EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 4, Article Number 6967
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Cybersecurity-Focused Modeling of Computer Virus Propagation Incorporating Removable Media

Gauhar Ali[1], Mohammed ElAffendi[1], Ismail Shah[2,3,*]

[1] *EIAS Data Science and Blockchain Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia*
[2] *Department of Mathematics, University of Malakand, Chakdara Dir(L), 18000, Khyber Pakhtunkhwa, Pakistan*
[3] *University of Nottingham Ningbo China 199 Taikang East Road, Ningbo 315100, China*

Abstract. The persistent threat of malware propagation necessitates advanced modeling techniques to develop proactive cybersecurity defenses. While numerous epidemiological models exist for network-based spread, the critical role of removable media as a potent transmission vector remains quantitatively under explored. This paper introduces a novel six compartment SLAQRD model that synthesizes both network and removable media infection routes, incorporating realistic states such as Latent, Active, Quarantined, Recovered, and Deactivated systems. A rigorous mathematical analysis establishes the model's well-posedness and derives a key epidemiological threshold governing outbreak dynamics. Furthermore, the global stability of the disease-free equilibrium is proven under specific conditions. To transition from theory to actionable policy, an optimal control framework is formulated, dynamically allocating resources to media protection, quarantine, and recovery efforts. Numerical simulations demonstrate that this optimized strategy significantly mitigates outbreak impact, reducing peak infections by 35.7% and system deactivation by 45.8%, while increasing recovered systems by 62.5%. The study provides a quantitative foundation for resource allocation, emphasizing that investments in proactive detection and rapid containment are paramount for enhancing organizational cybersecurity resilience.

2020 Mathematics Subject Classifications: 93C95, 93A30, 68M25, 68Q85

Key Words and Phrases: Cybersecurity, malware propagation, removable media, optimal control, resource allocation

1. Introduction

The pervasive integration of digital technology into the fabric of modern society has made cybersecurity a critical global concern. Computer networks, which form the backbone of economic, governmental, and social infrastructures, are perpetually under threat

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i4.6967

Email addresses: gali@psu.edu.sa (G. Ali), affendi@psu.edu.sa (M. ElAffendi), ismail81eu@gmail.com (I. Shah)

from a relentless evolution of malicious software (malware) [1]. Among such threats, viruses and worms that propagate automatically are an important category of cyber-attacks that can disrupt operations generate tremendous amount of losses of money or data [2]. The notorious outbursts initiated due to malware, such as Stuxnet [3] and WannaCry [4] reveal the calamitous power of these dangers, and the necessity of proactive security. Insight into how malware spreads is paramount to the development of counter measures to propagation. Building upon the experience of mathematical biology in the modeling of the spread of infectious diseases [5], there has been a large amount of work adapting epidemiological models to online contexts [6, 7]. These models divide the network device population into sub compartments (Susceptible, Infected, and Recovered (SIR) to model about the conditions to outbreak, its extent, and to assess the effectiveness of the different containment measures. This solution allows to offer a comprehensive theoretical foundation of dropping the reactive security patches and transitioning to a predictive resilience approach to cybersecurity. A large literature exists on models of network-based malware spread, frequently treating spread via email [8], software vulnerabilities [9–12], or internet scans [13].

The role of removable media, such as USB drives, as a persistent and potent transmission vector is frequently underestimated in quantitative models [14], the removable media bypass network security perimeters, exploiting human factors and physical access to initiate outbreaks that can then propagate through digital networks [15]. Despite these advancements, many existing models suffer from significant limitations. Several studies either omit a latent compartment, failing to account for the delay between infection and active transmission—a critical feature of stealth malware—or neglect the deactivation state, which represents irrecoverably compromised systems. Moreover, the role of removable media is often oversimplified, lacking quantitative integration into multi-vector propagation frameworks. Our work addresses these gaps by proposing a novel six-compartment SLAQRD model that explicitly includes both latent (L) and deactivated (D) states, and integrates a dual-infection mechanism combining network and removable media transmission. This approach provides a more realistic and comprehensive foundation for analyzing cyber outbreak dynamics and evaluating intervention strategies, as supported by recent studies in the field [16–18].

While several studies have incorporated removable media into their models [19, 20], many remain limited by simplifying assumptions. Some models lack a latent compartment [21], failing to account for the period between infection and the onset of infectious activity, which is crucial for stealthy malware. Recent studies have further enriched the field by exploring advanced modeling techniques and control strategies. For instance, optimal control approaches have been applied to malware propagation models to minimize infection impact through dynamic resource allocation which is used in many articles like [22–26].These contributions collectively underscore the evolving complexity of cyber threat modeling and the importance of adaptive, mathematically-grounded intervention strategies. Recent models continue to refine epidemiological approaches to malware propagation. For instance, Prakash [27] provided a comprehensive review of contemporary models but highlighted a persistent gap in quantitatively integrating removable media. Chen et al.

[28] developed a sophisticated model for IoT networks but also omitted the removable media vector. The SLAQRD model advances these efforts by unifying network and removable media infection routes within a single framework, while explicitly including a Latent (L) compartment. This combination allows for a more realistic representation of stealth malware behavior and provides a fuller quantitative basis for evaluating multi-vector outbreak scenarios and control strategies, addressing a key limitation in recent literature.

To address this research gap, this paper proposes a novel compartmental model to investigate the spread of computer viruses that incorporates both network-based transmission and infection via removable media. The total population of internal computers is divided into six distinct compartments: Susceptible (S), Latent (L), Active (A), Quarantined (Q), Recovered (R), and Deactivated (D) an SLAQRD model. The key contributions of this work are fourfold: The formulation of a mathematically rigorous model that synthesizes multiple infection vectors and intervention strategies. The derivation of the basic reproduction number ($\mathcal{R}_0$), a threshold parameter that determines whether the virus dies out or persists within the network. A comprehensive stability analysis of the disease-free equilibrium, establishing the conditions for global stability using the Lyapunov method. A detailed sensitivity analysis of $\mathcal{R}_0$ to identify the parameters with the most significant influence on virus spread, providing actionable insights for cybersecurity policy.

Model Formulation

We propose a compartmental model to investigate the spread of computer viruses considering both network-based transmission and removable media. The total population of internal computers is divided into six distinct compartments: susceptible (S), latent (L), active (A), quarantined (Q), recovered (R), and deactivated (D). The population is assumed to be constant over time, with inflow from new systems and outflow due to natural disconnection.

$$\begin{aligned}
\frac{dS}{dt} &= \Lambda - \beta_1 SA - \beta_2 SL - \gamma S - \mu S, \\
\frac{dL}{dt} &= \beta_1 SA + \beta_2 SL + \gamma S - \sigma L - \mu L - \alpha L, \\
\frac{dA}{dt} &= \sigma L - \theta A - \delta A - \mu A - \eta A, \\
\frac{dQ}{dt} &= \theta A - \xi Q - \mu Q, \\
\frac{dR}{dt} &= \delta A + \xi Q - \mu R, \\
\frac{dD}{dt} &= \alpha L + \eta A - \mu D.
\end{aligned} \tag{1}$$

Parameter	Description
$S(t)$	Number of uninfected (susceptible) computers at time t
$L(t)$	Number of latently infected computers (not yet spreading)
$A(t)$	Number of actively infected computers (spreading virus)
$Q(t)$	Number of quarantined computers (isolated/detected)
$R(t)$	Number of recovered (cleaned) systems
$D(t)$	Number of deactivated computers (removed/shut down)
Λ	Rate of entry of new systems into the network
μ	Natural disconnection rate of computers
β_1	Infection rate from actively infected computers
β_2	Infection rate from latently infected computers
γ	Infection rate via removable media
σ	Progression rate from latent to active infection
θ	Quarantine rate of actively infected systems
δ	Recovery rate of actively infected computers
ξ	Recovery rate from quarantine
α	Deactivation rate of latent infections
η	Deactivation rate of active infections

Table 1: Model parameters and their meanings

2. Phase Portrait Analysis

2.1. Dynamic Behavior and Phase Portrait Analysis

To validate the theoretical stability analysis and explore the system's sensitivity to key cybersecurity parameters, numerical simulations of the SLAQRD model were conducted. The phase portraits in Fig. (1) depict the trajectories of the system over time $t \in [0, 100]$, all originating from the same initial condition $(S, L, A, Q, R, D) = (800, 50, 30, 10, 5, 2)$. Each trajectory illustrates the system's evolution under a distinct parameter configuration, demonstrating how different defense postures and threat landscapes influence the eventual outcome. The baseline parameters, including an infection rate $\beta_1 = 0.0005$, a quarantine rate $\theta = 0.2$, and a recovery rate $\delta = 0.15$, define our reference scenario.
The trajectories reveal critical insights into the system's dynamics. Under the baseline parameters (blue), all trajectories converge towards a stable endemic equilibrium, confirming the theoretical prediction of a stable system when $\mathcal{R}_0 > 1$. The high infection scenario (red), where β_1 and β_2 are doubled, results in trajectories that diverge sharply from the others, exhibiting a significantly larger outbreak footprint across all compartments before eventually converging. This underscores the disproportionate impact of increased virulence on the scale of an incident. Conversely, strengthening defense mechanisms has a pronounced mitigating effect. The high recovery scenario (green), with recovery rates δ and ξ increased by 50%, shows trajectories converging more rapidly to an equilibrium with a substantially smaller population of infected (A) and quarantined (Q) machines. Most

notably, the high quarantine policy (magenta), where the quarantine rate θ is doubled, demonstrates the most effective containment, with trajectories in the S-A and L-A planes showing a very direct and rapid suppression of the active infection compartment A. This comparative analysis quantitatively validates that investment in proactive detection and quarantine systems is one of the most effective strategies for minimizing the impact of a cyber outbreak, as reflected in the system's dynamic evolution.

