Chapter 4
Synthetic Risk Environments for Next-Generation Cybersecurity

Otmane Azeroual
http://orcid.org/0000-0002-5225-389X
University of Hagen, Germany

ABSTRACT

The complexity and velocity of modern cyber threats expose the limits of static, compliance-driven risk assessments. Synthetic Risk Environments (SREs) offer dynamic, digitally constructed ecosystems that simulate adversarial behavior, system vulnerabilities, and socio-technical interdependencies. Integrating AI-driven scenario generation, digital twins, cyber ranges, and generative modeling, SREs enable organizations to anticipate multi-vector attacks, evaluate cascading failures, and test resilience in realistic conditions. This chapter reviews the theoretical foundations, methodologies, and strategic applications of SREs, discusses emerging trends and challenges, and positions SREs as essential tools for proactive, adaptive, and resilience-oriented cybersecurity.

1. INTRODUCTION

Over the past decade, cybersecurity has evolved from a primarily technical concern into a systemic challenge affecting organizations, governments, and critical infrastructures alike. The increasing digitization of industrial processes, public services, supply chains, and societal communication has created deeply interconnected socio-technical systems whose exposure to cyber threats is both persistent and expanding (Schwab, 2015; ENISA, 2023). At the same time, adversaries have become more

DOI: 10.4018/979-8-3693-8397-1.ch004

Copyright © 2027, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

adaptive, coordinated, and capable of exploiting not only technical vulnerabilities but also organizational dependencies, human behavior, and cross-sector interconnections (Tounsi & Rais, 2018; Bada & Nurse, 2019). As a consequence, cyber risk can no longer be understood as a set of isolated incidents affecting individual assets; rather, it must be approached as a dynamic and systemic phenomenon shaped by continuous interaction between attackers, defenders, and infrastructures.

Traditional cybersecurity risk assessment methods have made important contributions to governance, compliance, and control. Frameworks such as NIST SP 800-30 and ISO/IEC 27005 provide structured procedures for identifying, analyzing, and treating cyber risks, while threat intelligence reports by institutions such as ENISA offer up-to-date insights into evolving attack patterns (NIST, 2018/2023; ENISA, 2023). However, these approaches remain limited in important respects. Most conventional models rely heavily on historical evidence, static threat assumptions, or checklist-based assessments, and are therefore insufficient for capturing the adaptive, uncertain, and interconnected character of contemporary cyber threats (Tounsi & Rais, 2018; Bada & Nurse, 2019). Empirical evidence from recent cyber incidents, such as large-scale supply chain compromises and ransomware attacks, demonstrates that the most severe impacts often arise from cascading effects and systemic disruption rather than isolated vulnerabilities (Cebula & Young, 2010; Klasa et al., 2021).

Against this background, this chapter argues that Synthetic Risk Environments (SREs) represent a promising next-generation approach for cybersecurity risk analysis and resilience assessment. SREs can be understood as digitally constructed and dynamically configurable environments that simulate adversarial behavior, system vulnerabilities, and socio-technical interdependencies under controlled yet realistic conditions (Salvi, Spagnoletti & Noori, 2022; Ani et al., 2025). They build upon advances in cyber ranges, digital twins, and simulation modeling, and increasingly incorporate artificial intelligence techniques such as generative modeling and reinforcement learning to emulate adaptive attackers and defenders (Ligo, Kott & Linkov, 2021; Goodfellow et al., 2014).

The central premise of this chapter is that the value of SREs lies not merely in their technological sophistication, but in their ability to bridge a long-standing gap between governance-oriented cyber risk management and experimentally grounded cyber resilience testing. Existing research has highlighted the limitations of classical risk frameworks in dealing with uncertainty, interdependence, and adversarial adaptation (Cebula & Young, 2010; Naghshbandi et al., 2020). At the same time, advances in resilience engineering and complex systems theory emphasize the need to understand cyber systems as adaptive and interdependent environments rather than static infrastructures (Hollnagel, Woods & Leveson, 2006; Holland, 1995).

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/synthetic-risk-environments-for-next-generation-cybersecurity/413288

Related Content

Towards the Semantic Representation of Biological Images: From Pixels to Regions

Kenneth McLeod, D. N. F. Awang Iskandarand Albert Burger (2013). *International Journal of Intelligent Information Technologies (pp. 35-54).*

www.irma-international.org/article/towards-the-semantic-representation-of-biological-images/103878

Meta-Heuristic Structure for Multiobjective Optimization Case Study: Green Sand Mould System

T. Ganesan, I. Elamvazuthi, K. Z. KuShaariand P. Vasant (2014). *Smart Manufacturing Innovation and Transformation: Interconnection and Intelligence (pp. 38-58).*

www.irma-international.org/chapter/meta-heuristic-structure-for-multiobjective-optimization-case-study/102101

IMF Fiscal Surveillance during the Eurozone Crisis

Lena Golubovskaja (2016). *International Journal of Signs and Semiotic Systems (pp. 1-19).*

www.irma-international.org/article/imf-fiscal-surveillance-during-the-eurozone-crisis/153597

Algorithmic Bias and Farmers' Autonomy in AI-Driven Agricultural Marketing and Supply Chains

Farai Alice Gwelo (2025). *AI and Machine Learning Applications in Supply Chains and Marketing (pp. 313-344).*

www.irma-international.org/chapter/algorithmic-bias-and-farmers-autonomy-in-ai-driven-agricultural-marketing-and-supply-chains/359834

A Model of Complexity Levels of Meaning Constitution in Simulation Models of Language Evolution

Andy Lückingand Alexander Mehler (2011). *International Journal of Signs and Semiotic Systems (pp. 18-38).*

www.irma-international.org/article/model-complexity-levels-meaning-constitution/52601