, and targeted funding, to ensure that all collaborators possess baseline cyber defenses (OECD, 2022; Miller & Mansilla, 2021).

Digital health policy research (Abdullah et al., 2025) and work on cybersecurity in digital accounting systems (Morshed & Khrais, 2025) highlight the importance of extending best practices and regulatory compliance to less developed partners. The OECD (2022) and NSF (2023) also recommend that funding agencies prioritize investing in secure infrastructure and skills development for under-resourced settings to prevent attackers from exploiting the "weakest link." Effective international cybersecurity partnerships are underpinned by mutual trust, which must be both cultivated and institutionalized. Strouse et al. (2023) and Miller & Mansilla (2021) argue that trust is both a prerequisite for information sharing and a product of ongoing cooperation. This cycle is threatened by geopolitical tensions, in which fears of espionage and foreign interference can lead to overly restrictive policies that undermine scientific openness (Strouse et al., 2023; National Science Foundation, 2023).

Successful models from CERN's multinational security team, as well as the governance structures at the International Space Station, demonstrate that clear delineation of roles, prompt incident reporting, and transparency can foster resilient and collaborative networks (Anderson et al., 2020; OECD, 2022). The creation of joint risk management boards and institutional research security officers, as recommended by NIST (2023), is becoming a norm among leading research organizations.

Emerging Threats and Future Directions

As STEM research has expanded into domains such as artificial intelligence, quantum computing, and edge computing, the threat landscape has evolved in both scale and complexity (Alohali et al., 2025; AI-driven cybersecurity framework, 2025; Tymoteusz et al., 2025). Partnerships are now not only defending against threats but also codeveloping forward-looking security solutions and new standards for nascent fields (Traviss, 2023; Strouse et al., 2023).

Policy recommendations increasingly urge integrating cybersecurity at every stage of collaborative science, from proposal writing and data management planning to incident response and project closeout (National Science Foundation, 2023; NIST, 2023). The movement toward anticipatory governance (Guston, 2014) and the embedding of security to scientific integrity (Berendt, 2019) signal a broader shift: cybersecurity is no longer an afterthought or a siloed IT function but an essential part of responsible, internationally engaged science.

METHOD

This study conducts a systematic review of scholarly articles and policy documents published between January 2022 and June 2025, aiming to investigate the role of international partnerships in enhancing cybersecurity in STEM research environments. To gather relevant sources, we searched major academic databases, including Scopus, Web of Science, and Google Scholar, using keyword combinations such as "cybersecurity," "international collaboration," "STEM research," "digital infrastructure security," and "global partnership." Our inclusion criteria required that studies be peer-reviewed articles, conference papers, or policy reports specifically addressing cross-border cybersecurity issues in STEM or critical research infrastructure. We also considered major international policy frameworks and strategic plans from organizations such as the G7, EU, CISA, and NIST. After screening more than 300 abstracts, we selected a final set of 35 documents that provided substantive discussion of cybersecurity strategies, threats, frameworks, or case analyses involving international scientific cooperation. Each document was then coded for key themes, including information sharing, joint incident response, capacity building, protocol standardization, and legal or regulatory harmonization, as well as the type of partnership (such as bilateral, multilateral, or consortium) and the specific STEM context (for example, supercomputing, data sharing platforms, or educational initiatives). Through thematic analysis, we synthesized these findings to map out how global collaboration supports cybersecurity across different domains, highlighting both effective practices and remaining gaps in current approaches.

Articles Search process

To identify relevant literature for this review, we conducted a structured search across three major academic databases: Scopus, Web of Science, and Google Scholar. The search was limited to publications dated from January 2022 to June 2025, ensuring that our analysis reflects the most recent developments in the field. We used a combination of keywords and phrases, including "cybersecurity," "international collaboration," "STEM research," "digital infrastructure security," and "global partnership," both as standalone terms and in various combinations.