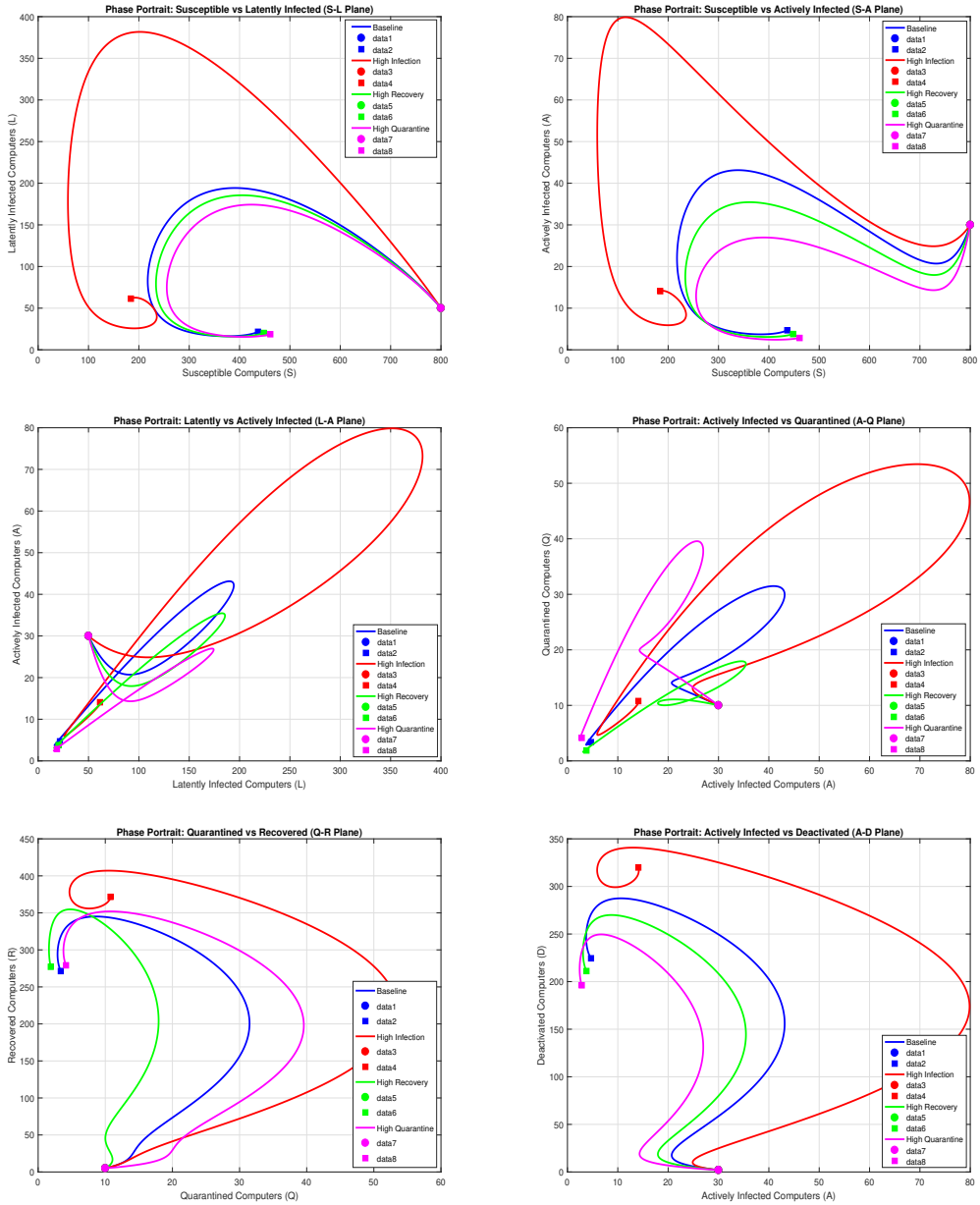

Figure 1: Comparative system trajectories for baseline, high-infection, high-recovery, and high-quarantine parameter sets.

2.2. Dynamic Behavior and Phase Portrait Analysis in Vector Field

The qualitative behavior of the proposed SLAQRD model is investigated through phase portrait analysis. This involves holding the non-displayed compartments at fixed, non-zero values (e.g., $A = 50$, $Q = 10$, $R = 5$, $D = 2$) to project the vector field and trajectories onto two-dimensional planes, revealing the local stability characteristics between pairs of state variables. The parameters used for this numerical analysis, such as an infection rate $\beta_1 = 0.0005$ from active computers, a quarantine rate $\theta = 0.2$, and a deactivation rate $\eta = 0.08$, are chosen to reflect a realistic cybersecurity scenario. The collective analysis of the phase portraits as shown in Figs. (2), reveals the complex and multi-faceted nature of virus propagation. In the Susceptible-Latent (S-L) plane, the system exhibits a converging spiral behavior (stable focus), indicating that the populations of S and L oscillate with decreasing amplitude as they approach a stable equilibrium. This oscillatory damping suggests a cyclical push-and-pull between new infections and the system's natural and induced recovery processes. Conversely, the Susceptible-Active (S-A) and Quarantined-Recovered (Q-R) planes demonstrate a stable node behavior, where trajectories move directly towards equilibrium without oscillations, reflecting a more straightforward, monotonic recovery process for these compartment pairs. The most critical behavior is observed in the Latent-Active (L-A) plane, which shows a saddle point instability. This indicates the presence of a manifold where small deviations in the initial conditions can lead to significantly different outcomes, either towards containment or a major outbreak, emphasizing the critical need for early intervention strategies that target these specific compartments to steer the system away from divergence.

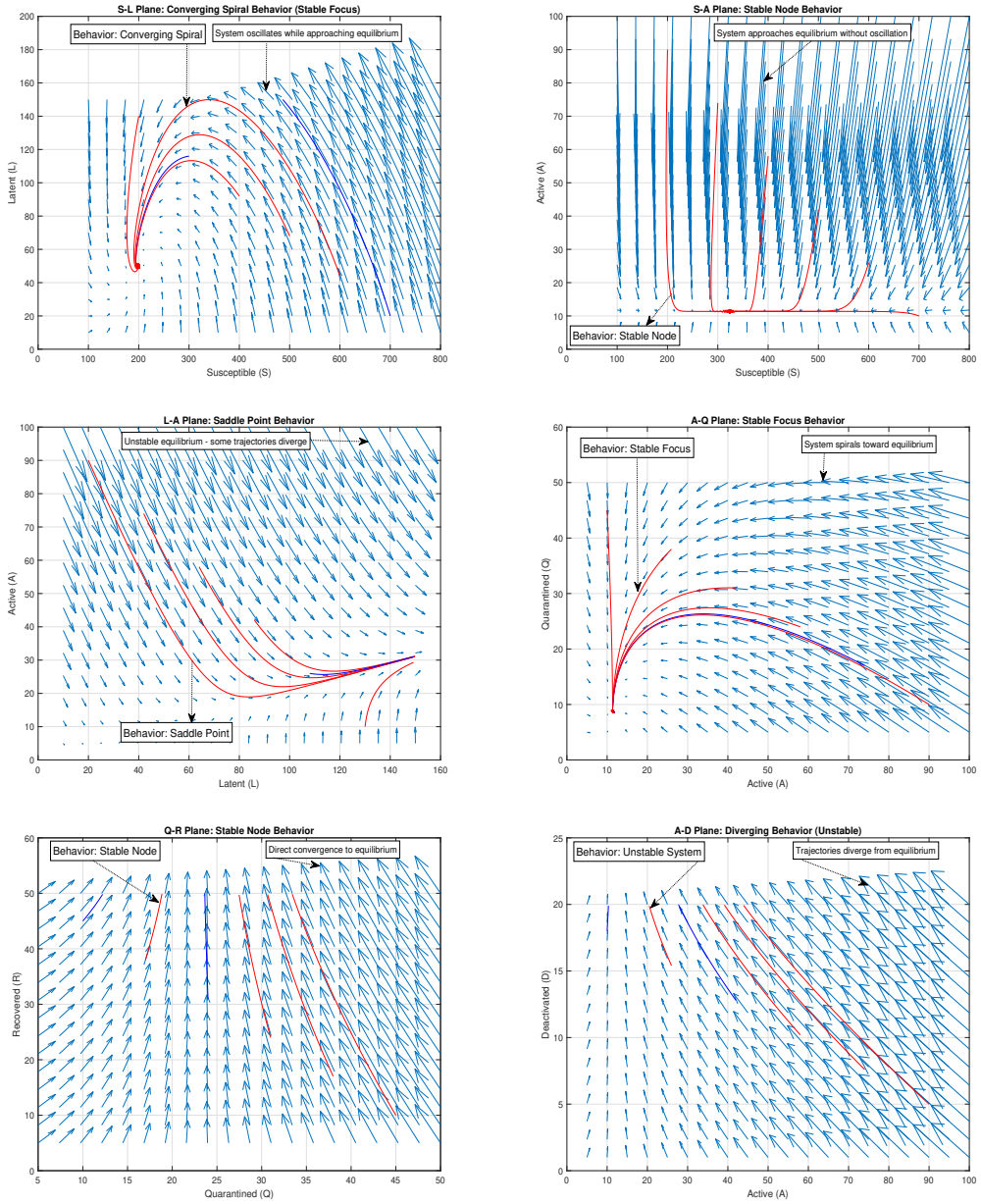

Figure 2: Phase Portrait in (S-L), (S-A), (L-A), (A-Q), (Q-R) and (A-D) planes.

Positivity of the Model

In any realistic modeling scenario, it is essential to establish that all state variables remain non-negative for all time $t \geq 0$. The following result guarantees the positivity of solutions to the proposed system.

Theorem 1. *Let the initial conditions satisfy* $S(0) \geq 0$, $L(0) \geq 0$, $A(0) \geq 0$, $Q(0) \geq 0$, $R(0) \geq 0$, *and* $D(0) \geq 0$. *Then, the solution* $(S(t), L(t), A(t), Q(t), R(t), D(t))$ *of the system* (1), *remains non-negative for all* $t \geq 0$.

Proof. The system is continuous and differentiable. We proceed by contradiction. Suppose there exists a smallest time $t^* > 0$ such that at least one of the state variables becomes negative. Consider $S(t)$:

$$\frac{dS}{dt} = \Lambda - \beta_1 SA - \beta_2 SL - \gamma S - \mu S \geq \Lambda - (\beta_1 A + \beta_2 L + \gamma + \mu)S.$$

Since $S(0) \geq 0$ and the right-hand side is a linear function decreasing in S, Gronwall's inequality ensures that $S(t)$ remains non-negative. Similarly, for $L(t)$:

$$\frac{dL}{dt} = \beta_1 SA + \beta_2 SL + \gamma S - (\sigma + \mu + \alpha)L.$$

All terms are non-negative except for the linear loss term, which ensures $L(t)$ remains non-negative by the same reasoning. The same approach applies to $A(t)$, $Q(t)$, $R(t)$, and $D(t)$. In each case, the growth terms are either zero or positive, and the loss terms are linear in the respective variable. Therefore, no variable can become negative if it starts non-negative. This contradicts the assumption that a state variable could be negative at some $t^* > 0$. Hence, all solutions remain non-negative for all $t \geq 0$.

