Challenge Scenario 2: Combating Malicious Downloads to Protect User Safety and Digital Integrity

Innovatia, a rapidly industrialising nation, has positioned itself as a global hub for technology innovation. Innovatia's "Digital Leap 2030" initiative has rapidly expanded internet access, bringing millions of first-time users online. While this digital revolution has created opportunities for e-commerce, digital payments, and social connectivity, it has also made users vulnerable to malicious actors. Malicious apps that mimic legitimate services have emerged as a significant threat, siphoning sensitive data and undermining trust in the digital ecosystem.

In 2023, Innovatia's Cyber Crime Coordination Centre reported that Innovatia lost $3.6B USD fraud. In 2024, Innovatia reported nearly 800 digital payment fraud cases daily, 10 times more than the financial regulator's annual report. The rapid growth of internet usage also brought with it an increased risk of cybercrime, particularly financial fraud. Its Cyber Crime Coordination Centre reported that over 740,000 cybercrime complaints were lodged on the National Cybercrime Reporting Portal between January and April alone this year. In May 2024, the portal received an average of 7,000 complaints daily, with 85% related to online financial fraud.

In early 2025, Innovatia witnessed a surge in cybercrimes stemming from malicious app downloads from unverified sources. A gaming app called "TreasureQuest" promised users cash prizes but secretly collected sensitive information, including banking credentials and personal data. Similarly, "LoanEasy," an app offering instant loans with zero interest, gained traction among rural users, only to misuse their data for blackmail and fraud. Another app, "BankMate," impersonating a popular banking platform, appeared legitimate and offered features like transaction history and mobile payments. Once downloaded from the web, the app covertly harvested sensitive credentials and accessed users' contacts and photos.

These incidents led to financial losses exceeding $3 billion, with countless users falling victim to identity theft and unauthorized transactions. Public outrage erupted, and confidence in digital platforms plummeted, threatening the growth of Innovatia's nascent but promising startup ecosystem.

Stakeholder Positions:

- Government: Tasked with safeguarding citizens and ensuring trust in digital platforms.
- Large Tech Companies: Started work internally and collaborating with the government to identify impactful solutions that mitigate this.
- Consumers: Particularly first-time technology users, demanding safer digital environments and improved awareness.
- Civil Society Groups: Advocating for transparency and user education to reduce vulnerabilities.

Problem Statement

The National Cybersecurity Task Force has been convened to address the growing risks posed by malicious app downloads. You are tasked with developing policy recommendations that:

1. Propose a policy framework to reduce the risk of harmful app downloads from unverified sources that do not have robust capabilities and established policies to keep users safe (i.e. website downloads), while also leveraging emerging technologies and the reach of large tech platforms.
2. Recommend strategies for public-private partnerships to enhance user safety within the same framework.
3. Suggest mechanisms for cross-border collaboration to counter foreign threat actors and bolster cybersecurity defenses.