Application of Impulsive SIRQ Models for the Development of Forecasting and Cyberattack Mitigation Scenarios

Valentyn Sobchuk , Vitalii Savchenko * , Bohdan Stepanchenko , Halyna Haidur

Posted Date: 26 February 2026

doi: 10.20944/preprints202602.1283.v1

Keywords: impulsive systems; periodic solutions; functional stability; nonlinear dynamics; SIR model; control;stable dynamics; adaptive strategies counter

 doi:10.20944/preprints202602.1283.v1

Article

Application of Impulsive SIRQ Models for the Development of Forecasting and Cyberattack Mitigation Scenarios

Valentyn Sobchuk [1], Vitalii Savchenko [2,*], Bohdan Stepanchenko [2] and Halyna Haidur [2]

[1] Faculty of Mechanics and Mathematics, Taras Shevchenko National University of Kyiv, Volodymyrska Street 64, 01601 Kyiv, Ukraine

[2] Educational and Scientific Institute of Cybersecurity and Information Protection, State University of Information and Communication Technologies, Solomyanska St., 7, 03110 Kyiv, Ukraine

* Correspondence: savitan@ukr.net

Abstract

This paper proposes an impulsive SIRQ model for the analysis of computer network resilience against malware propagation and distributed denial-of-service (DDoS) attacks. The model extends classical epidemic frameworks by combining continuous-time dynamics of malicious object spreading with discrete control actions corresponding to mass updates, node isolation, and access control policies. A qualitative analysis of the resulting system of impulsive differential equations is performed. The basic reproduction number $\mathcal{R}_0$ identified as a threshold parameter characterizing the intensity of attack propagation, and sufficient conditions for the global asymptotic stability of the infection-free regime are established. It is shown that, under periodic impulsive control, the infection-free state can be stabilized with respect to the target population coordinates even when $\mathcal{R}_0 > 1$. An exponential decay estimate for the total active threat is derived, guaranteeing the asymptotic extinction of the infected and quarantined node populations. The proposed approach provides quantitative criteria for the effectiveness of impulsive cyber-defense strategies and offers a theoretical foundation for the design of adaptive multi-layer protection systems for critical information infrastructures.

Keywords: impulsive systems; periodic solutions; functional stability; nonlinear dynamics; SIR model; control; stable dynamics; adaptive strategies counter

MSC: 34A37; 93C27; 68M25; 62M20

1. Introduction

Over recent years, cyberattacks against critical infrastructure have assumed a systemic character and evolved from isolated incidents into an integral component of hybrid threats. Energy systems, transportation networks, the banking sector, communication systems, and water and heat supply facilities are increasingly becoming targets of well-organized and technically sophisticated adversaries. Of particular concern are distributed denial-of-service (DDoS) attacks [1,2], which are capable of paralyzing the operation of critically important services within minutes, causing significant economic losses and large-scale social consequences.

Unlike traditional cyberattacks, which are typically aimed at data theft or unauthorized access, DDoS attacks primarily seek to disrupt service availability [3]. For critical infrastructure facilities, this entails the risk of halting production processes, losing control over technological systems, and experiencing disruptions in the supply of electricity, water, or heat, and in some cases poses a direct threat to human life and health. Consequently, cybersecurity in this domain acquires strategic importance and is no longer viewed solely as a technical issue, but rather as a transnational security challenge [4,5].

 doi:10.20944/preprints202602.1283.v1

Modern attacks on critical infrastructure are characterized by a high degree of automation, the use of botnets comprising hundreds of thousands of compromised devices, and sophisticated techniques for masquerading as legitimate traffic [2]. This significantly complicates their timely detection by conventional filtering and monitoring mechanisms. Under these conditions, mathematical models are gaining increasing importance, as they make it possible not only to describe the dynamics of attack propagation within a network, but also to forecast its evolution and to assess the effectiveness of various defense strategies [6]

At present, the modeling of malicious object propagation in computer networks is increasingly carried out using methodologies borrowed from classical epidemiological models [7]. The spread of computer viruses, botnets, or DDoS agents exhibits a pronounced structural analogy with the dynamics of biological epidemics [8], which makes compartmental approaches – particularly SIR and SIRQ models – an effective tool for analysis and forecasting [6].