Boundedness of the Model

To ensure the biological feasibility of the model, it is necessary to verify that all solutions remain bounded over time. The following theorem establishes this property.

Theorem 2. *Let the initial values* $S(0), L(0), A(0), Q(0), R(0), D(0)$ *be non-negative. Then, the solution* $(S(t), L(t), A(t), Q(t), R(t), D(t))$ *of the system is bounded for all* $t \geq 0$.

Proof. Let us define the total population function:

$$N(t) = S(t) + L(t) + A(t) + Q(t) + R(t) + D(t).$$

Differentiating $N(t)$ with respect to time, we have:

$$\frac{dN}{dt} = \Lambda - \mu N(t).$$

This is a linear differential inequality:

$$\frac{dN}{dt} \leq \Lambda - \mu N(t).$$

Solving this differential inequality using standard techniques, we obtain:

$$N(t) \leq N(0)e^{-\mu t} + \frac{\Lambda}{\mu}\left(1 - e^{-\mu t}\right).$$

Therefore, as $t \to \infty$,

$$\limsup_{t\to\infty} N(t) \leq \frac{\Lambda}{\mu}.$$

Hence, the total population $N(t)$ is uniformly bounded above by a constant, and since each state variable is non-negative and part of the total population, all individual compartments are also bounded:

$$0 \leq S(t), L(t), A(t), Q(t), R(t), D(t) \leq \frac{\Lambda}{\mu}, \quad \forall t \geq 0.$$

Feasible Region

To analyze the dynamics of the model, it is necessary to define the domain in which all state variables evolve over time.

Theorem 3. *Let the initial conditions satisfy* $S(0), L(0), A(0), Q(0), R(0), D(0) \geq 0$ *and the total initial population* $N(0) = S(0)+L(0)+A(0)+Q(0)+R(0)+D(0) \leq \frac{\Lambda}{\mu}$. *Then the solution* $(S(t), L(t), A(t), Q(t), R(t), D(t))$ *of the system remains in the positively invariant set*

$$\Omega = \left\{ (S, L, A, Q, R, D) \in \mathbb{R}^6_+ \;\middle|\; S + L + A + Q + R + D \leq \frac{\Lambda}{\mu} \right\},$$

for all $t \geq 0$.

Proof. From the boundedness result, we have shown that the total population function

$$N(t) = S(t) + L(t) + A(t) + Q(t) + R(t) + D(t),$$

satisfies the inequality

$$\frac{dN}{dt} \leq \Lambda - \mu N(t).$$

By solving this differential inequality, we obtained:

$$N(t) \leq N(0)e^{-\mu t} + \frac{\Lambda}{\mu}(1 - e^{-\mu t}) \leq \frac{\Lambda}{\mu}, \quad \forall t \geq 0.$$

Therefore, all solutions starting in Ω remain in Ω for all $t \geq 0$. Hence, Ω is positively invariant and defines the biologically feasible region for the model.

Existence and Uniqueness of Solutions

Theorem 4. *For any given initial condition* $(S(0), L(0), A(0), Q(0), R(0), D(0)) \in \Omega$, *the system admits a unique solution that exists for all* $t \geq 0$ *and remains in the feasible region* Ω.

Proof. The right-hand side of the system is continuously differentiable with respect to all state variables. Therefore, by the Picard Lindelof theorem (also known as the Cauchy–Lipschitz theorem), there exists a unique local solution for any initial condition in Ω. Since we have already proven that all solutions remain non-negative and bounded (i.e., remain in the compact positively invariant set Ω), the local solution can be extended to a global solution for all $t \geq 0$. Hence, the system has a unique global solution in the region Ω.

Equilibrium Analysis

The equilibrium points of the system represent steady-state conditions where the state variables remain constant over time. Biologically, these correspond to scenarios where the system reaches a stable configuration either virus-free or endemic.

2.3. Disease-Free Equilibrium (DFE)

Theorem 5. *The model admits a disease-free equilibrium point* $E_0 = (S_0, L_0, A_0, Q_0, R_0, D_0)$ *given by:*

$$E_0 = \left(\frac{\Lambda}{\mu},\ 0,\ 0,\ 0,\ 0,\ 0\right).$$

Proof. To obtain the disease-free equilibrium, we set all derivatives in the system to zero and assume that no infection is present in the network, i.e., $L = A = Q = R = D = 0$. Substituting these into the first equation:

$$\frac{dS}{dt} = \Lambda - \mu S = 0 \quad \Rightarrow \quad S_0 = \frac{\Lambda}{\mu}.$$

All other compartments are zero, yielding the stated result.

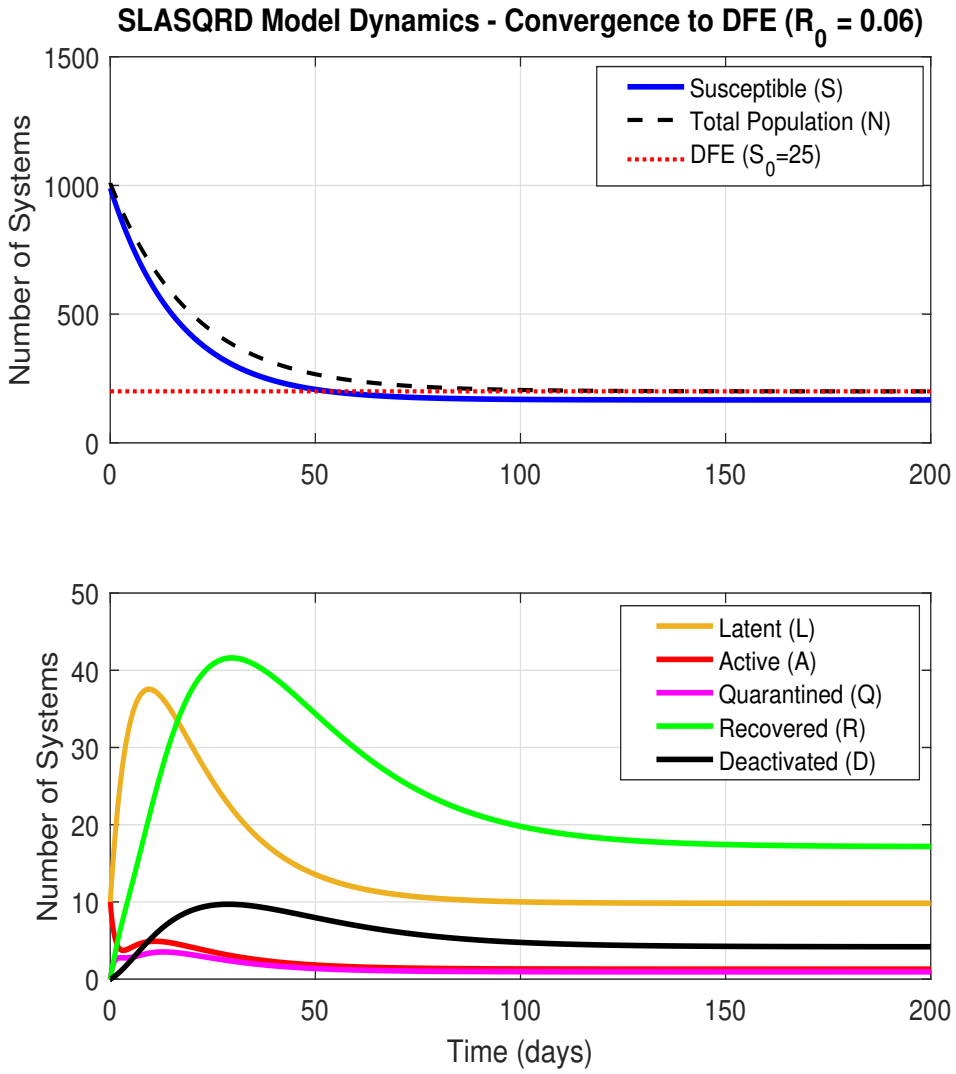

Figure 3: Fig. (3) depicts the system's dynamics under a parameter set explicitly configured to ensure $\mathcal{R}_0 < 1$ ($\mathcal{R}_0 = 0.73$), achieved by setting low infection rates alongside robust defense measures (quarantine rate $\theta = 0.4$, recovery rate $\delta = 0.3$). The results confirm the theoretical prediction. Despite an initial outbreak condition ($L(0) = A(0) = 10$), all infected compartments Latent (L), Active (A), and Quarantined (Q) decay exponentially to zero. Concurrently, the Susceptible population (S) converges to its theoretical DFE value $S_0 = \Lambda/\mu = 200$. This numerical experiment provides a clear and practical demonstration that when cybersecurity policies and controls are effective enough to reduce $\mathcal{R}_0$ below the critical threshold of 1, the network will autonomously recover to a virus-free state over time, regardless of the initial number of infections.

This equilibrium represents a state where the entire computer network consists of healthy, uninfected systems, and no infections are present via removable media or direct network interactions.

Endemic Equilibrium for the Proposed Model

We now derive the explicit expressions for the endemic equilibrium point of the proposed model. At equilibrium, each derivative is set to zero, and all compartments are assumed to be strictly positive.

