

Cyber Security Experts Association of Nigeria (CSEAN)  
Society for Multidisciplinary & Advanced Research Techniques (SMART)  
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana  
SMART Scientific Projects & Research Consortium (SMART SPaRC)  
Sekinah-Hope Foundation for Female STEM Education  
ICT University Foundations USA

---

---

**Proceedings of the Cyber Secure Nigeria Conference – 2023**

---

---

## **Achieving Sustainable Development Goals from a Cybersecurity Perspective**

**Odumesi, John O. & Sanusi, Bayonle S.**

Department of Computer Science, University of Abuja, Nigeria  
Global Digital Innovation (GDI-GITTP), Korea Advance Institute of Science and Technology  
(KAIST), South Korea

**E-mails:** olayemijohn@yahoo.com; boyorules@gmail.com

### **ABSTRACT**

Rapid digitalisation and society's interconnection have provided both opportunities and problems for sustainable development, as such, this paper aims to understand how cybersecurity measures might help achieve Sustainable Development Goals (SDGs). As more critical infrastructure, key services, and personal data are kept and sent via digital networks, the significance of cybersecurity in accomplishing the SDGs becomes clear. Through a comprehensive literature review, the paper analyses the role of cybersecurity in enhancing economic growth, promoting social inclusivity, and safeguarding environmental sustainability. The paper thoroughly analyses the seventeen (17) SDGs listed by the United Nations (UN) and their underlying goals. The paper looks at how cybersecurity relates to the SDGs, emphasising potential synergies and interdependencies. Finally, this paper emphasises the critical importance of recognising the interdependence between cybersecurity and sustainable development. By mapping cybersecurity with the SDGs, societies can harness the transformative power of digital technologies to build a secure, inclusive, and sustainable future for all.

**Keywords:** SDGs, Cybersecurity, Personal Data, Critical Infrastructure, United Nations, Cyber Threats

---

---

#### **Proceedings Citation Format**

Odumesi, J.O. & Sanusi, B.S. (2023): Achieving Sustainable Development Goals from a Cybersecurity Perspective. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12<sup>th</sup> July, 2023. Pp 1-10  
<https://www.csean.org.ng/>. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P3

---

---

### **1. INTRODUCTION**

The seventeen (17) interconnected global goals that make up the Sustainable Development Goals were accepted by all United Nations Member States in 2015 and are aimed at resolving

some of the world's most pressing issues, including eradicating poverty, promoting health and well-being, providing high-quality education, achieving gender equality, and combating climate change. Although the nature and scope of these objectives vary, they all aim to build a more just, sustainable, and prosperous world for all people. This paper aims to examine the connection between cybersecurity and achieving Sustainable Development Goals. The vulnerability of critical infrastructure, personal data, and national security to cyber threats has expanded tremendously as digital technologies penetrate every part of our lives. The possible effects of cyberattacks, which can range from human rights violations to economic disruptions, highlight how urgent it is to create effective cybersecurity measures to protect sustainable development goals.

## **2. MAPPING CYBERSECURITY TO SUSTAINABLE DEVELOPMENT GOALS (SDGS)**

### **Goal 1: No Poverty (End poverty in all its forms everywhere):**

To achieve this goal (UN SDGs, 2015), governments, organisations, communities, and individuals must work together to address the underlying causes of poverty and implement strategies for its eradication, as well as establish and strengthen social protection systems that can serve as a safety net for the most vulnerable populations.

How cybersecurity contributes to the goal:

Protecting the security and integrity of digital financial services, which can help to reduce poverty by giving people access to financial services (Sultana, 2009), protecting the security and integrity of e-commerce platforms, which can help to increase economic growth (Odumesi & Longe, 2016) and reduce poverty by making it easier for people to buy and sell goods and services online, and protecting the security and integrity of digital educational resources, which can help to improve education (Altamimi et. al., 2022).

### **Goal 2: Zero Hunger (End hunger, achieve food security and improved nutrition and promote sustainable agriculture)**

To achieve this goal (UN SDGs, 2015), everyone should always have access to secure, nourishing, and sufficient food. It entails tackling the underlying factors that contribute to hunger, such as poverty, poor access to resources, and a lack of infrastructure as well as the need for sustainable agricultural practices that minimise environmental degradation, preserve natural resources, and promote rural employment opportunities.