In the cybersecurity context, the variables $\mathcal{S}$ (*Susceptible*), $\mathcal{I}$ (*Infected*), $\mathcal{R}$ (*Removed/Recovered*), and $\mathcal{Q}$ (*Quarantined*) are interpreted as components of a network: in particular, $\mathcal{I}$ represents bots actively attacking a server, $\mathcal{S}$ denotes potential new bots, $\mathcal{Q}$ corresponds to blocked IP addresses, network segments, or VLANs, and $\mathcal{R}$ refers to cleaned and patched devices. Such a representation makes it possible to estimate the rate of malicious code propagation, identify critical thresholds (analogous to the epidemiological threshold $\mathcal{R}_0$), and forecast cyberattack development scenarios in real time [9].

However, the practical operation of a network is characterized by the presence of sudden and irregular influences that cannot be adequately captured within the framework of classical continuous models. Such influences include mass antivirus updates, forced reboots, the enforcement of isolation policies, traffic throttling, or other instantaneous mitigation measures. These effects are naturally described by so-called impulsive systems [10], which make it possible to model discrete control actions embedded within the continuous dynamics of threat propagation.

The application of impulsive approaches in SIR-type models enables the formulation of realistic cyberattack response scenarios. In particular, periodically or quasi-periodically acting impulses allow one to represent situations in which preventive or protective measures are applied irregularly but within certain constraints – for example, in the case of unscheduled updates, nonuniform security checks, or automated responses to traffic anomalies. The analysis of the existence and asymptotic stability of infection-free periodic or quasi-periodic solutions of such systems reflects the conditions under which a network can maintain functional stability [11,12] and return to a secure state after sudden impulsive perturbations. This constitutes an important component that qualitatively distinguishes the controllability of complex systems described by classical models with well-studied mathematical formalisms [13–16].

The use of such models is critically important for the development of adaptive cyberattack mitigation strategies and for forecasting their evolution [6]. They make it possible to:

- Assess network infection rates as a function of network topology and the security level of individual nodes;
- Evaluate the effectiveness of different types of impulsive control, ranging from mass updates to the isolation of individual segments;
- Develop resilience scenarios for critical infrastructure under conditions of repeated attacks;
- Model the behavior of malicious botnets and substantiate optimal intervention points;
- Forecast the consequences of large-scale DDoS campaigns in environments with varying densities of vulnerable IoT devices;
- Design multi-layered cyber defense systems based on principles of controllability and asymptotic stability.

Thus, extending epidemic models to incorporate impulsive periodic effects enhances their applied value and enables the development of realistic tools for risk forecasting and control in the field of cybersecurity. This approach combines the mathematical rigor of classical stability theory with the practical demands of modern complex telecommunication and information systems, and

 doi:10.20944/preprints202602.1283.v1

can be effectively employed in tasks related to planning, threat analysis, and the design of adaptive protection strategies for both epidemiological and cyber applications.

In this paper, we investigate an electronic epidemic model of a DDoS attack on target resources in a computer network. Particular attention is devoted to a detailed analysis of the stability conditions of periodic regimes in the corresponding impulsive system.

2. Motivation and Problem Statement

In the proposed model, the entire set of network nodes is divided into two populations: an attacking population and a targeted population. It is natural to assume that the primary objective of an adversary is to identify as many vulnerable nodes as possible within the attacking population and subsequently exploit them to carry out an attack against a specified targeted population. In practice, the total size of the targeted population can be assumed to be constant. Accordingly, the loss of any infected nodes as a result of a DDoS attack is considered to be compensated through their recovery, cleansing from compromise ("infection") in a quarantine mode, and subsequent return to the class of recovered target nodes [9]. This assumption ensures the constancy of the targeted population size throughout the entire modeling process.

Vulnerable nodes operate according to a dual scheme: on the one hand, they are used to discover new nodes for the subsequent propagation of the attack, and on the other hand, they are directly involved in attacks on target resources (Figure 1). At the same time, vulnerable nodes do not enter a state of permanent recovery and, after completing the corresponding stages, return to the susceptible class.

Since attacks on critical infrastructure facilities are typically extremely intensive and destructive, the target network resources must therefore be equipped with significantly more powerful protection and response mechanisms compared to conventional information systems.

In the model presented in Figure 1, the following system of variables and parameters is employed. The symbol S denotes the class of susceptible attacking nodes, i.e., nodes of the attacking population that have not yet been involved in the attack but may be compromised. The class $\mathcal{I}$ corresponds to infected attacking nodes that actively participate in the generation of malicious traffic and the execution of DDoS attacks.