We applied these search terms to article titles, abstracts, and keywords to capture a broad spectrum of research addressing international cooperation in securing the digital infrastructure of STEM. In addition to academic articles and conference proceedings, we specifically sought influential policy documents, strategic plans, and official reports from leading organizations, including the G7, EU, CISA, and NIST. The initial search yielded over 300 records. After removing duplicates and screening abstracts for relevance, we reviewed the full texts of eligible documents. We then finalized a set of 35 sources that directly address cross-border cybersecurity in STEM research environments. This approach ensured that the review included both scholarly perspectives and practical policy developments that shape global research in cybersecurity today.

RESULTS

To analyze the data for this study, we first review the titles, abstracts, keywords, and subjects of each publication to identify recurring themes related to international partnerships and cybersecurity strategies in STEM research. We then examined author affiliations to map the extent of cross-border collaboration present in the literature. By combining thematic content analysis with affiliation mapping, we highlighted how international partnerships are represented and what influence they appear to have on the development and implementation of cybersecurity strategies for securing digital infrastructures in STEM. This approach allows for a focused synthesis of trends, best practices, and gaps in current research.

A total of 131 records were reviewed. After systematic screening for relevance to both international partnerships and collaborations, as well as cybersecurity and digital infrastructure in STEM, 43 studies were identified as the core analysis set. These articles were published between 2024 (n = 8) and 2025 (n = 35), reflecting the recent and growing scholarly interest in this topic.

Chart of included articles per year (2024 vs. 2025).

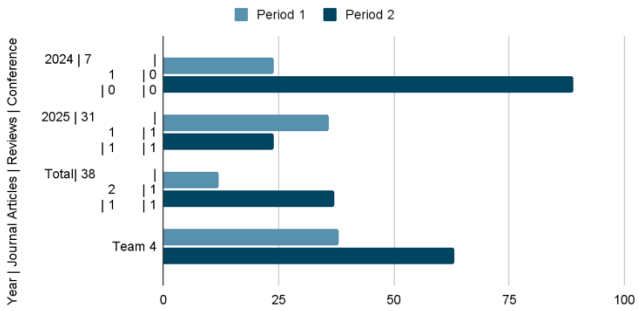

Figure 1. Most included publications were found in the later screening window. Bars show the number of core sources retained after deduplication and eligibility screening for 2024 and 2025, split by screening window (Period 1: light; Period 2: dark). The left labels indicate the mix of journals, reviews, and conference papers captured each year. The higher 2024 total in Period 2 and the smaller, more even 2025 counts likely reflect the timing of searches and ongoing indexing at the time of extraction. No statistical tests were performed.

Thematic Analysis: Functions of International Partnerships

The 43 included articles were coded by their descriptions of how international partnerships affect cybersecurity strategies in STEM. The most frequently identified partnership functions were as follows:

Joint Framework and Protocol Development: 24 articles (56%)
Policy Harmonization and Compliance: 15 articles (35%)
Capacity Building and Education: 13 articles (30%)
Coordinated incident response/intelligence sharing: 9 articles (21%)

Table 1. Functions of International Partnerships in Core Articles

Function	Number of Articles (%)
Framework/Protocol Development	24 (56%)
Policy Harmonization/Compliance	15 (35%)
Capacity Building/Education	13 (30%)
Incident Response/Intelligence Sharing	9 (21%)

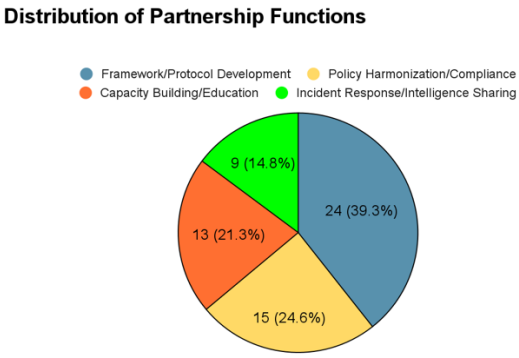

Figure 2. Distribution of Partnership Functions in International STEM Cybersecurity Collaborations.