How cybersecurity contributes to the goal:

Agriculture can benefit from using digital technologies to increase productivity, efficiency, and sustainability (Ibrahim & Truby, 2023). By ensuring that these technologies are used properly and securely, cybersecurity measures can help stop them from being used to disrupt or destroy agricultural systems. By safeguarding food security, encouraging the use of digital technology in agriculture, empowering smallholder farmers (Simelton & McCampbell, 2021), and fostering trust and confidence in digital agriculture (Simone et al., 2021).

**Goal 3: Good Health and Well-Being (ensuring healthy lives and promoting well-being for all at all ages)**

To achieve this goal (UN SDGs, 2015), we must guarantee healthy lifestyles and foster well-being for all. The improvement of early disease detection and treatment, support for early childhood development, immunization, and nutrition programs, and achieving universal health coverage by ensuring that everyone has access to necessary healthcare services without financial hardship are some strategies and actions that can help achieve this goal.

**How cybersecurity contributes to the goal:**

Cybersecurity can help to improve the health and well-being of people all over the world by protecting health data from unauthorized access, disclosure, disruption, modification, or destruction (Javaid et al., 2023), ensuring the availability of crucial health infrastructure (Wasserman & Wasserman, 2022), encouraging the use of telemedicine to provide healthcare services remotely (Bitar & Alismail, 2021), and supporting research and development of new healthcare technologies (Driouchi, 2015) that may result in the development of new treatments and cures for diseases.

**Goal 4: Quality Education (ensuring inclusive and equitable quality education and promoting lifelong learning opportunities for all)**

To achieve this goal (UN SDGs, 2015), all children, regardless of background or circumstances, should have access to high-quality pre-primary education and ensure equal access to quality education at all levels. To overcome problems like poor infrastructure, a teacher shortage, gender-based discrimination, and socioeconomic hurdles to education, governments, educational institutions, civil society organisations, and individuals must work together.

**How cybersecurity contributes to the goal:**

Cybersecurity education will be even more crucial as the world becomes more digital to guarantee all students access to high-quality education (Venter et al., 2019). By defending students against online threats towards their academic progress and personal safety (Shersad, & Salam, 2020), maintaining the data and network security of educational institutions (Yaokumah & Ansah, 2019), and encouraging the responsible and safe use of technology (Veckalne & Tambovceva, 2022) without compromising their security.

**Goal 5: Gender Equality (Achieve gender equality and empower all women and girls)**

To achieve this goal (UN SDGs, 2015), we must build a world in which women and girls have equal rights, opportunities, and representation in all aspects of life, resulting in a more inclusive and sustainable society. It acknowledges that gender equality is a fundamental human right and a prerequisite for a peaceful, successful, and sustainable world.

**How cybersecurity contributes to the goal:**

Women and girls are immensely affected by cybercrime because they are more likely to be the targets of online harassment and abuse (Choudhary & Deva, 2023), thus it is crucial to ensure that they have access to safe and secure online environments. Women and girls can use technology as a potent instrument to fight for their rights, get access to education and career opportunities (Kiani et al., 2023), and take part in decision-making processes.

Gender-sensitive cybersecurity rules and procedures are necessary to prevent discrimination against women and girls (Rosser, 2005).

**Goal 6: Clean Water and Sanitation: Ensure availability and sustainable management of water and sanitation for all**

To achieve this goal (UN SDGs, 2015), it is necessary to enhance access to clean water and suitable sanitation facilities, particularly in developing countries, and to address the global water issue. The main goals are to guarantee everyone has access to clean water and adequate sanitation, to ensure sustainable water management practices, to improve water quality, and to increase resilience to water-related problems around the world.

**How cybersecurity contributes to the goal:**

Cybersecurity will be more crucial as the world becomes more dependent on digital technology to ensure the availability and sustainable management of water resources (Limba et al., 2017), safeguard water infrastructure from cyberattacks (Clark et al., 2018), monitor water quality, maximize water use, manage water resources, and ensure the security of water data (Moy de Vitry et al., 2019).

**Goal 7: Affordable and Clean Energy: Ensure access to affordable, reliable, sustainable and modern energy for all**

To achieve this goal (UN SDGs, 2015), we must make sure that everyone has access to affordable, dependable, and sustainable energy sources. This aids in addressing climate change and alleviating poverty, in addition to promoting economic growth and well-being.