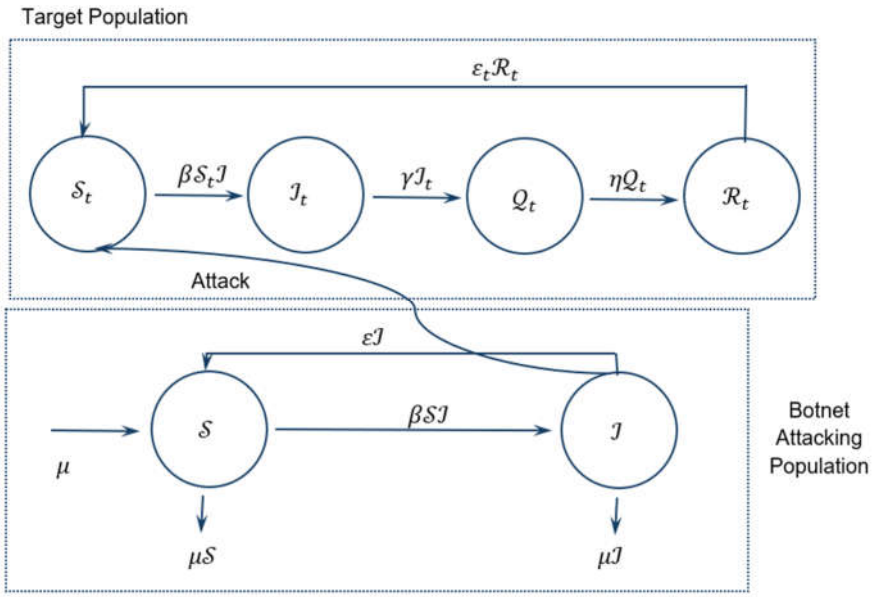

Figure 1. Schematic representation of the model.

 doi:10.20944/preprints202602.1283.v1

The quantity $\mathcal{S}_t$ characterizes the number of susceptible target nodes that are in a normal operational state but may be affected by an attack. The variable $\mathcal{I}_t$ corresponds to infected target nodes whose functioning is disrupted as a result of a DDoS attack. The notation $\mathcal{Q}_t$ denotes target nodes that have been placed in a quarantine mode in order to localize the attack and carry out recovery measures. The class $\mathcal{R}_t$ describes recovered target nodes that, after cleansing and technical maintenance, have returned to normal operating conditions [9].

The parameter β is the infection contact rate and determines the intensity of attack propagation in the network, proportional to the product of the numbers of susceptible and infected nodes. The parameter μ characterizes the natural rate of removal and admission of attacking nodes in the network, corresponding to node failures due to technical reasons and the appearance of new nodes, respectively. The parameter ε defines the rate at which infected attacking nodes return to the susceptible class, while the parameter ε_t describes the rate of immunity loss of recovered target nodes and their subsequent transition back to the susceptible class.

The intensity of transferring infected nodes into quarantine is determined by the parameter γ. The parameter η characterizes the rate at which quarantined nodes, after undergoing recovery procedures, return to the class of recovered target nodes.

Note that the coefficients $\beta,\ \delta,\ \eta,\ \varepsilon,\ \mu,$ and γ are positive.

3. Impulsive SIRQ Model

Accordingly, the model can be mathematically represented by a system of differential equations of the form:

$$\begin{cases} \dot{\mathcal{S}}_t = -\beta \mathcal{S}_t \mathcal{I} + \varepsilon_t \mathcal{R}_t, \\ \dot{\mathcal{I}}_t = \beta \mathcal{S}_t \mathcal{I} - \gamma \mathcal{I}_t, \\ \dot{\mathcal{Q}}_t = \gamma \mathcal{I}_t - \eta \mathcal{Q}_t, \\ \dot{\mathcal{R}}_t = \eta \mathcal{Q}_t - \varepsilon_t \mathcal{R}_t. \end{cases} \tag{1}$$

Here is $\mathcal{S}_t + \mathcal{I}_t + \mathcal{Q}_t + \mathcal{R}_t = 1.$

$$\begin{cases} \dot{\mathcal{S}} = \mu - \beta \mathcal{S}\mathcal{I} + \mu \mathcal{S} + \varepsilon \mathcal{I}, \\ \dot{\mathcal{I}} = \mu \mathcal{S}\mathcal{I} - (\mu + \varepsilon)\mathcal{I}. \end{cases} \tag{2}$$

