

Letter to the Editor

Cite this article: Kuday AD (2024). Sustainable Development in the Digital World: The Importance of Cybersecurity. *Disaster Medicine and Public Health Preparedness*, **18**, e279, 1–2 <https://doi.org/10.1017/dmp.2024.306>

Received: 26 July 2024
Accepted: 08 October 2024

Corresponding author:
Ahmet Doğan Kuday;
Email: dogankuday@gmail.com

Dear Editor,

Digitalization has become an integral part of our lives, playing a critical role in achieving the Sustainable Development Goals (SDGs).¹ The integration of digital technologies across various sectors has brought about unprecedented efficiency and connectivity, yet it has also exposed significant vulnerabilities. The successful realization of SDGs relies on a trustworthy data and secure digital infrastructure. Cyberattacks can target critical infrastructures, adversely affecting economic and social development. Data are the backbone of modern economies, and securing them in critical areas such as health, education, and energy is vital at both individual and societal levels.² Critical infrastructures, including power plants, water treatment facilities, and transportation systems, are essential for societal functioning. Protecting these infrastructures from cyberattacks is fundamental for sustainable development. For instance, a cyberattack on the energy infrastructure could lead to widespread power outages, triggering economic, and social crises.³ Therefore, data security and cybersecurity are foundational pillars of the digital world and should be incorporated into the SDGs. Recently, high-profile cyber incidents, such as the MOVEit attack, which compromised millions of records globally, and ransomware attacks on organizations like MGM Resorts and T-Mobile, illustrate the potential for extensive socio-economic disruptions and underscore the critical need for robust cybersecurity measures.

While the SDGs do not explicitly address data security or cyberattacks, certain goals and targets are indirectly related. For example, *Goal 9 - Industry, Innovation, and Infrastructure* includes the target of significantly increasing access to information and communication technologies and striving to provide universal and affordable internet access in least developed countries. This target implies the need for data security and cybersecurity as ICT development and dissemination are promoted. The proliferation of information technologies also underscores the importance of security and protection against cyberattacks. Another example is *Goal 16 - Peace, Justice, and Strong Institutions*, which aims to ensure public access to information and protect fundamental freedoms in accordance with national legislation and international agreements. This goal focuses on access to information and freedom of expression, implicitly requiring secure and reliable data storage and transmission, as well as protection against cyber threats.

Incorporating data security and cybersecurity into the SDGs should guide policy-makers at national and international levels. International cooperation and information sharing on these



Figure 1. Cybersecurity for SDGs.

issues are essential for a safer digital world. In conclusion, data security and cybersecurity play a critical role in achieving sustainable development goals (Figure 1). Therefore, these issues should be prioritized within the SDG framework. Developing and implementing data security and cybersecurity policies are necessary for building a secure and sustainable future in the digital world.

Sources of Support. None.

Competing interest. The author(s) declare none.

References

1. **UNDP.** Digital technologies directly benefit 70 percent of SDG targets, say ITU, UNDP and partners. Accessed 26 July 2024. <https://www.undp.org/press-releases/digital-technologies-directly-benefit-70-percent-sdg-targets-say-itu-undp-and-partners>.
2. **Mondejar ME, Avtar R, Diaz HLB,** et al. Digitalization to achieve sustainable development goals: steps towards a smart green planet. *Sci Total Environ.* 2021;**794**:148539. doi:10.1016/j.scitotenv.2021.148539
3. **Darıçılı AB, Çelik S.** National security 2.0: the cyber security of critical infrastructure. *Perceptions.* 2022;**26**(2):259–276.