**How cybersecurity contributes to the goal:**

As the energy sector becomes more reliant on digital technology, cybersecurity will become increasingly important in maintaining the safe and secure operation of renewable energy systems (Krause et al., 2021) and promoting the use of smart grid technologies (Kim, et al., 2019). It is critical to guarantee that energy infrastructure and systems operate reliably and securely.

**Goal 8: Decent Work and Economic Growth: Promote, inclusive and sustainable economic growth, full and productive employment and decent work for all**

To achieve this goal (UN SDGs, 2015), an environment must be created that promotes inclusive economic growth, effective employment, and opportunities for decent work for all, which will ultimately help alleviate poverty and promote sustainable development.

**How cybersecurity contributes to the goal:**

The demand for cybersecurity expertise will rise as the digital economy expands (Afonasova, 2019), which implies that those who are interested in a career in cybersecurity have numerous opportunities (Sussman, 2020). Although the digital economy is a significant contributor to economic expansion, it is also open to cyberattacks (Venkatachary, 2017).

**Goal 9: Industry, Innovation, and Infrastructure: Build resilient infrastructure, promote inclusive and sustainable industrialization, and foster innovation**

To achieve this goal (UN SDGs, 2015), the collaboration between international organizations, industry, civic society, and governments is necessary. Infrastructure, technology, and innovation investments are needed, along with enabling legislative and regulatory frameworks.

**How cybersecurity contributes to the goal:**

These critical systems can be protected from attack with the aid of cybersecurity, which also ensures that they will continue to operate even in the event of a cyberattack (Mtukushe, 2023), that they will continue to be reliable and available, that they will be safe and secure for innovation to take place (Jang-Jaccard & Nepal, 2014), and that it will help to foster the trust that will support economic growth and development (Mohanty & Mishra, 2023).

**Goal 10: Reduced Inequalities: Reduce inequality within and among countries**

To achieve this goal (UN SDGs, 2015), governments, civil society organizations, the private sector, and international organizations must collaborate. It entails putting in place focused policies, advancing social fairness, ensuring accessibility to necessities, and tackling the underlying causes of inequality.

**How cybersecurity contributes to the goal:**

By fostering a more secure and stable environment for economic growth and development and by levelling the playing field for businesses of all sizes and locations, cybersecurity will become more crucial as the digital economy expands for promoting social inclusion (Teoh & Mahmood, 2017; Ozili, 2018) and reducing inequality.

**Goal 11: Sustainable Cities and Communities: Make cities and human settlements inclusive, safe, resilient and sustainable**

To achieve this goal (UN SDGs, 2015), inclusive, secure, resilient, and sustainable cities and human settlements must be built. This will improve the quality of life for urban dwellers while preserving the environment for future generations.

**How cybersecurity contributes to the goal:**

Smart cities are increasingly connected to the internet (Khatoun & Zeadally, 2017) and rely on a variety of critical infrastructure, including power grids, water systems, and transportation networks, making them vulnerable to cyberattacks (Hammi et al., 2022). Additionally, a lot of essential city services, like healthcare, education, and banking, are now provided online (Saini et al., 2023) while protecting personal data.

**Goal 12: Sustainable Consumption and Production: Ensure sustainable consumption and production patterns**

To achieve this goal (UN SDGs, 2015) is necessary to encourage more responsible and efficient resource usage, limit waste generation, and stimulate long-term economic growth. It acknowledges that present consumption and production practices put a great deal of pressure on the environment, deplete natural resources, and fuel climate change and other environmental problems.

**How cybersecurity contributes to the goal:**

Investments in cybersecurity can contribute to environmental protection, economic development, and bettering the lives of people all around the world (Fedele & Roner, 2021). Critical infrastructure must be safeguarded, data privacy must be maintained, supply chains must be secure, cybercrime must be avoided, innovation must be encouraged, and resilience must be built (Pursiainen, 2017; Roege et al., 2017).

**Goal 13: Climate Action (Take urgent action to combat climate change and its impacts)**

To achieve this goal (UN SDGs, 2015), it is necessary to recognise that everyone has a responsibility to play their part in creating a more resilient and sustainable future for future generations by taking practical steps, adopting sustainable behaviours, and supporting climate-friendly policies.

**How cybersecurity contributes to the goal:**

The development of a more resilient and sustainable society that is better able to respond to the problems posed by climate change by enhancing cybersecurity (Cassotta & Maria, 2019) through the protection of critical infrastructure, securing personal data, and promoting the use of digital technology (Cassotta & Sidortsov, 2019).