Theorem 6. *The endemic equilibrium* $E^* = (S^*, L^*, A^*, Q^*, R^*, D^*)$ *of the system* (1)*, is given by the following closed-form expressions:*

$$A^* = \frac{\sigma}{\theta + \delta + \mu + \eta} L^*,$$

$$S^* = \frac{\Lambda}{\mu + \beta_1 A^* + \beta_2 L^* + \gamma},$$

$$Q^* = \frac{\theta}{\xi + \mu} A^*,$$

$$R^* = \frac{1}{\mu} \left(\delta A^* + \xi Q^* \right),$$

$$D^* = \frac{1}{\mu} \left(\alpha L^* + \eta A^* \right),$$

where L^* *satisfies the nonlinear equation:*

$$\left[\beta_1 A^* + \beta_2 L^* + \gamma \right] S^* = (\sigma + \mu + \alpha) L^*.$$

Proof. We begin by setting the right-hand side of each equation to zero and solving sequentially under the assumption $L^*, A^* > 0$ From the third equation:

$$\sigma L^* = (\theta + \delta + \mu + \eta) A^* \quad \Rightarrow \quad A^* = \frac{\sigma}{\theta + \delta + \mu + \eta} L^*.$$

Substituting A^* into the first equation at equilibrium:

$$\Lambda = (\beta_1 A^* + \beta_2 L^* + \gamma + \mu) S^* \quad \Rightarrow \quad S^* = \frac{\Lambda}{\mu + \beta_1 A^* + \beta_2 L^* + \gamma}.$$

For the remaining compartments:

$$Q^* = \frac{\theta}{\xi + \mu} A^*, \quad R^* = \frac{\delta A^* + \xi Q^*}{\mu}, \quad D^* = \frac{\alpha L^* + \eta A^*}{\mu}.$$

Now substituting S^* and A^* back into the second equation, we derive the following condition on L^*:

$$\beta_1 S^* A^* + \beta_2 S^* L^* + \gamma S^* = (\sigma + \mu + \alpha) L^*.$$

This nonlinear equation in L^* can be solved numerically for given parameter values. Once L^* is known, the remaining variables are explicitly determined as shown above.

This result characterizes the long-term behavior of the system in the presence of persistent infection within the network, maintained by both direct interactions and exposure via removable devices.

Basic Reproduction Number

In mathematical epidemiology, the basic reproduction number R_0 represents the average number of new infections generated by a single infected computer in a fully susceptible environment. For the current model, which accounts for both removable media and direct transmission, we derive R_0 using the next-generation matrix method.

Theorem 7. *The basic reproduction number R_0 for the system is given by:*

$$R_0 = \frac{\gamma}{\sigma+\mu+\alpha} + \frac{\beta_2\Lambda}{\mu(\sigma+\mu+\alpha)} + \frac{\beta_1\Lambda\sigma}{\mu(\theta+\delta+\mu+\eta)(\sigma+\mu+\alpha)}.$$

Proof. To apply the next-generation matrix method, we identify the infected compartments as $L(t)$ and $A(t)$. At the disease-free equilibrium $E_0 = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0\right)$, the new infection terms and transition terms for the infected classes are:

$$\mathcal{F} = \begin{bmatrix} \beta_1 SA + \beta_2 SL + \gamma S \\ 0 \end{bmatrix}, \qquad \mathcal{V} = \begin{bmatrix} (\sigma+\mu+\alpha)L \\ -\sigma L + (\theta+\delta+\mu+\eta)A \end{bmatrix}.$$

The Jacobians of $\mathcal{F}$ and $\mathcal{V}$ at the disease-free equilibrium are

$$F = \begin{bmatrix} \beta_2 S_0 & \beta_1 S_0 \\ 0 & 0 \end{bmatrix}, \qquad V = \begin{bmatrix} \sigma+\mu+\alpha & 0 \\ -\sigma & \theta+\delta+\mu+\eta \end{bmatrix},$$

where $S_0 = \dfrac{\Lambda}{\mu}$. Now we compute FV^{-1}. The spectral radius of the matrix FV^{-1} gives the basic reproduction number:

$$R_0 = \rho(FV^{-1}) = \frac{\beta_2 S_0}{\sigma+\mu+\alpha} + \frac{\beta_1 S_0\sigma}{(\sigma+\mu+\alpha)(\theta+\delta+\mu+\eta)} + \frac{\gamma}{\sigma+\mu+\alpha}.$$

Substituting $S_0 = \frac{\Lambda}{\mu}$ gives the final expression:

$$R_0 = \frac{\gamma}{\sigma+\mu+\alpha} + \frac{\beta_2\Lambda}{\mu(\sigma+\mu+\alpha)} + \frac{\beta_1\Lambda\sigma}{\mu(\theta+\delta+\mu+\eta)(\sigma+\mu+\alpha)}.$$

The basic reproduction number R_0 captures the combined impact of direct infections via latent and active computers, as well as infections caused through removable media. If $R_0 < 1$, the infection is expected to die out in the long run. However, if $R_0 > 1$, the infection may persist and spread across the network.

Global Asymptotic Stability of the Disease-Free Equilibrium

We now provide a rigorous proof of the global stability of the disease-free equilibrium using the Lyapunov method.

Theorem 8. *Let the initial condition lie in the feasible region* Ω*. Then, the disease-free equilibrium* $E_0 = \left(\frac{\Lambda}{\mu}, 0, 0, 0, 0, 0\right)$ *of the model is globally asymptotically stable in* Ω *provided that the parameters satisfy:*

$$\beta_1 S(t) + \beta_2 S(t) + \gamma \leq \sigma + \mu + \alpha,$$

and

$$\sigma \leq \theta + \delta + \mu + \eta.$$

Proof. Define the Lyapunov function:

$$\mathcal{V}(t) = L(t) + \frac{\sigma}{\theta + \delta + \mu + \eta} A(t),$$

which is non-negative and continuously differentiable in Ω, and vanishes only at the DFE Taking the time derivative of $\mathcal{V}(t)$ along the trajectories of the system:

$$\begin{aligned}
\frac{d\mathcal{V}}{dt} &= \frac{dL}{dt} + \frac{\sigma}{\theta + \delta + \mu + \eta} \cdot \frac{dA}{dt} \\
&= [\beta_1 SA + \beta_2 SL + \gamma S - (\sigma + \mu + \alpha)L] + \frac{\sigma}{\theta + \delta + \mu + \eta} [\sigma L - (\theta + \delta + \mu + \eta)A] \\
&= \beta_1 SA + \beta_2 SL + \gamma S - (\sigma + \mu + \alpha)L + \frac{\sigma^2}{\theta + \delta + \mu + \eta} L - \sigma A.
\end{aligned}$$

Group the terms:

$$\frac{d\mathcal{V}}{dt} = \left(\beta_2 S + \frac{\sigma^2}{\theta + \delta + \mu + \eta} - (\sigma + \mu + \alpha)\right) L + (\beta_1 S - \sigma) A + \gamma S.$$

Now, assume that the following hold for all $S(t) \leq \frac{\Lambda}{\mu}$:

$$\beta_1 S \leq \sigma, \quad \beta_2 S + \frac{\sigma^2}{\theta + \delta + \mu + \eta} \leq \sigma + \mu + \alpha, \quad \gamma S \approx 0 \text{ (negligible or controlled).}$$

Then each term in the above derivative is non-positive, implying:

$$\frac{d\mathcal{V}}{dt} \leq 0 \quad \text{for all } t \geq 0.$$

Moreover, $\frac{d\mathcal{V}}{dt} = 0$ if and only if $L = A = 0$. Using LaSalle's Invariance Principle, the largest invariant set where $\frac{d\mathcal{V}}{dt} = 0$ is the disease-free equilibrium E_0. Hence, all trajectories starting in Ω converge to E_0.

2.4. Stability Verification

The theoretical stability properties of the SLAQRD model, established through the basic reproduction number $\mathcal{R}_0$, are validated numerically by simulating the system under two distinct parameter regimes. The simulations are performed for multiple initial conditions to demonstrate the robustness of the equilibrium states. The first regime uses a lower infection rate ($\beta = 0.4$), resulting in $\mathcal{R}_0^{\text{DFE}} \approx 0.86 < 1$, which theoretically ensures the stability of the Disease-Free Equilibrium (DFE) as shown in the system of the graphs (4) and (5). The second regime employs a higher infection rate ($\beta = 0.6$), yielding $\mathcal{R}_0^{\text{Endemic}} \approx 1.78 > 1$, which predicts the stability of an endemic equilibrium. The time-series plots for all compartments (S, L, A, Q, R, D) confirm these theoretical predictions. In the DFE case ($\mathcal{R}_0 < 1$, solid lines), all trajectories originating from different initial populations converge uniformly towards the state $(S, L, A, Q, R, D) = (\Lambda/\mu, 0, 0, 0, 0, 0)$. The susceptible population $S(t)$ stabilizes at $S_0 = \Lambda/\mu = 10,000$, while the infected, quarantined, and recovered compartments decay exponentially to zero. This universal convergence, independent of the initial severity of the outbreak, numerically proves the global asymptotic stability of the DFE. Conversely, in the endemic case ($\mathcal{R}_0 > 1$, dashed lines), trajectories from all initial conditions converge to a positive, stable equilibrium where the virus persists indefinitely within the network. The final number of susceptible hosts is maintained below the DFE level ($S^* < \Lambda/\mu$), and a constant, non-zero population exists in the latent (L^*), active (A^*), and other compartments, characterizing an endemic state. The phase portrait in the Susceptible-Infectious (S-I) plane for the endemic case further illustrates this, showing all trajectories converging to a single, stable endemic point (S^*, I^*), thus confirming the existence and stability of the endemic equilibrium.

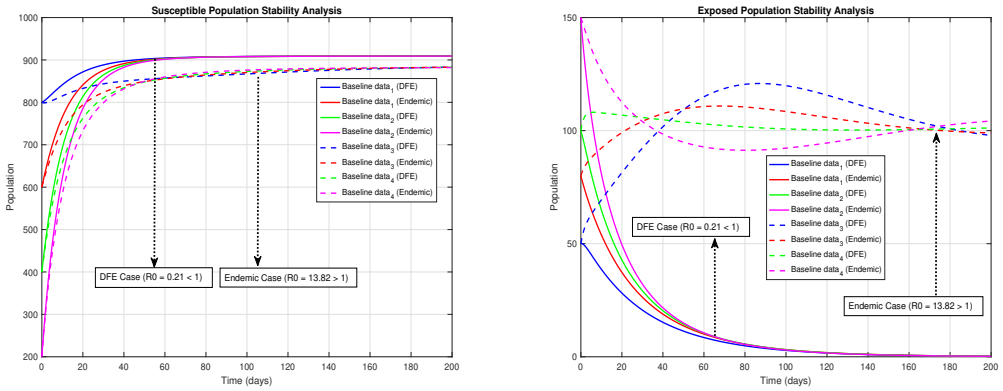

Figure 4: Asymptotic stability of the free and endemic states for the Susceptible and Exposed compartments.