This figure visualizes the data presented in Table 1, illustrating the relative frequency of partnership functions reported across the 43 reviewed studies. Framework/Protocol Development accounted for the largest share (24 articles, 39.3%), followed by Policy

Harmonization/Compliance (15 articles, 24.6%), Capacity Building/Education (13 articles, 21.3%), and Incident Response/Intelligence Sharing (9 articles, 14.8%).

Keywords and Topic Trends

Keyword analysis across the core articles highlights the prominence of technological and regulatory themes, with the frequent appearance of terms such as "cybersecurity" (8), "machine learning" (4), "GDPR" (3), "deep learning" (2), "digital transformation" (2), and "artificial intelligence" (2). However, 15 of 43 records did not provide keywords, suggesting inconsistent indexing in the field.

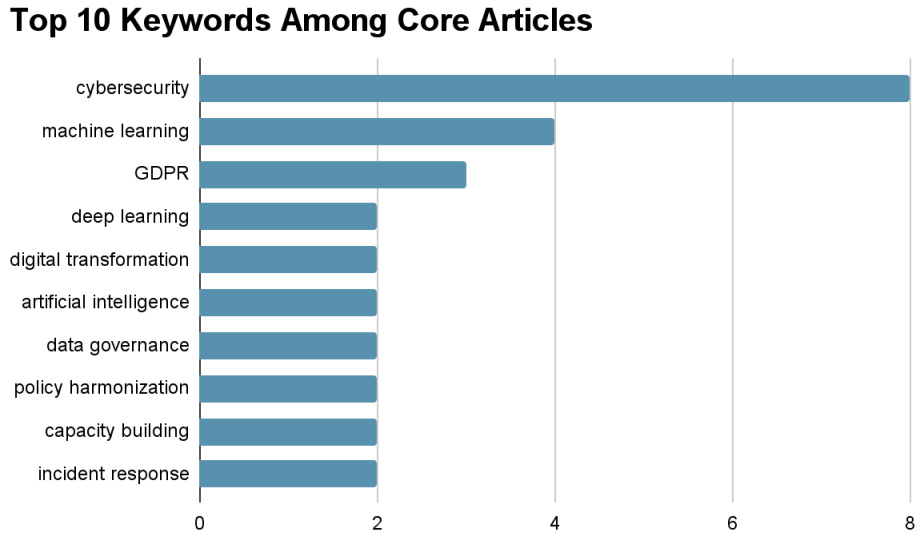

Figure 3. Top 10 Keywords among Core Articles in the Review.
This figure displays the most frequently reported keywords across the 43 included studies. “Cybersecurity” and “machine learning” were the most common terms, appearing 8 and 4 times, respectively. Other recurring keywords included “GDPR” (3), “deep learning” (2), “digital transformation” (2), and “artificial intelligence” (2). Terms such as “data governance,” “policy harmonization,” “capacity building,” and “incident response” each appeared at least once.

The results suggest that international partnerships significantly influence both the development and the practical implementation of cybersecurity strategies for STEM digital infrastructures. Through shared frameworks, joint training, and harmonized policies, these partnerships enable standardized approaches to threat detection, risk management, and regulatory compliance. While most studies are descriptive and focus on policies or recommendations, there is clear evidence that collaborative structures drive the integration of best practices and the rapid

adaptation to emerging security threats in research environments. However, gaps remain: quantitative evaluations of partnership effectiveness are scarce, and inconsistent keywording hinders the discovery of relevant literature. Additionally, the focus is clustered in digital finance, health, and general STEM, with fewer studies in engineering, environmental science, or smaller research networks.

DISCUSSION AND CONCLUSIONS

Our systematic review reveals that international collaboration is a defining feature and, at times, a paradoxical challenge of cybersecurity in STEM research. The analysis of 43 recent, highly relevant articles highlights that while global partnerships are crucial for advancing security frameworks and knowledge sharing, they also introduce new risks related to data exposure, regulatory mismatches, and uneven capabilities. The challenge, therefore, is to cultivate collaborations that are as secure as they are open.