Here is $\mathcal{S} + \mathcal{I} = 1.$

Eliminating from systems (1) and (2) $\mathcal{R}_t = 1 - \mathcal{S}_t - \mathcal{I}_t - \mathcal{Q}_t$ and $\mathcal{S} = 1 - \mathcal{I}$, we obtain

$$\begin{cases} \dot{\mathcal{S}}_t = -\beta \mathcal{S}_t \mathcal{I} + \varepsilon_t (1 - \mathcal{S}_t - \mathcal{I}_t - \mathcal{Q}_t), \\ \dot{\mathcal{I}}_t = \beta \mathcal{S}_t \mathcal{I} - \gamma \mathcal{I}_t, \\ \dot{\mathcal{Q}}_t = \gamma \mathcal{I}_t - \eta \mathcal{Q}_t, \\ \dot{\mathcal{I}} = \beta (1 - \mathcal{I})\mathcal{I} - (\mu + \varepsilon)\mathcal{I}. \end{cases} \tag{3}$$

Let's put

$$\Omega = \{P = \{\mathcal{S}_t, \mathcal{I}_t, \mathcal{Q}_t, \mathcal{I}\} \in \mathbb{R}_+^4 \mid \mathcal{S}_t + \mathcal{I}_t + \mathcal{Q}_t \le 1, \mathcal{I} \le 1\}.$$

An important indicator characterizing the epidemic threshold is – $\mathcal{R}_0$, the value of which is determined by the ratio

$$\mathcal{R}_0 = \frac{\beta}{\mu + \varepsilon}.$$

Theorem 1 [9]. *For any initial data* $P(0) \in \Omega$, *the solution* $P(t)$ *of system (3) exists on the interval* $[0, +\infty)$ *and satisfies* $P(t) \in \Omega$ *for all* $t \ge 0$.

If $\mathcal{R}_0 \le 1$, then there exists a unique equilibrium point (infection-free) in the set Ω,

$$P_0^* = \{\mathcal{S}_t^* = 1, \mathcal{I}_t^* = 0, \mathcal{Q}_t^* = 0, \mathcal{I}^* = 0\},$$

which is *globally asymptotically stable* in Ω.

If $\mathcal{R}_0 > 1$, an avalanche-like propagation of the attack occurs. In this case, P_0^* is unstable and another equilibrium point

 doi:10.20944/preprints202602.1283.v1

$$P_0^{**} = \{\mathcal{S}_t^{**}, \mathcal{I}_t^*, \mathcal{Q}_t^*, \mathcal{I}^*\}$$

with positive components (endemic equilibrium) emerges in Ω, which is globally asymptotically stable in $\operatorname{int}\Omega$.

By modeling the processes of updating the corresponding antivirus software of the target node population as abrupt reductions in the number of vulnerable nodes at prescribed time instants, we arrive at an impulsive problem

$$\Delta\mathcal{S}_t|_{t=t_n} := \mathcal{S}_t(t_n + 0) - \mathcal{S}_t(t_n) = -b_n\mathcal{S}(t_n), \tag{4}$$

where $\{b_n\} \subset (0,1)$, $\{t_n\}$ are the given values and moments of impulse disturbances, respectively.

We assume that the presence of the *immunizing perturbation* (4) can fundamentally alter the linear behavior of the solutions of system (3) described in Theorem 1.

In particular, when $\mathcal{R}_0 > 1$ and under certain conditions on the sequences $\{b_n\}$ and $\{t_n\}$, system (3), (4) admits an *infection-free periodic solution* $\bar{P}(t)$ that is asymptotically stable with respect to the subset of coordinates corresponding to the target nodes.

