Chapter 10
Securing the Digital Frontier: Cybersecurity, AI, and Autonomous Systems in Customs and Border Management

Fajar Amjad
Government Graduate College, Lahore, Pakistan

Muhammad Haseeb Shakil
http://orcid.org/0000-0002-3192-0497
The University of Lahore, Pakistan & COMSATS University Islamabad, Lahore Campus, Pakistan

Naveed Anwer
http://orcid.org/0000-0002-6774-3752
The University of Lahore, Pakistan

Sarfraz Zaman
http://orcid.org/0000-0002-2609-1727
The University of Lahore, Pakistan

Rana Nadir Idrees
http://orcid.org/0000-0001-5651-4279
COMSATS University Islamabad, Lahore, Pakistan

ABSTRACT

The global shift to digitized customs platforms, including Single Windows and autonomous trade systems, introduces unprecedented cybersecurity vulnerabilities

DOI: 10.4018/979-8-3373-8362-0.ch010

across the global supply chain. This chapter examines the critical challenges posed by an expanding attack surface, data integrity attacks, ransomware, and AI-specific threats, such as adversarial manipulation of predictive risk models. It argues that security can no longer be an afterthought; rather, it must be integrated as a foundational principle. A robust response requires a multilayered security framework, the implementation of data integrity solutions like blockchain for non-repudiation, and a strict governance model for AI that ensures accountability, transparency, and fairness (ATF). Ultimately, a collective defense built on strong public-private partnerships and aligned international cooperation is essential to safeguard highly sensitive trade data, maintain operational resilience, and secure the future of global digital commerce.

1. INTRODUCTION

The global customs and border management environment is experiencing a significant modernization, transitioning from manual, paper-based procedures to a digital, data-centric ecosystem (Sarker, 2023). This shift, typified by the implementation of Single Window platforms, paperless trade systems, and electronic manifest solutions, has yielded notable improvements in operational efficiency, transparency, and speed within international trade (Epps, 2024). The streamlining of administrative processes and the facilitation of real-time data exchange directly align customs operations with policy objectives supporting sustainable, efficient, and transparent trade in accordance with this book's thematic goals.

Nonetheless, this essential digitalization comes with a significant security problem. The contemporary custom practices are no longer manualized operations. Rather, they have become a tangled, hypernet grid of national databases, cloud solutions, and logistics systems. These connect government agencies to the supply chain of the company immediately (Baah et al., 2024). This interdependence makes it more efficient, yet opens a huge, vulnerable target to cyber syndicates (Mallick & Nath, 2024). Any single point of failure, e.g., a manifest breach or a ransomware attack in a port, or manipulated digital certificates, will have a global impact. This threatens the economic stability and the national security (Vidović et al., 2025).

The chapter is designed based on the intersection of digitalization and the development of AI and autonomous systems with the cybersecurity imperative. The digital edge of customs is no longer concerned with modifying ancient processes. It has now become adopting new technologies that alter the risk assessment and decision-making processes (Makhanya, 2024). We consider the potent application of Artificial Intelligence (AI) and Machine Learning (ML). These are technologies that facilitate predictive risk management and document auditing by Natural Lan-