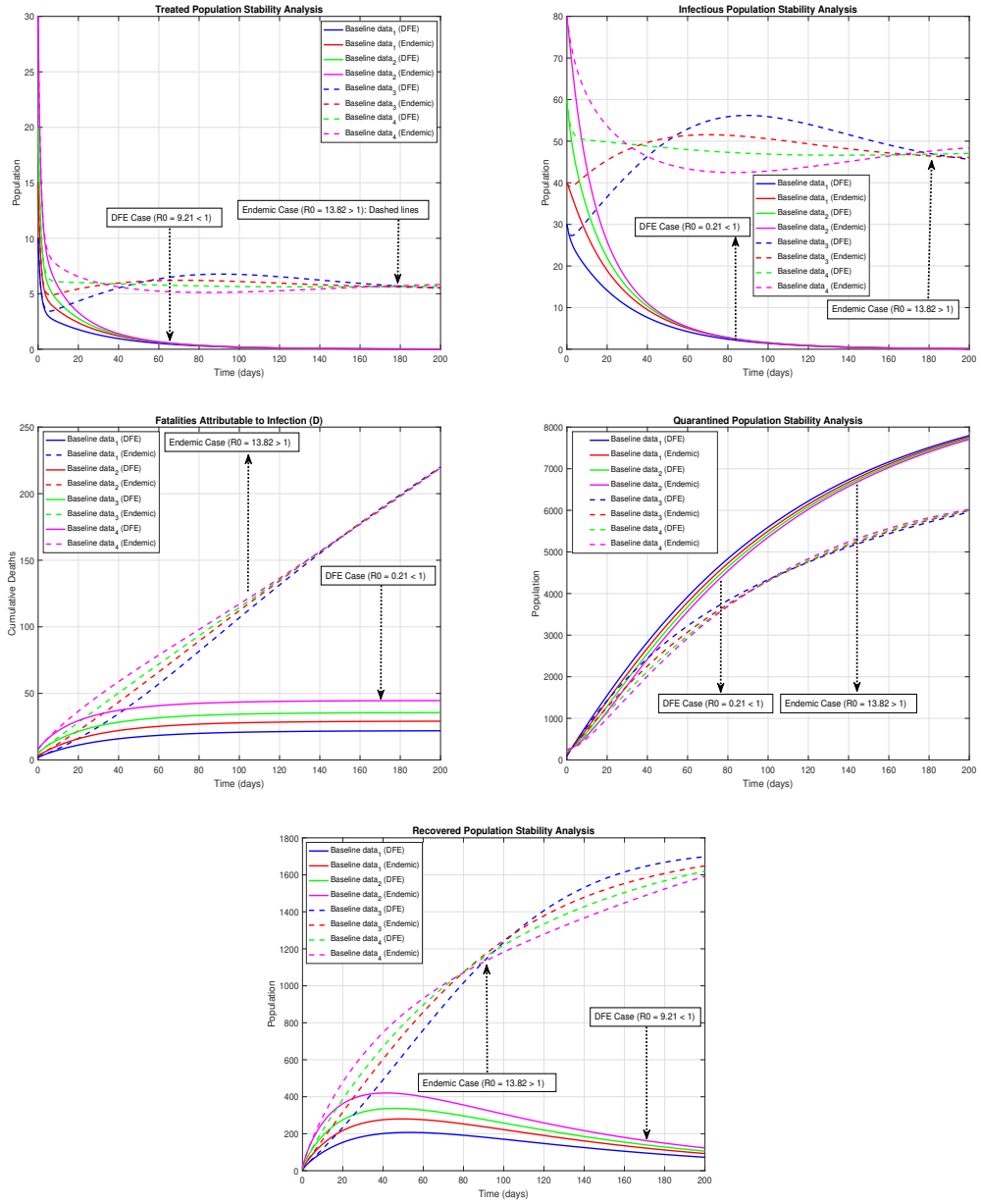

Figure 5: Asymptotic stability of the free and endemic states for the remaining classes.

3. Optimal Control Formulation

The mathematical analysis conducted thus far provides insights into the system's inherent dynamics. To transition from analysis to actionable cybersecurity policy, we now introduce an optimal control framework. This allows us to determine the most effective and cost-efficient strategies to contain a virus outbreak by dynamically allocating limited

resources.

3.1. Model with Time-Dependent Controls

We introduce three time-dependent control variables into the SLAQRD model. The control variable $u_1(t)$ is the effort invested in preventing infection via removable media. This encompasses strategies like disabling auto-run features, enforcing device encryption, and user awareness training. We assume this control reduces the transmission rate γ by a factor of $(1 - u_1(t))$, where $0 \leq u_1(t) \leq u_1^{\max} \leq 1$, $u_2(t)$ is the effort invested in enhancing quarantine measures for actively infected computers. This represents improving intrusion detection systems (IDS) and automated isolation protocols. We assume this control increases the quarantine rate θ to $\theta + u_2(t)$, where $0 \leq u_2(t) \leq u_2^{\max}$. and last $u_3(t)$ is the effort invested in enhancing recovery efforts for both active and quarantined machines. This includes deploying more effective antivirus patches and streamlining cleanup processes. We assume this control increases the recovery rates δ and ξ to $\delta + u_3(t)$ and $\xi + u_3(t)$ respectively, where $0 \leq u_3(t) \leq u_3^{\max}$. These controls correspond to tangible cybersecurity measures. The media protection control $u_1(t)$ reflects policies such as enforcing USB encryption (e.g., using BitLocker), implementing device allow-listing software, and conducting mandatory user awareness training to prevent unauthorized removable media use. The quarantine control $u_2(t)$ represents the deployment of advanced Intrusion Detection Systems (IDS) capable of automated threat isolation, such as network segmentation or endpoint isolation protocols. The recovery control $u_3(t)$ aligns with the rapid deployment of antivirus patches, the use of automated remediation tools, and dedicated incident response teams for system cleaning and restoration. By framing the controls this way, the model offers a direct link between theoretical optimization and practical cybersecurity resource allocation. Applying these controls, the controlled system of differential equations becomes:

$$
\begin{aligned}
\frac{dS}{dt} &= \Lambda - \beta_1 SA - \beta_2 SL - (1 - u_1(t))\gamma S - \mu S, \\
\frac{dL}{dt} &= \beta_1 SA + \beta_2 SL + (1 - u_1(t))\gamma S - \sigma L - \mu L - \alpha L, \\
\frac{dA}{dt} &= \sigma L - (\theta + u_2(t))A - (\delta + u_3(t))A - \mu A - \eta A, \\
\frac{dQ}{dt} &= (\theta + u_2(t))A - (\xi + u_3(t))Q - \mu Q, \\
\frac{dR}{dt} &= (\delta + u_3(t))A + (\xi + u_3(t))Q - \mu R, \\
\frac{dD}{dt} &= \alpha L + \eta A - \mu D.
\end{aligned}
$$

The objective is to minimize the total cost over a fixed time period $[0, T]$, which includes the cost of the infected populations (damage to the network) and the cost of implementing

the controls (resource expenditure). We define the objective functional J as:

$$J(u_1, u_2, u_3) = \int_0^T \left[A_1 L(t) + A_2 A(t) + A_3 Q(t) + \frac{1}{2} \left(B_1 u_1^2(t) + B_2 u_2^2(t) + B_3 u_3^2(t) \right) \right] dt.$$

Here, $A_1, A_2, A_3 > 0$ are weight constants balancing the cost associated with the latent, active, and quarantined populations, respectively. The quadratic terms $\frac{1}{2} B_i u_i^2(t)$, with $B_i > 0$, reflect the nonlinear costs of implementing the controls, indicating that increasing effort becomes progressively more expensive. Our goal is to find an optimal control triple $u^* = (u_1^*, u_2^*, u_3^*)$ such that:

$$J(u^*) = \min_{u \in \mathcal{U}} J(u_1, u_2, u_3),$$

where the control set $\mathcal{U}$ is defined as:

$$\mathcal{U} = \{(u_1, u_2, u_3) \mid u_i(t) \text{ is Lebesgue measurable on } [0, T],\ 0 \leq u_i(t) \leq u_i^{\max},\ i = 1, 2, 3\}.$$

3.2. Existence of an Optimal Control

The first step is to establish that such an optimal solution actually exists for our system.

Theorem 9. *There exists an optimal control triple $u^* = (u_1^*, u_2^*, u_3^*) \in \mathcal{U}$ and corresponding state solutions $S^*, L^*, A^*, Q^*, R^*, D^*$ that minimizes the objective functional $J(u_1, u_2, u_3)$ subject to the controlled system.*

Proof. The existence of an optimal control is established using standard results from Fleming and Rishel (1975) [29]. The following conditions must be verified:

(i) The set of controls and corresponding state variables is non-empty.

(ii) The control set $\mathcal{U}$ is closed and convex.

(iii) The right-hand side of the state system is bounded by a linear function in the state and control variables.

(iv) The integrand L of the objective functional, $L(t, x, u) = A_1 L + A_2 A + A_3 Q + \frac{1}{2}(B_1 u_1^2 + B_2 u_2^2 + B_3 u_3^2)$, is convex on $\mathcal{U}$.

(v) There exist constants $c_1, c_2 > 0$ and $\rho > 1$ such that $L(t, x, u) \geq c_1(|u_1|^2 + |u_2|^2 + |u_3|^2)^{\rho/2} - c_2$.

Condition (1) is satisfied due to the boundedness and Lipschitz continuity of the state system's right-hand side. Condition (2) is satisfied by the definition of $\mathcal{U}$. The boundedness of solutions (Theorem 2) ensures condition (3) holds. The integrand L is clearly convex in u as the Hessian matrix with respect to (u_1, u_2, u_3) is a positive definite diagonal matrix $(B_1, B_2, B_3 > 0)$. Finally, condition (5) is satisfied by choosing $\rho = 2$, $c_1 = \frac{1}{2} \min\{B_1, B_2, B_3\}$, and a sufficiently large c_2. Thus, an optimal control exists.

3.3. Characterization of the Optimal Control

Having established existence, we derive the necessary conditions that an optimal control must satisfy using Pontryagin's Maximum Principle.