Let us consider the following problem (4):

$$0 < t_1 < t_2 < \cdots < t_p < T, \qquad t_{n+p} = t_n + T, \qquad n \geq 1, \qquad b_{n+p} = b_n, \qquad n \geq 1. \tag{5}$$

Theorem 2. *Under conditions (5), problem (3) admits a T-periodic impulsive solution $\bar{P}(t) = \{\bar{\mathcal{S}}(t), 0, 0, 0\}$, which is infection-free. Moreover,*

$$\sup_{t\geq 0} \bar{\mathcal{S}}(t) \to 0, \qquad T \to 0. \tag{6}$$

Proof of Theorem 2. Let us find $\bar{\mathcal{S}}(t)$ as a T-periodic impulse solution of the problem

$$\begin{cases} \dot{\mathcal{S}} = \varepsilon(1 - s), \\ \Delta\mathcal{S}|_{t=t_n} = -b_n\mathcal{S}(t_n). \end{cases} \tag{7}$$

System (7) is obtained from (3) for $\mathcal{I}_t \equiv 0$, $\mathcal{Q}_t \equiv 0$, $\mathcal{I} \equiv 0$. For convenience, we denote $\mathcal{S} = \mathcal{S}_t$, $\varepsilon = \varepsilon_t$. On the interval of continuity $[\tau, t]$

$$\mathcal{S}(t) = (\mathcal{S}(\tau) - 1)e^{-\varepsilon(t-T)} + 1.$$

Therefore

$$\mathcal{S}(t_1 + 0) = [(\mathcal{S}(0) - 1)e^{-\varepsilon t_1} + 1](1 - b_1) = \mathcal{S}(0)e^{-\varepsilon t_1}(1 - b_1) + \alpha_1,$$

where $0 < \alpha_1 < 1 - e^{-\varepsilon t_1}$.

Next, we calculate $\mathcal{S}(t_2 + 0)$, $\mathcal{S}(t_3 + 0)$, etc. At the p-th step, we obtain

$$\mathcal{S}(t_p + 0) = \mathcal{S}(0)e^{-\varepsilon t_p}\prod_{i=1}^{p}(1 - b_i) + \alpha_p,$$

where $0 < \alpha_p < 1 - e^{-\varepsilon t_p}$.

Therefore

$$\mathcal{S}(T) = \mathcal{S}(0)e^{-\varepsilon T}\prod_{i=1}^{p}(1 - b_i) + (\alpha_p - 1)e^{-\varepsilon(T-t_p)} + 1.$$

Then the initial data for the T-periodic solution $\bar{\mathcal{S}}(t)$ is determined in the following way:

$$\mathcal{S}(0) = \frac{(\alpha_p - 1)e^{-\varepsilon(T-t_p)} + 1}{1 - e^{-\varepsilon T}\prod_{i=1}^{p}(1 - b_i)}. \tag{8}$$

At the same time, from (8)

$$\mathcal{S}(0) < \frac{1 - e^{-\varepsilon T}}{1 - e^{-\varepsilon T}\prod_{i=1}^{p}(1 - b_i)},$$

 doi:10.20944/preprints202602.1283.v1

which means that $\mathcal{S}(0) \to 0$ when $T \to 0$. Then from (7) we deduce that $\forall \varepsilon > 0 \ \exists T^* > 0$ $\forall T \in (0, T^*)$

$$\bar{\mathcal{S}}(t) < \varepsilon$$

for $\forall t \geq 0$.

Hence we have (6). □

Corollary 1. *In problem (7), the T-periodic solution $\bar{\mathcal{S}}(t)$ is asymptotically stable; that is, for any $\mathcal{S}(0) \in (0,1)$, the corresponding solution $\mathcal{S}(t)$ of problem (7) satisfies:*

$$\mathcal{S}(t) - \bar{\mathcal{S}}(t) \to 0, \qquad t \to \infty. \tag{9}$$

It is easy to see that for $\mathcal{R}_0 > 1$ the equilibrium position $\mathcal{I} = 0$ of the fourth equation of system (3) is unstable. Moreover, for $\forall \mathcal{I}(0) \in (0,1)$, $\forall t > 0$, $\mathcal{I}(t) \in (0,1)$

$$\lim_{t \to \infty} \mathcal{I}(t) = 1 - \frac{1}{\mathcal{R}_0}.$$

Thus, it is fundamentally impossible to achieve asymptotic stability of $\bar{P}(t) = \{\bar{\mathcal{S}}(t), 0, 0, 0\}$ with respect to all coordinates. However, from the standpoint of the original model, this is not required. It is essential to achieve asymptotic stability of the infection-free impulsive solution with respect to the first three coordinates, which correspond to the state of the target node population.