**Goal 14: Life Below Water (Conserve and sustainably use the oceans, seas and marine resources for sustainable development)**

To achieve this goal (UN SDGs, 2015), governments, international organizations, the commercial sector, and civil society must work together to address the many complex issues that maritime habitats face. The ocean is vital to maintaining life on Earth, regulating the temperature, and supplying millions of people with a means of subsistence.

**How cybersecurity contributes to the goal:**

By protecting critical infrastructure, preventing illegal fishing, ensuring the safety of marine scientists, and promoting the responsible use of marine resources (Berawi, 2019; Menzel & Otto, 2020).

**Goal 15: Life on Land (Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity)**

To achieve this goal (UN SDGs, 2015), governments, corporations, civil society organisations, and individuals must work together if we are to make any real strides toward a more sustainable and peaceful coexistence with nature. By fostering sustainable development that benefits both the environment and humanity, maintaining biodiversity, preserving terrestrial ecosystems, and tackling climate change.

**How cybersecurity contributes to the goal:**

By safeguarding sensitive information, ensuring the secure operation of technology-driven conservation efforts, supporting wildlife protection, facilitating international collaboration, and improving the overall resilience of initiatives aimed at safeguarding terrestrial ecosystems and biodiversity (Hoffmann, 2022).

**Goal 16: Peace, Justice and Strong Institutions (Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels.**

To achieve this goal (UN SDGs, 2015), everyone must be guaranteed access to justice and develop efficient, responsible, and inclusive institutions at all levels of governance, all pertinent parties must construct societies that are peaceful, inclusive, and sustainable.

**How cybersecurity contributes to the goal:**

Building and maintaining peaceful, just, and powerful institutions in the digital age requires a strong cybersecurity framework (Mishra et al., 2022). Encouraging trust, inclusivity, accountability, and the protection of fundamental rights in the digital sphere, helps societies flourish sustainably (Fife & Pereira, 2016). Cybersecurity measures help in the prevention of cyberattacks and cyberwarfare between states or other actors (Li & Liu, 2021). Cybersecurity promotes a more stable international environment and supports peaceful relations between nations by preventing such attacks (Al-Hawamleh, 2023). Cybersecurity is a crucial component of diplomatic relations on a global scale (Attatfa et al., 2020).

**Goal 17: Partnerships For The Goals: Strengthen the means of implementation and revitalise the global partnership for sustainable development.**

To achieve this goal (UN SDGs, 2015), new partnerships that cut through conventional borders must be formed for a better, more sustainable future for all. It acknowledges that to achieve sustainable development, numerous stakeholders including governments, the private sector, civil society, and international organizations must work together.

**How cybersecurity contributes to the goal:**

A solid cybersecurity foundation is essential for fostering international collaboration, encouraging teamwork (Dalal, 2022), and establishing a secure online environment that supports the achievement of Partnerships for the Goals and, by extension, all other Sustainable Development Goals.

### **3. CONCLUSION**

Cybersecurity is an important issue that affects all aspects of sustainable development. It is critical to ensure the security of technology and online services to achieve the SDGs and create a better, more sustainable future for everybody. Governments, the private sector, civil society, and relevant stakeholders must collaborate to solve cyber security and ensure that technology is used to enhance, rather than undermine, sustainable development. Secure Infrastructure for critical services, protecting environmental data and critical infrastructure connected to biodiversity conservation and natural resource management are some means of how cybersecurity may promote the SDGs. Putting in place strong cybersecurity safeguards, maintaining data integrity, safeguarding emergency response networks, enhancing cybersecurity collaboration between public and private sectors, and improving cybersecurity in the healthcare Sector. By funding cybersecurity research and development, new technologies and solutions that can improve cybersecurity defences are developed. Combating cyber threats to financial inclusion, promoting the ethical use of Artificial Intelligence (AI), increasing citizen awareness of cybersecurity, preserving personal data and privacy, encouraging global

cooperation and information sharing, and developing cybersecurity capacity are just a few of the recommendations that need to be addressed.