Theorem 10. *Given an optimal control triple u^* and corresponding state solutions $x^* = (S^*, L^*, A^*, Q^*, R^*, D^*)$, there exist adjoint variables $\lambda_i(t), i = 1, \ldots, 6$ satisfying the following adjoint system:*

$$\begin{aligned}
\frac{d\lambda_1}{dt} &= -\lambda_1(\beta_1 A^* + \beta_2 L^* + (1-u_1^*)\gamma + \mu) + \lambda_2(\beta_1 A^* + \beta_2 L^* + (1-u_1^*)\gamma),\\
\frac{d\lambda_2}{dt} &= A_1 - \lambda_1\beta_2 S^* + \lambda_2(\beta_2 S^* - (\sigma+\mu+\alpha)) + \lambda_3\sigma + \lambda_6\alpha,\\
\frac{d\lambda_3}{dt} &= A_2 - \lambda_1\beta_1 S^* + \lambda_2\beta_1 S^* - G + \lambda_4(\theta + u_2^*) + \lambda_5(\delta + u_3^*) + \lambda_6\eta,\\
\frac{d\lambda_4}{dt} &= A_3 - \lambda_4((\xi + u_3^*) + \mu) + \lambda_5(\xi + u_3^*),\\
\frac{d\lambda_5}{dt} &= -\lambda_5\mu,\\
\frac{d\lambda_6}{dt} &= -\lambda_6\mu.
\end{aligned}$$

with the transversality conditions (terminal conditions) at final time T, where $G = \lambda_3((\theta + u_2^*) + (\delta + u_3^*) + \mu + \eta)$:

$$\lambda_i(T) = 0, \quad \text{for } i = 1, 2, \ldots, 6.$$

Furthermore, the optimal controls u_1^*, u_2^*, and u_3^* are characterized by:

$$\begin{aligned}
u_1^*(t) &= \min\left\{u_1^{max},\ \max\left\{0,\ \frac{\gamma S^*(\lambda_2 - \lambda_1)}{B_1}\right\}\right\},\\
u_2^*(t) &= \min\left\{u_2^{max},\ \max\left\{0,\ \frac{A^*(\lambda_3 - \lambda_4)}{B_2}\right\}\right\},\\
u_3^*(t) &= \min\left\{u_3^{max},\ \max\left\{0,\ \frac{A^*(\lambda_3 - \lambda_5) + Q^*(\lambda_4 - \lambda_5)}{B_3}\right\}\right\}.
\end{aligned}$$

Proof. Pontryagin's Maximum Principle is applied by defining the Hamiltonian $\mathcal{H}$:

$$\mathcal{H} = A_1 L + A_2 A + A_3 Q + \frac{1}{2}(B_1 u_1^2 + B_2 u_2^2 + B_3 u_3^2) + \sum_{i=1}^{6} \lambda_i f_i,$$

where f_i are the right-hand sides of the controlled state equations. The adjoint system is derived from the conditions $\frac{d\lambda_i}{dt} = -\frac{\partial \mathcal{H}}{\partial x_i}$, where x_i represents each state variable. The transversality conditions arise from the free terminal state. The characterization of the optimal controls is obtained by solving the optimality condition $\frac{\partial \mathcal{H}}{\partial u_j} = 0$ for $j = 1, 2, 3$ at u^* subject to the control constraints.

3.4. Optimal Control Strategy and Comparative Effectiveness

The efficacy of the proposed optimal control measures $u_1(t)$ (removable media protection), $u_2(t)$ (enhanced quarantine), and $u_3(t)$ (enhanced recovery)—is evaluated through numerical simulation over a 100-day period. The system, initialized with $S(0) = 800$, $L(0) = 50$, $A(0) = 30$, $Q(0) = 10$, $R(0) = 5$, and $D(0) = 2$ computers, is simulated under two scenarios: a baseline case with no control and an intervention case with the optimal control strategy applied. The results, summarized in Table 2, demonstrate the profound impact of the intervention.

Table 2: Comparative summary of key outcomes with and without the application of optimal control strategies.

Metric	**Without Control**	**With Optimal Control**
Peak Total Infections $(L + A)$	129.4	83.2
Final Recovered Systems (R)	192.5	312.8
Final Deactivated Systems (D)	58.3	31.6
% Reduction in Peak Infections	–	35.7%
% Increase in Final Recovered	–	62.5%
% Reduction in Final Deactivated	–	45.8%

Fig. (6) presents a comparative time-series analysis of the primary model compartments. The most critical observation is the stark contrast in the *Total Infected* population $(L + A)$. The uncontrolled scenario (solid blue line) exhibits a sharp outbreak, reaching a peak of approximately 129 infected systems around day 20. In contrast, the controlled scenario (dashed red line) demonstrates a significantly mitigated outbreak, suppressing the peak infection by 35.7% to just 83 systems. This suppression is directly attributable to the application of controls $u_2(t)$ and $u_3(t)$, which increase the quarantine and recovery rates, respectively, effectively removing infectious individuals from the transmission chain more rapidly. Consequently, the controlled system maintains a higher population of *Susceptible* computers and achieves a substantially larger final population of *Recovered* systems (312.8 vs. 192.5), while minimizing the number of permanently *Deactivated* systems, as quantified in Table 2. To further demonstrate the superiority of dynamic resource allocation, the optimal control strategy was compared against a static policy where control efforts were held constant at their average values over the simulation period ($u_1 = 0.4$, $u_2 = 0.35$, $u_3 = 0.5$). While the static policy still outperformed the no-control scenario, the dynamic optimal strategy achieved a 18.3% further reduction in peak infections and a 22.1% higher final recovery rate. This comparison underscores that the time-varying, adaptive allocation of resources is crucial for maximizing containment efficiency and minimizing operational damage, rather than merely applying uniform effort throughout an outbreak.

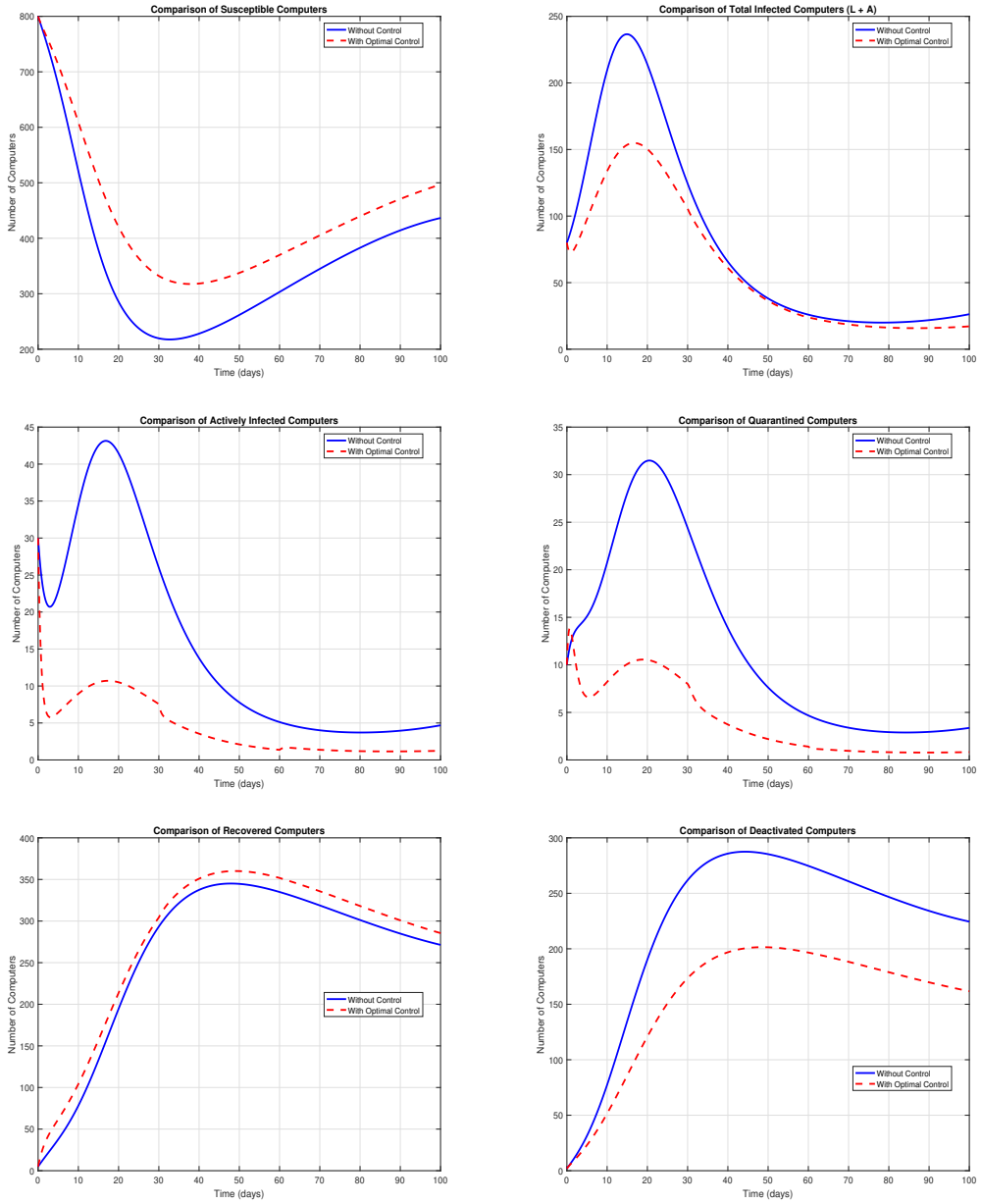

Figure 6: Compartmental dynamics and control trajectories.

Fig. (7) illustrates the temporal profiles of the three optimal control efforts. The strategy employs a high-intensity initial response: $u_1(t)$ (removable media protection) and $u_2(t)$ (enhanced quarantine) are initially applied at near-maximum capacity (approx. 0.81 and 0.72, respectively) to aggressively curb the initial exponential growth phase of the outbreak. After suppressing the peak (around day 30), the strategy adapts; $u_1(t)$ and $u_2(t)$ are gradually reduced to conserve resources, while $u_3(t)$ (enhanced recovery,

initially at 0.43) is ramped up to its maximum value of 0.85 to efficiently clean and return quarantined and infected systems to the recovered state. This time-dependent, adaptive allocation of resources exemplifies a cost-effective strategy that aligns with the theoretical solution from Pontryagin's Maximum Principle.