Definition 1. *The solution $\bar{P}(t) = \{\bar{\mathcal{S}}(t), 0, 0, 0\}$ of problems (3), (4) is said to be asymptotically stable with respect to the variables $(\mathcal{S}_t, \mathcal{I}_t, \mathcal{Q}_t)$ if for any $\varepsilon > 0$ there exists $\tau \geq T$ such that*

$$\forall P(0) = \{\mathcal{S}_t(0), \mathcal{I}_t(0), \mathcal{Q}_t(0), \mathcal{I}(0)\} \in int\ \Omega$$

is true

$$\mathcal{S}_t(t) < \bar{\mathcal{S}}(t) + \varepsilon,$$
$$|\mathcal{I}_t(t)| + |\mathcal{Q}_t(t)| < \varepsilon.$$

Theorem 3. *Suppose that in problems (5), (6) the impulsive perturbation satisfies condition (5), and let $\bar{P}(t) = \{\bar{\mathcal{S}}(t), 0, 0, 0\}$ be the corresponding infection-free impulsive periodic solution. Then there exists $T^* > 0$ such that for $T < T^*$, the solution $\bar{P}(t)$ is asymptotically stable with respect to the variables $(\mathcal{S}_t, \mathcal{I}_t, \mathcal{Q}_t)$ in the sense of Definition 1.*

Proof of Theorem 3. For fixed functions $\mathcal{I}(t)$, $\mathcal{I}_t(t)$, and $\mathcal{Q}_t(t)$, consider the impulsive problem associated with the first equation of system (3).

$$\begin{cases} \dot{\mathcal{S}}_t = -\beta \mathcal{S}_t \mathcal{I} + \varepsilon_t (1 - \mathcal{S}_t - \mathcal{I}_t - \mathcal{Q}_t), \\ \Delta \mathcal{S}|_{t=t_n} = -b_n \mathcal{S}(t_n), \end{cases} \tag{10}$$

$$\Delta \mathcal{S}|_{t=0} = \mathcal{S}_t^0 \in (0,1).$$

Since $\mathcal{I}(t) \geq 0$, $\mathcal{I}_t(t) \geq 0$, $\mathcal{Q}_t(t) \geq 0$, then

$$\forall t \geq 0, \mathcal{S}_t(t) \leq \mathcal{S}(t), \tag{11}$$

where $\mathcal{S}(t)$ is the solution to (7), $\mathcal{S}(0) = \mathcal{S}_t^0$, and therefore, according to Corollary 1 of Theorem 2

$$\mathcal{S}(t) - \bar{\mathcal{S}}(t) \to 0, \qquad t \to \infty. \tag{12}$$

Now, with fixed $\mathcal{I}(t)$, $\mathcal{S}_t(t)$, let us consider the second and third equations of system (3)

$$\begin{cases} \dot{\mathcal{I}}_t = \beta \mathcal{S}_t \mathcal{I} - \gamma \mathcal{I}_t, \\ \dot{\mathcal{Q}}_t = \gamma \mathcal{I}_t - \eta \mathcal{Q}_t, \end{cases} \tag{13}$$

$$\mathcal{I}_t(0) = \mathcal{I}_t^0 \in (0,1), \mathcal{Q}_t(0) = \mathcal{Q}_t^0 \in (0,1).$$

Since system (13) is cooperative, then by Kamke's theorem

$$0 \leq \mathcal{I}_t(t) \leq Y(t), 0 \leq \mathcal{Q}_t(t) \leq Z(t),$$

where $\{Y(t), Z(t)\}$ is the solution of the system

 doi:10.20944/preprints202602.1283.v1

$$\begin{cases} \dot{Y} = \beta \mathcal{S}(t) Z - \gamma Y, \\ \dot{Z} = \gamma Y - \eta Z, \end{cases} \tag{14}$$
$$Y(0) = \mathcal{I}_t^0, Z(0) = \mathcal{Q}_t^0.$$

where $\mathcal{S}(t)$ satisfies (12).

Then for sufficiently large t

$$\begin{aligned} &\frac{d}{dt}\big(2Y(t) + Z(t)\big) = 2\beta \mathcal{S}(t) Z - \gamma Y - \eta Z = \\ &= -\frac{\gamma}{2} \cdot 2Y - \big(\eta - 2\beta \mathcal{S}(t)\big) Z \le \lambda(2Y + Z), \end{aligned} \tag{15}$$

where $\lambda = \min\left\{\frac{\gamma}{2}, \frac{\varepsilon}{2}\right\}$, if T^* is chosen so that for $T < T^*$

$$\sup_{t \ge 0} \bar{\mathcal{S}}(t) < \frac{\varepsilon}{4\beta}. \tag{16}$$

Thus, $\forall t \ge 0$

$$\mathcal{I}_t(t) + \mathcal{Q}_t(t) \le K \cdot \big(\mathcal{I}_t(0) + \mathcal{Q}_t(0)\big) e^{-\lambda t}, \tag{17}$$

where $K > 0$ is some constant.