## REFERENCES

1. Afonaso, M., Panfilova, E., Galichkina, M. & Ślusarczyk, B. (2019). Digitalization in Economy and Innovation: The Effect on Social and Economic Processes. *Polish Journal of Management Studies*. 19. 22-32. 10.17512/pjms.2019.19.2.02.
2. Al-Hawamleh, A. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*. 14. 2023. 10.14569/IJACSA.2023.0140292.
3. Altamimi, A., Al-Bashayreh, M., Aloudat, M. & Almajali, D. (2022). Blockchain technology adoption for sustainable learning. *International Journal of Data and Network Science*. 6. 983-994. 10.5267/j.ijdns.2022.1.013.
4. Attatfa, A., Renaud, K. & Paoli, S. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science*. 176. 60-69. 10.1016/j.procs.2020.08.007.
5. Berawi, M. (2019). The Role of Industry 4.0 in Achieving Sustainable Development Goals. *International Journal of Technology*. 10. 644. 10.14716/ijtech.v10i4.3341.
6. Bitar, H & Alismail, S. (2021). The role of eHealth, telehealth, and telemedicine for chronic disease patients during COVID-19 pandemic: A rapid systematic review. *DIGITAL HEALTH*. 7. 205520762110093. 10.1177/20552076211009396.
7. Cassotta, S. & Maria, P. (2019). Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example. *Beijing Law Review*. 10. 616-642. 10.4236/blr.2019.103035.
8. Cassotta, S. & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*. 51. 10.1016/j.erss.2019.01.003.
9. Choudhary, L. & Deva, R. (2023). Cyber Sexual Victimization of Female College Students and its Impacts: A study in Rajasthan. *Journal of Advance Research in Science and Social Science*. 6. 82-95. 10.46523/jarssc.06.01.08.
10. Clark, R., Hakim, S. & Panguluri, S. (2018). Protecting water and wastewater utilities from cyber-physical threats. *Water and Environment Journal*. 10.1111/wej.12340.
11. Dalal, R., Howard, D., Bennett, R., Posey, C., Zaccaro, S. & Brummel, B. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*. 37. 1-29. 10.1007/s10869-021-09732-9.
12. Driouchi, A. (2015). *New Health Technologies and Health Workforce in Developing Economies*. Paper. MPRA Paper No. 67993.
13. Fedele, A. & Roner, C. (2021). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*. 36. 10.1111/joes.12456.
14. Fife, E. & Pereira, F. (2016). The promise and reality: Assessing the gap between theory and practice in ICT4D. *Telecommunications Policy*. 40. 10.1016/j.telpol.2016.05.004.
15. Hammi, B., Zeadally, S., Khatoun, R. & Jamel, N. (2022). Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. *Computers & Security*. 117. 102677. 10.1016/j.cose.2022.102677.

16. Hoffmann, S. (2022). Challenges and opportunities of area-based conservation in reaching biodiversity and sustainability goals. *Biodiversity and Conservation*. 31. 10.1007/s10531-021-02340-2.
17. Ibrahim, I & Truby, J (2023). FarmTech: Regulating the use of digital technologies in the agricultural sector. *Food and Energy Security*. 10.1002/fes3.483.
18. Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 80. 10.1016/j.jcss.2014.02.005.
19. Javid, M., Haleem, A., Singh, R. & Suman, R. (2023). Towards insighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*. 1. 100016. 10.1016/j.csa.2023.100016.
20. Khatoun, R. & Zeadally, S. (2017). Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine*. 55. 51-59. 10.1109/MCOM.2017.1600297CM.
21. Kiani, M., Tavakoli, R. & Mura, P. (2023). Iranian Women Traveling in vTime—A Cyberfeminist Approach. *Journal of Travel Research*. 004728752211492. 10.1177/00472875221149202.
22. Kim, S., Lee, T., Kim, S., Park, L. & Park, S. (2019). Security Issues on Smart Grid and Blockchain-based Secure Smart Energy Management System. *MATEC Web of Conferences*. 260. 01001. 10.1051/mateconf/201926001001.
23. Krause, T., Ernst, R., Klaer, B., Hacker, I. & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. <https://doi.org/10.3390/s21186225>
24. Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 7. 10.1016/j.egy.2021.08.126.
25. Limba, T., Plêta, T., Agafonov, K. & Damkus, M. (2017). Cyber security management model for critical infrastructure. *ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES*. 4. 559-573. 10.9770/jesi.2017.4.4(12).
26. Menzel, A. & Otto, L. (2020). Connecting the Dots: Implications of the Intertwined Global Challenges to Maritime Security. 10.1007/978-3-030-34630-0\_14.
27. Mishra, A., Alzoubi, Y., Anwar, M. J. & Gill, A. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*. 120. 102820. 10.1016/j.cose.2022.102820.
28. Mohanty, B. & Mishra, S. (2023). Role of Artificial Intelligence in Financial Fraud Detection. *Academy of Marketing Studies Journal*. 27. 1528-2678.
29. Moy de Vitry, M., Schneider, M., Wani, O., Manny, L., Leitão, J. & Eggimann, S. (2019). Smart urban water systems: what could possibly go wrong?. *Environmental Research Letters*. 14. 081001. 10.1088/1748-9326/ab3761.
30. Mtukushe, N., Onaolapo, A., Aluko, A. & Dorrell, D. (2023). Review of Cyberattack Implementation, Detection, and Mitigation Methods in Cyber-Physical Systems. *Energies*. 16. 5206. 10.3390/en16135206.
31. Odumesi, J. & Longe, O. (2016). Users' Perspective on Electronic Payment Channel Services in Nigeria. *Digital Innovations and Contemporary Research in Science & Engineering Journal*. 4. 93-100. 10.22624/AIMS/D/V4N4P9.
32. Ozili, P. (2018). Impact of Digital Finance on Financial Inclusion and Stability. 18. 329-340. 10.1016/j.bir.2017.12.003.
33. Pursiainen, C. (2017). Critical infrastructure resilience: A Nordic model in the making?. *International Journal of Disaster Risk Reduction*. 27. 10.1016/j.ijdr.2017.08.006.