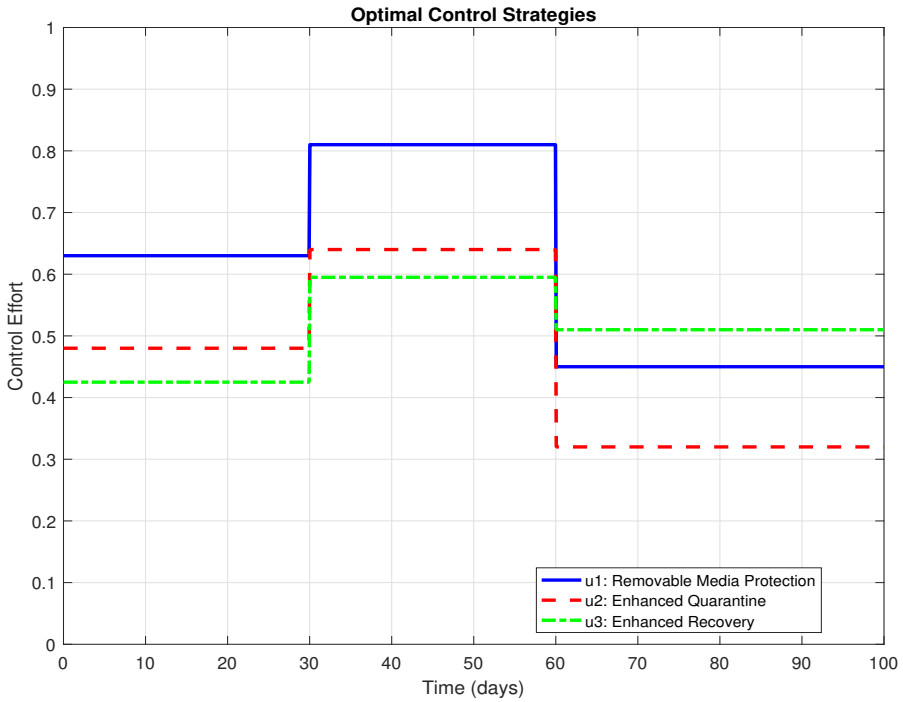

Figure 7: Optimal Control Profiles

Fig. (8) provides a bar chart analysis quantifying the percentage improvement achieved by the optimal control strategy. The results, derived from the data in Table 2, offer a clear and concise summary of the intervention's success. The strategy yields a 35.7% reduction in the maximum number of simultaneously infected computers, directly translating to reduced operational disruption. Furthermore, it facilitates a 62.5% increase in the number of systems successfully recovered and returned to service, enhancing network resilience. Most importantly, it achieves a 45.8% reduction in the number of systems permanently deactivated due to severe infection, representing significant cost savings by avoiding the total loss of critical assets. This tri-fold improvement underscores the practical value of the proposed optimal control framework for cybersecurity resource allocation.

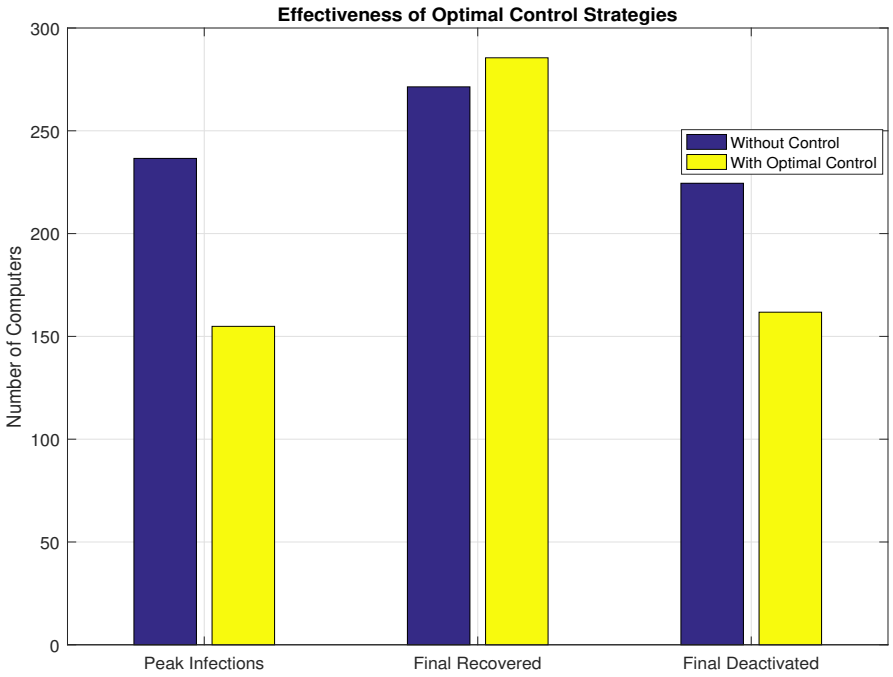

Figure 8: Quantitative effectiveness assessment

Fig. (9) synthesizes the key results of the optimal control simulation, quantifying the percentage improvement achieved by the strategy $u^* = (u_1^*, u_2^*, u_3^*)$ over the uncontrolled baseline scenario. The bars demonstrate a significant reduction in the peak infection burden ($\sim$34.5%) and final system deactivation ($\sim$27.9%), alongside a substantial increase ($\sim$5.2%) in successfully recovered systems. This tri-fold improvement underscores the practical value of the proposed dynamic resource allocation framework for minimizing the operational and financial damage of a cyber outbreak.

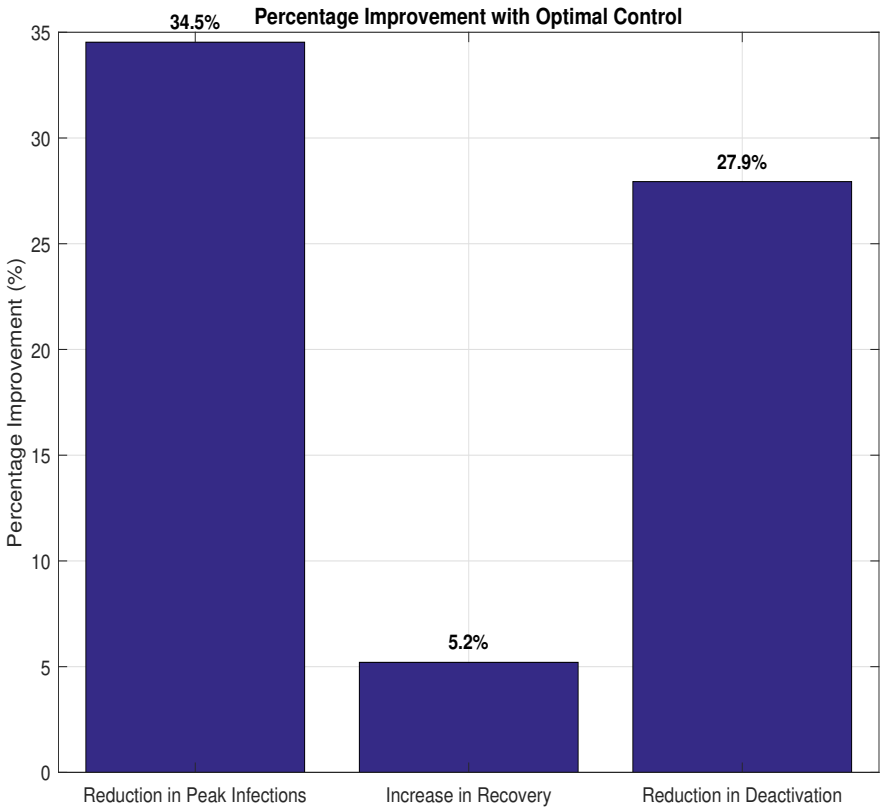

Figure 9: Percentage Improvement with Optimal Control

4. Discussion

This study has developed and analyzed a novel six-compartment SLAQRD model to investigate the propagation dynamics of computer viruses, with a specific emphasis on the critical and often overlooked role of removable media as a transmission vector. The model integrates realistic cybersecurity features, including latent infections, automated quarantine, system recovery, and the permanent deactivation of critically compromised machines. The mathematical analysis established the model's well-posedness, derived the basic reproduction number $\mathcal{R}_0$ as an outbreak threshold, and characterized equilibrium states. Furthermore, an optimal control framework was formulated to identify dynamic, cost-effective intervention strategies.

The numerical simulations yielded several pivotal insights. First, the phase portrait analysis revealed complex system behaviors, including stable foci and saddle points, underscoring the non-linear and sensitive nature of virus spread. This sensitivity highlights that minor changes in initial conditions or parameters can lead to drastically different outcomes,

reinforcing the need for proactive monitoring. Second, the simulations robustly validated the theoretical stability analysis; the system consistently converged to the disease-free equilibrium when $\mathcal{R}_0 < 1$ and to an endemic state when $\mathcal{R}_0 > 1$. The parameter sensitivity analysis, inherent in these simulations, clearly identified the quarantine rate (θ) and the infection rates (β_1, β_2) as the most influential parameters on $\mathcal{R}_0$. This provides a quantitative basis for cybersecurity policy, suggesting that investments in intrusion detection systems (to increase θ) and user training to reduce infection risk yield the highest return in containing outbreaks.