Then from (11), (12), (17) we have the desired result. □

4. Discussion

It should be noted that estimate (17) formalizes the requirement of functional resilience of an information system subjected to aggressive adversarial interference. Even for $\mathcal{R}_0 > 1$ (which corresponds to a natural tendency toward avalanche-like growth of a botnet), properly organized periodic impulses (updates, blocking, and segmentation) ensure *exponential reduction* of the active component of the attack within the target population (Figure 2).

The left-hand side of inequality (17), $\mathcal{I}_t(t) + \mathcal{Q}_t(t)$, describes the total "*active threat*" to the target network, comprising active bots I_t and isolated but not yet recovered nodes Q_t. The factor $e^{-\lambda t}$ guarantees that, under appropriately selected impulsive control (mass updates or node isolation applied with period $T < T^*$), the active threat decays at an exponential rate.

The parameter $\lambda = \min\left\{\frac{\gamma}{2}, \frac{\varepsilon}{2}\right\}$ reflects the "*bottleneck*" in the defense mechanism:

- If γ is small, the network is characterized by slow isolation processes (IDS/IPS/IDPS and SOC respond sluggishly);
- If ε is small, rapid loss of immunity is observed (outdated patches, policies, etc.).

The constant K aggregates the initial conditions and the comparison inequalities (Kamke conditions); in practical terms, it represents the model's safety margin.

In Figure 2, the red dashed line depicts the "teeth," corresponding to the moments of impulsive intervention t_n, when software updates or isolation measures lead to an abrupt reduction in the number of infected nodes. The pink dashed line visualizes estimate (17). It demonstrates that, provided the impulse frequency is sufficiently high ($T < T^*$), the attack is guaranteed to decay, regardless of any attempts by adversaries to propagate it. Overall, Figure 2 shows that over time the system converges to an infection-free state (the values tend toward zero), which constitutes the objective of protection.

 doi:10.20944/preprints202602.1283.v1

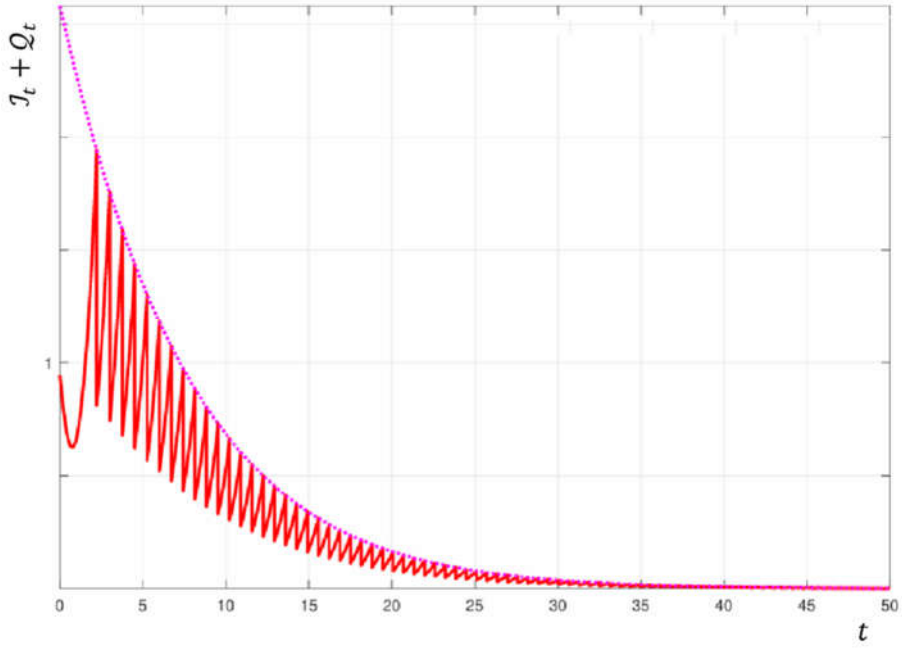

Figure 2. Visualization of the infection free behavior of the pulsed periodic solution of (5), (6).