34. Roege, P., Collier, Z., Chevardin, V., Chouinard, P., Florin, M., Lambert, J., Nielsen, K., Nogal, M. & Todorovic, B. (2017). Bridging the Gap from Cyber Security to Resilience. 10.1007/978-94-024-1123-2\_14.
35. Rosser, S. (2005). Through the Lenses of Feminist Theory: Focus on Women and Information Technology. *Frontiers: A Journal of Women Studies*. 26. 1-23. 10.1353/fro.2005.0015.
36. Saini, S., Chauhan, A., Thakur, G. & Sapra, L. (2023). Challenges and Opportunities in Secure Smart Cities for Enhancing the Security and Privacy. 10.1007/978-3-031-22922-0\_1.
37. Shersad, F. & Salam, S. (2020). Managing Risks of E-learning During COVID-19. 10.13140/RG.2.2.12722.63689.
38. Simelton, E & McCampbell, M (2021). Do Digital Climate Services for Farmers Encourage Resilient Farming Practices? Pinpointing Gaps through the Responsible Research and Innovation Framework. *Agriculture*. 11. 953. 10.3390/agriculture11100953.
39. Simone, V.D.B., Wiseman, L. G., & Krkeljas, J (2021). Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing. *Ethics and Information Technology*. 23. 10.1007/s10676-020-09543-1.
40. Sultana, R. (2009). Mobile Banking: Overview of Regulatory Framework in Emerging Markets. *SSRN Electronic Journal*. 10.2139/ssrn.1554160.
41. Sussman, L. (2020). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that May Expand the Expectations of the Cyber Workforce. 1. 19-39.
42. Teoh, C. & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*. 95. 6510-6522.
43. United Nations Sustainable Development Goals (2015). Retrieved from <https://sustainabledevelopment.un.org/topics/sustainabledevelopmentgoals#>
44. Veckalne, R. & Tambovceva, T. (2022). The Role of Digital Transformation in Education in Promoting Sustainable Development. *Virtual Economics*. 5. 65-86. 10.34021/ve.2022.05.04 (4).
45. Venkatachary, S., Prasad, J. & Ravi, S. (2017). Economic Impacts of Cyber Security in Energy Sector: A Review. *International Journal of Energy Economics and Policy*. 7. 250-262.
46. Venter, I., Blignaut, R., Renaud, K. & Venter, M. (2019). Cyber security education is as essential as “the three R’s”. *Heliyon*. 5. e02855. 10.1016/j.heliyon.2019.e02855.
47. Wasserman, L. & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*. 4. 862221. 10.3389/fdgth.2022.862221.
48. Yaokumah, W. & Ansah, A. (2019). Network and Data Transfer Security Management in Higher Educational Institutions. 10.4018/978-1-5225-8455-1.ch001.