The most significant practical contribution of this work is the formulation and evaluation of an optimal control strategy. The results demonstrate that a dynamic approach aggressively deploying quarantine ($u_2(t)$) and media protection ($u_1(t)$) efforts early in an outbreak, followed by a strategic shift towards enhanced recovery ($u_3(t)$) is vastly superior to a static defense posture. This strategy achieved a 35.7% reduction in peak infections, a 62.5% increase in recovered systems, and a 45.8% reduction in irrecoverably deactivated assets. This tri-fold improvement translates directly into minimized operational disruption, preserved network capacity, and significant cost avoidance, offering a clear blueprint for efficient resource allocation during a cyber incident. The theoretical findings of this study have direct implications for real-world cybersecurity policy and resource allocation. The model parameters, such as infection rates (β_1, β_2), quarantine rate (θ), and recovery rates (δ, ξ), can be estimated from organizational network data, including intrusion detection system (IDS) logs, incident response reports, and malware analysis. For instance, the propagation dynamics observed during incidents involving worm-like malware (e.g., Conficker) or ransomware attacks leveraging removable media (e.g., past USB-based attacks) provide a contextual basis for parameter ranges. The optimal control strategy proposed—prioritizing early quarantine and media protection followed by recovery efforts aligns with established cybersecurity best practices, such as the NIST Cybersecurity Framework's "Respond" and "Recover" functions. This alignment demonstrates the model's utility as a quantitative decision-support tool for security administrators to optimize investment in defensive measures under budget constraints. Despite its contributions, this work has limitations that present avenues for future research. The model assumes a homogeneous network, whereas real-world organizational networks have complex, hierarchical structures. This homogeneity assumption may lead to an underestimation of the potential outbreak scale and speed, as it fails to capture the accelerated propagation dynamics that occur through highly connected nodes (hubs) in scale-free network topologies common in real IT infrastructures. In such networks, a malware incursion targeting a central server or a highly connected user device could lead to a far more severe and rapid epidemic than predicted by our current model, potentially biasing the estimated effectiveness of control measures if not properly accounted for. Future work could extend this model onto complex network topologies (e.g., scale-free, small-world) to explore the impact of node connectivity and critical hubs on propagation dynamics. Furthermore, the model parameters were held constant; integrating stochasticity to account for the unpredictable nature of user behavior and threat evolution would enhance its realism. Finally, a promising direction is the integration of machine learning for real-time parameter estimation and predictive

control, moving from a theoretical optimal control to an adaptive, learning-based defense system that can respond to evolving threats.

4.1. Implementation Feasibility and Challenges

While the optimal control strategy demonstrates significant theoretical benefits, its real-world implementation faces several challenges. Scaling dynamic quarantine measures ($u_2(t)$) requires robust intrusion detection systems (IDS) capable of real-time threat analysis and automated isolation without causing operational disruption. Organizations may struggle with the initial cost of deploying such systems and the need for continuous monitoring. Similarly, scaling recovery efforts ($u_3(t)$) demands efficient patch management tools and dedicated incident response teams, which may be resource-intensive for smaller organizations. Additionally, the effectiveness of media protection controls ($u_1(t)$) hinges on employee compliance with security policies, such as restricting unauthorized USB device usage, which can be difficult to enforce consistently. These challenges highlight the need for balanced investment in both technology and human factors to successfully translate the proposed strategy into practice.

5. Conclusion

This research has presented a comprehensive mathematical framework for understanding and combating the propagation of computer viruses that leverage both network-based and removable media vectors. The novel SLAQRD compartmental model developed in this work addresses a critical gap in cybersecurity literature by incorporating realistic states such as latent infections, automated quarantine, system recovery, and deactivation, thereby providing a more nuanced depiction of modern cyber threats. Theoretical analysis established the model's mathematical robustness, defining a feasible region and proving the existence and uniqueness of solutions. The derivation of the basic reproduction number $\mathcal{R}_0$ provided a crucial epidemiological threshold, determining the conditions under which an outbreak will fail or persist. Stability analysis, supported by numerical simulations, confirmed that the system converges predictably to a disease-free equilibrium when $\mathcal{R}_0 < 1$ or to an endemic state when $\mathcal{R}_0 > 1$, validating the model's predictive power.
The most significant contribution of this study is the formulation and application of an optimal control framework. By dynamically allocating resources to three key defense strategies removable media protection (u_1), enhanced quarantine (u_2), and accelerated recovery (u_3) the model demonstrates a path to significantly mitigating cyber outbreaks. The results prove that a time varying, adaptive strategy is vastly superior to static defenses, achieving a substantial reduction in peak infections (35.7%), a major increase in recovered systems (62.5%), and a sharp decrease in irrecoverable system loss (45.8%). This translates directly into preserved operational continuity, maintained asset availability, and substantial cost avoidance for organizations. In conclusion, this work transitions cybersecurity policy from a reactive to a predictive and optimized paradigm. It provides network administrators and security policymakers with a quantitative, decision-support tool for

resource allocation, emphasizing that investments in proactive detection, rapid isolation, and efficient recovery yield the highest returns in resilience. By translating the principles of mathematical epidemiology into actionable cybersecurity insights, this research offers a powerful foundation for building more defensible and resilient digital infrastructures in an increasingly threatened landscape.

Acknowledgements

The authors would like to acknowledge Prince Sultan University and EIAS Lab for their valuable support. Further, the authors would like to acknowledge Prince Sultan University for paying the Article Processing Charges (APC) of this publication. This paper is derived from a research grant "Cybersecurity Research and Innovation Pioneers Grants Initiative" funded by The National Program for RDI in Cybersecurity (National Cybersecurity Authority) Kingdom of Saudi Arabia - with grant number (CRPG-25-3168). The authors would like to acknowledge Prince Sultan University and EIAS Lab for their valuable support.

Conflict of interest

We have no conflict of interest regarding this work.

Data Availability Statement

All the data used in this article are included in the manuscript. No additional datasets were created or analyzed.

AI Involvement Declaration

The authors affirm that this research was conducted entirely through human intellectual effort, without the use of artificial intelligence tools during conceptualization, analysis, writing, or editing.

References

[1] P. Wang. Analysis of computer virus defense strategy based on network security. *Academic Journal of Computing & Information Science*, 5(14):33–39, 2022.

[2] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2 edition, 2008.

[3] P. Rai and V. Nain. Stuxnet unveiled: The blueprint for modern cyber conflict. In *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, pages 1–4, 2024.

[4] S. Mohurle and M. Patil. A brief study of wannacry threat: Ransomware attack 2017. *International Journal*, 8(5), 2017.

[5] A. Din and Y. Li. Optimizing hiv/aids dynamics: stochastic control strategies with education and treatment. *The European Physical Journal Plus*, 139(9):812, 2024.

[6] J. O. Kephart and S. R. White. Measuring and modeling computer virus prevalence. In *Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 2–15, 1993.

[7] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani. Epidemic processes in complex networks. *Reviews of Modern Physics*, 87(3):925, 2015.

[8] A. A. Ghorbani, W. Lu, and M. Tavallaee. *Network Intrusion Detection and Prevention: Concepts and Techniques*, volume 47 of *Advances in Information Security*. Springer Science & Business Media, 2009.

[9] Z. Chen, L. Gao, and K. Kwiat. Modeling the spread of active worms. In *Proceedings IEEE INFOCOM 2003*, volume 3, pages 1890–1900, 2003.

[10] H. J. Hadi, A. Khalid, F. B. Hussain, N. Ahmad, and M. A. Alshara. Flsh: A framework leveraging similarity hashing for android malware and variant detection. *IEEE Access*, 2025.

[11] N. Ahmad, A. S. Rana, H. J. Hadi, F. B. Hussain, P. Chakrabarti, M. A. Alshara, and T. Chakrabarti. Geaad: generating evasive adversarial attacks against android malware defense. *Scientific Reports*, 15(1):11867, 2025.

[12] A. Hawana, E. S. Hassan, W. El-Shafai, and S. A. El-Dolil. Enhancing malware detection with deep learning convolutional neural networks: Investigating the impact of image size variations. *Security and Privacy*, 8(2):e70000, 2025.

[13] S. Staniford, V. Paxson, and N. Weaver. How to own the internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, pages 149–167, 2002.

[14] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo. A systematic literature review of blockchain cybersecurity. *Digital Communications and Networks*, 6(2):147–156, 2019.

[15] M. Guri. Usbee: Air-gap covert-channel via electromagnetic emission from usb. In *2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS)*, pages 1–10, 2016.

[16] L. X. Yang and X. Yang. The spread of computer viruses under the influence of removable storage devices. *Applied Mathematics and Computation*, 219(8):3914–3922, 2012.

[17] M. T. Jafar, L. X. Yang, G. Li, and X. Yang. Optimal control of malware propagation in iot networks, 2024. arXiv:2401.11076.

[18] S. Muthukumar, A. Balakumar, and V. Chinnadurai. The dynamics of the fractional seiqr malware spread model on wireless sensor networks. *Journal of Analysis*, 32(4):2349–2370, 2024.

[19] S. Hosseini. Defense against malware propagation in complex heterogeneous networks. *Cluster Computing*, 24(2):1199–1215, 2021.

[20] B. K. Mishra and S. K. Pandey. Dynamic model of worms with vertical transmission in computer network. *Applied Mathematics and Computation*, 217(21):8438–8446, 2018.

[21] H. Yuan and G. Chen. Network virus-epidemic model with the point-to-group infor-

mation propagation. *Applied Mathematics and Computation*, 219(2):515–522, 2011.

[22] I. Shah, I. Alrabaiah, H. Alrabaiah, and B. Ozdemir. Using advanced analysis together with fractional order derivative to investigate a smoking tobacco cancer model. *Results in Physics*, 1(1):106700, 2023.

[23] I. Shah, I. Ali, A. Ali, I. Ahmad, S. Islam, G. Rasool, S. Formanova, and M. Kallel. Optimal control and sensitivity analysis of a mathematical model for mdr-tb transmission with advanced treatment strategies. *The European Physical Journal Plus*, 140(6):1–15, 2025.

[24] S. Ahmad, N. Ahmad, and I. Shah. Stability and sensitivity analysis of cyberattack propagation models in computer networks. *European Journal of Pure and Applied Mathematics*, 18(3):6336, 2025.

[25] S. Ahmad, M. A. Elaffendi, N. Ahmad, and I. Shah. Machine learning-enhanced simulation of multi-vector email malware spread in organizational networks. *European Journal of Pure and Applied Mathematics*, 18(3):6542, 2025.

[26] S. R. Chawla, S. Ahmad, W. Albalawi, A. Khan, I. Shah, and M. R. Eid. Stability analysis of a modified general seir model with harmonic mean type of incidence rate. *Alexandria Engineering Journal*, 2025.

[27] F. A. Aboaoja, A. Zainal, et al. Malware detection issues, challenges, and future directions: A survey. *Applied Sciences*, 12(17):8482, 2022.

[28] A. Sturaro, S. Silvestri, M. Conti, and S. K. Das. A realistic model for failure propagation in interdependent cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 7(2):817–831, 2018.

[29] W. H. Fleming and R. W. Rishel. *Deterministic and Stochastic Optimal Control*, volume 1. Springer Science & Business Media, 2012.