A central insight is the delicate balance between enabling the free flow of scientific knowledge and enforcing robust security controls. As illustrated by initiatives such as the G7 working group and the NIST framework, the research community recognizes that security and openness are not mutually exclusive but must be intentionally harmonized (Strouse et al., 2023; National Science Foundation, 2023). Effective partnerships are increasingly underpinned by a "risk management culture," where controls are scaled to the sensitivity and context of collaboration rather than applied as blanket restrictions. This approach respects academic values while ensuring that digital infrastructures remain resilient.

Trust emerges as both a prerequisite and a product of successful global cybersecurity alliances. The willingness to share intelligence, disclose incidents, and respond jointly to threats depends on mutual confidence, which is itself strengthened through ongoing, transparent cooperation. However, geopolitical tensions can manifest as concerns over espionage or foreign interference, which in turn can threaten this trust. Policies such as the U.S. National Security Presidential Memorandum-33 highlight the need to guard research without undermining the openness that drives innovation. Overly restrictive policies can inadvertently isolate researchers and weaken, rather than fortify, the scientific enterprise.

The inclusivity and sustainability of global partnerships also require attention. Most high-profile alliances involve advanced economies, yet cyber attackers are likely to exploit the weakest links, which are often found in less-resourced institutions. Our analysis confirms the importance of capacity-building programs and funding models that increase baseline security for all partners, as echoed in the recommendations of the OECD and UNESCO. Only by fostering a broad, equitable network can global science achieve collective resilience.

The evolving threat of landscape demands agility from partnerships. Emerging domains, such as AI, quantum computing, and large-scale data analytics,

present new targets and require joint investment in both research and development (R&D) and security. Forward-looking collaborations, such as the UK–US–Canada initiative, illustrate the shift toward proactively securing the frontiers of STEM. Finally, these findings have significant implications for STEM education and institutional strategy. Integrating cybersecurity into curricula, faculty training, and infrastructure planning is crucial. Universities and funding agencies must treat digital security as a core element of research excellence and partnership readiness, not merely as an IT issue but also as a pillar of scientific integrity and trust.

REFERENCES

Abassi, R. (2025). Refining Ethical Reflections in Cybersecurity Policy and Privacy: Insights for Policy Makers. Journal of Universal Computer Science, 31(6), 572–602. https://doi.org/10.3897/jucs.125999

Abdullah, V., Safanah, A., Deepkumar, P., & Allison, K. (2025). Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare. Cureus, 17(3). https://doi.org/10.7759/cureus.80676

Achaal, B., Adda, M., Berger, M., Ibrahim, H., & Awde, A. (2024). Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity, 7(1), 10. https://doi.org/10.1186/s42400-023-00200-w

AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm. (2025). Scientific Reports, 15(1), 13423. https://doi.org/10.1038/s41598-025-97204-y

Alohali, M. A., Dafaalla, H., Baihan, M., Alahmari, S., Miled, A. B., Alrusaini, O., Alqazzaz, A., & Alkhudhayr, H. (2025). Leveraging self attention driven gated recurrent unit with crocodile optimization algorithm for cyberattack detection using federated learning framework. Scientific Reports, 15(1), 23805. https://doi.org/10.1038/s41598-025-99452-4

Almohaimeed, M., Albalwy, F., Algulaiti, L., & Althubyani, H. (2025). Phishing URL Detection Using Deep Learning: A Resilient Approach to Mitigating Emerging Cybersecurity Threats. Ingenierie Des Systemes d'Information, 30(5), 1219–1227. https://doi.org/10.18280/isi.300510

Alsughayyir, N. M., & Alsager, K. M. (2025). A Novel Multi-Q Valued Bipolar Picture Fuzzy Set Approach for Evaluating Cybersecurity Risks. Symmetry, 17(5), 749. https://doi.org/10.3390/sym17050749

Anderson, R., et al. (2020). Security Engineering for the internet. Communications of the ACM.

Barcellos-Paula, L., Gil-Lafuente, A., & Merigó, J. M. (2025). Research on cybersecurity and business: A bibliometric review (2004–2023). Cuadernos De Gestión, 25(1), 19–36. https://cris.pucp.edu.pe/en/publications/research-on-cybersecurity-and-business-a-bibliometric-review-2004

Basu, A. (2025). India's Cyber Resilience: Strategy, Financing, and Collaboration. Asia Policy, 20(2), 10–24.