In this way, estimate (17) provides a quantitative guarantee of exponential suppression of the active phase of a DDoS attack in the target network under properly configured impulsive control, which directly corresponds to the engineering requirements for the resilience of critical infrastructure services. Moreover, estimate (17) establishes a necessary condition for ensuring the functional resilience of a critical infrastructure information system and for designing multi-layered defense systems for it.

5. Conclusions

This paper proposes an impulsive SIRQ model that generalizes classical epidemic approaches to the analysis of cyberattacks and consistently integrates the continuous dynamics of malware propagation in a network with discrete control actions representing mass updates, node isolation, and the enforcement of access policies. Such an approach provides an adequate mathematical description of real-world response mechanisms to large-scale viral and DDoS attacks.

The fundamental role of the basic reproduction number $\mathcal{R}_0$ is established as a threshold parameter determining the attack dynamics: for $\mathcal{R}_0 \leq 1$, the infection-free equilibrium is globally asymptotically stable, whereas for $\mathcal{R}_0 > 1$ the system admits an endemic regime with a nonzero fraction of infected nodes.

It is shown that the application of periodic impulsive control actions enables stabilization of the infection-free regime with respect to the target population even when the threshold value $\mathcal{R}_0$ is exceeded. Such stabilization constitutes a practically sufficient condition for ensuring the availability of critical services and maintaining the functional resilience of network infrastructure under large-scale attacks.

The derived estimate (17) establishes exponential decay of the total active threat $\mathcal{I}_t + \mathcal{Q}_t$ with rate λ, which admits a clear applied interpretation in terms of the isolation rate of infected nodes and the level of immunity retention in recovered systems. This estimate provides a quantitative guarantee of the effectiveness of impulsive cyber defense strategies.

The proposed model forms a theoretical foundation for the design of adaptive cybersecurity systems, the determination of optimal frequency and intensity of preventive impulses, the forecasting of the consequences of large-scale DDoS campaigns, and the development of multi-layered defense strategies for critical information infrastructure.

 doi:10.20944/preprints202602.1283.v1

Author Contributions: Conceptualization, and methodology, V.Sob.; formal analysis, and writing—original draft preparation, V.Sav.; software, validation, and data curation, B.S.; supervision, and writing—review and editing, H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was carried out under partial sub-grant of the Research Project No. 24BF038-01 «Asymptotic behavior, stability and controllability in infinite-dimensional evolutionary systems with deterministic and random perturbations».

Informed Consent Statement: Not applicable.

Data Availability Statement: The research reported in this article did not involve the use of any data.

Conflicts of Interest: The authors state that they have no financial or personal relationships that could have inappropriately affected or influenced the content of this article.

Abbreviations

The following abbreviations are used in this manuscript:

DDoS	Distributed Denial-of-Service
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
SIR	Susceptible (S), Infective (I), and Recovered (R)
SIRQ	Susceptible (S), Infective (I), Recovered (R) and Quarantined (Q)
SOC	Security Operations Center
VLAN	Virtual Local Area Network

References

1. Mishra, B.K., Keshri, A.K., Mallick, D.K., Mishra, B.K. A mathematical model on DDoS attack in IoT network. *Nonlinear Eng.* **2019**, *8*(*1*), 486–495. https://doi.org/10.1515/nleng-2017-0094
2. Sobchuk, V., Pykhnivskyi, R., Barabash, O. Sequential IDS for Zero-Trust Cyber Defence of IoT/IIoT Networks. *Adv. Inf. Syst.* **2024**, *8*(*3*), 92–99. https://doi.org/10.20998/2522-9052.2024.3.11
3. Balarezo, J.F., Wang, S., Chavez, K.G., Al-Hourani, A., Kandeepan, S. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Eng. Sci. Technol. Int. J.* **2022**, *31*, 101065. https://doi.org/10.1016/j.jestch.2021.09.011
4. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. et. al. *Models of socio-cyber-physical systems security*. Kharkiv: PC Technology Center, Ukraine, **2023**, 184. http://doi.org/10.15587/978-617-7319-72-5
5. Kyrychok, R., Laptiev, O., Lisnevsky, R., Kozlovsky, V., Klobukov, V. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. *East.-Eur. J. Enterp. Technol.* **2022**, *1*(*9*(*115*)), 93–101. https://doi.org/10.15587/1729-4061.2022.253530
6. Savchenko, V.A., