Chapter 5
Enhancing Security Intelligence Through Biometrics:
Strengthening Global Institutions

Manmeet Kaur Kaur Arora
https://orcid.org/0009-0002-5071-117X
Sharda University, India

Hind Hammouch
https://orcid.org/0000-0002-5897-1649
University Sidi Mohamed Ben Abdellah, Fez, Morocco

Bhupinder Singh
https://orcid.org/0009-0006-4779-2553
Sharda University, India

Sahil Lal
https://orcid.org/0000-0001-9827-3717
Sharda University, India

ABSTRACT

The focus is biometric technologies and security intelligence systems. It points out that biometric technology could enhance security measures and also enumerates some of the challenges attached thereto. Biometrics measures and statistically analyses the unique physical or behavioural properties of individuals, provides a robust alternative to traditional authentication methods. The future in this area includes multimodal biometrics, continuous authentication technology, and artificial intelligence integration with blockchain technology. These innovations promise to

DOI: 10.4018/979-8-3693-9405-2.ch005

increase accuracy and user convenience while simultaneously addressing some vulnerabilities, like spoofing and algorithmic bias. However, a range of issues accompany the adoption of biometric technologies. Due to technical constraints, public perception, and legal complications, large numbers of people have yet been unable to use these in everyday life. The chapter points out how to establish public confidence through openness, good business practices, and legislative compliance.

INTRODUCTION

The changing contours of security in a globalized world Digital technologies have transformed the traditional paradigms of security; consequently, a more comprehensive approach to protecting assets, information and people has been required. In this regard, security intelligence has become an important component, which helps organizations recognize and mitigate risks proactively (Horng et al., 2023). It also gives suggestions for legislators to create a well-run environment conducive to responsible implementation of biometrics. The chapter relates these technologies to Sustainable Development Goal 16 (SDG16), which seeks to build peaceful and inclusive societies that afford access to justice and strong institutions (Zhang & Wang, 2025). By increasing public safety, promoting inclusiveness within governance processes and helping those who lack it today obtain identity using highly accurate methods, biometrics has a real contribution role here. Overall, the need for an approach which balances innovation with the protection of individual rights and societal values is an important theme running through this chapter (Raghav et al., 2024). As biometric technologies become increasingly sophisticated and widespread, their integration into the security intelligence system of organizations in a digital world is bound to affect future ways security is managed. Such response is the growing focus in security intelligence as a key component, in helping organizations take pre-emptive steps against risks (Kaushik et al., 2024). In this chapter it engage with the intersection between security intelligence and Sustainable Development Goal (SDG) 16, which focuses on peace, justice and strong institutions. It also emphasizes the significance of biometrics in contemporary security systems, underlining the ways in which such aspects together foster a more secure collective.

Security intelligence encompasses the systematic gathering, analysis, and use of threat and vulnerability information throughout different sectors (Singh et al., 2024). It combines information from various sources both internal and external to create actionable intelligence that improves an organisation's response to possible threats (Abdullah & Elfadil, 2020). It engages in real-time data monitoring as well as historical analysis to spot trends and predict risks before they arise. Security Intelligence Is About Minimizing Risk and Expedient Decision Making Security