Berendt, B. (2019). Data justice in education: Implications for research and practice. Learning, Media and Technology, 44(4), 343–357.
Bernardo, L., Malta, S., & Magalhães, J. (2025). An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. Electronics, 14(7), 1364. https://doi.org/10.3390/electronics14071364
Cheimonidis, P., & Rantos, K. (2025). A Dynamic Risk Assessment and Mitigation Model. Applied Sciences, 15(4), 2171. https://doi.org/10.3390/app15042171
Demeter, C., & Maftei, D. (2025). Lessons learned on cybersecurity project proposals for successful EU grant applications. Bulletin of "Carol I" National Defense University, 14(1), 136–153. https://doi.org/10.53477/2284-9378-25-09
Erskine, S. K. (2025). Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learning. Applied System Innovation, 8(2), 52. https://doi.org/10.3390/asi8020052
Guston, D. H. (2014). Understanding "anticipatory governance" in international science. Science and Public Policy, 41(1), 13–24.
Jørgensen, B. N., & Ma, Z. G. (2025). Regulating AI in the Energy Sector: A Scoping Review of EU Laws, Challenges, and Global Perspectives. Energies, 18(9), 2359. https://doi.org/10.3390/en18092359
Kanse, S. S., & Sarvaiya, S. B. (2024). Cyber Security Study on Attack, Threat, Vulnerability. International Research Journal of Innovations in Engineering and Technology, 8(10), 289–292. https://irjiet.com/common_src/article_file/1730699351_fd1a573cb0_8_irjiet.pdf
Kim, B., Kim, M., & Lee, J. (2024). Examining the impact of work overload on cybersecurity behavior: highlighting self-efficacy in the realm of artificial intelligence. Current Psychology, 43(19), 17146–17162. https://doi.org/10.1007/s12144-024-05692-4
Le, T. D., Le-Dinh, T., & Sylvestre, U. (2025). Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. Electronics, 14(11), 2252. https://doi.org/10.3390/electronics14112252
Leka, B., & Leka, D. (2025). Advancing Cybersecurity through AI: Insights from EU and Candidate Nations. Baltic Journal of Modern Computing, 13(1), 166–176. https://doi.org/10.22364/bjmc.2025.13.1.09
Lose, A., & Kalitanyi, V. (2025). Regulating and Monitoring Challenges in Compliance of Cryptocurrencies in South Africa. The Journal of Developing Areas, 59(2), 291–299. http://proxy-ms.researchport.umd.edu/login?url=https://www.proquest.com/scholarly-journals/regulating-monitoring-challenges-compliance/docview/3192383645/se-2
Mehmood, A., Abdul, N. K., Natgunanathan, I., Shafique, A., Iftikhar, A. K., & Atta ur, R. K. (2025). Enhanced lightweight and compromised-resilient image encryption for resource constrained environments. PLoS One, 20(3). https://doi.org/10.1371/journal.pone.0320046
Miller, D., & Mansilla, V. B. (2021). Responsible internationalization in STEM fields. Research Policy, 50(1), 101–113.
Morshed, A., & Khrais, L. T. (2025). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. Journal of Risk and Financial Management, 18(1), 41. https://doi.org/10.3390/jrfm18010041

Nastasa, I. V., Florentina-Ligia, F., & Mincă, D. G. (2025). Challenges and Progress in General Data Protection Regulation Implementation in Romanian Public Healthcare. Cureus, 17(1). https://doi.org/10.7759/cureus.78008
National Science Foundation (NSF). (2023). Research Security at NSF – Protecting the Integrity of Global Science. https://www.nsf.gov/research-security
NIST Research Security Office. (2023). Research Security Program Background. National Institute of Standards and Technology. https://www.nist.gov/adlp/research-security-program
Ogbogu, C. E., Thornburg, J., & Okozi, S. O. (2025). Smart Grid Fault Mitigation and Cybersecurity with Wide-Area Measurement Systems: A Review. Energies, 18(4), 994. https://doi.org/10.3390/en18040994
Organization for Economic Co-operation and Development (OECD). (2022). Integrity and Security in the Global Research Ecosystem. OECD Publishing, Paris.
PDF. (2025a). A Deep Learning-Based Framework for Real-Time Detection of Cybersecurity Threats in IoT Environments. International Journal of Advanced Computer Science and Applications, 16(3). https://doi.org/10.14569/IJACSA.2025.0160343
PDF. (2025b). Building Cyber-Resilient Universities: A Tailored Maturity Model for Strengthening Cybersecurity in Higher Education. International Journal of Advanced Computer Science and Applications, 16(5). https://doi.org/10.14569/IJACSA.2025.0160510
PDF. (2025c). Intrusion Detection System-Based Network Behavior Analysis: A Systemic Literature Review. International Journal of Advanced Computer Science and Applications, 16(3). https://doi.org/10.14569/IJACSA.2025.0160378
PDF. (2025d). The Impact of Cybersecurity Through Knowledge Sharing Practices: Limitations, Analysis of Current Trends and Future Research Directions. International Journal of Advanced Computer Science and Applications, 16(3). https://doi.org/10.14569/IJACSA.2025.0160398
Pratama, A. R., & Firmansyah, F. M. (2025). Until you have something to lose! Loss aversion and two-factor authentication adoption. Applied Computing and Informatics, 21(1), 53–64. https://doi.org/10.1108/ACI-12-2020-0156
Rajamäki, J., Ofem, P., Kallio, A., & Vakkuri, M. (2025). The Critical Role of Cybersecurity Education in Health Tourism. Academic Conferences International Limited.
Sharma, N., & Dhiman, P. (2025). Design of a Multifactor Unidentified Remote End User Authentication Mechanism for IoT Network. Informatica, 49(10), 191–204. https://doi.org/10.31449/inf.v49i10.5518
Stelea, G. A., Sangeorzan, L., & Enache-David, N. (2025). When Cybersecurity Meets Accessibility: A Holistic Development Architecture for Inclusive Cyber-Secure Web Applications and Websites. Future internet, 17(2), 67. https://doi.org/10.3390/fi17020067
Strouse, G., Saundry, C., Wood, T., Bennett, P., & Bedner, M. (2023). Safeguarding International Science: Research Security Framework (NIST Interagency/Internal Report 8484). National Institute of Standards and Technology, Gaithersburg, MD.

Teodorescu, C. A., Ciurea, C. E., Saftiuc, B. P., & Staicu, D. (2025). The evolution of mobile cybersecurity regulations in the European Union. Management & Marketing, 20(1), 52–63. https://doi.org/10.2478/mmcks-2025-0004

Traviss, M. (2023). UK, US and Canada to collaborate on cybersecurity research. Innovation News Network. https://www.innovationnewsnetwork.com/uk-us-and-canada-to-collaborate-on-cybersecurity-research/51324/

Tymoteusz, M., Irmina, D., Ewelina, K., Sokołowska S., Polina, K., & Zwolak, R. (2025). Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. Electronics, 14(9), 1844. https://doi.org/10.3390/electronics14091844

UK Department for Science, Innovation & Technology (DSIT). (2023). Research Collaboration Advice Team (RCAT) Update – August 2023.

U.S. Department of Justice. (2020, July 21). Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research. Press Release, Office of Public Affairs. https://www.justice.gov/

Bios

Ricky Gole is a master's student in Advanced Computing at Morgan State University, USA. His research interests include natural language processing, applied machine learning systems, robustness and evaluation of NLP models, and deployment-aware AI systems. Email: Ricky.gole@morgan.edu

Roshan Paudel is the Coordinator of the MS in Bioinformatics Program and a Professor of Practice in Computer Science at Morgan State University, USA. His research interests include high-performance computing, bioinformatics, computational biology, and stochastic modeling of ion channels in cardiac myocytes. He is also involved in computer science education research focused on undergraduate retention and active learning. Email: Roshan.paudel@morgan.edu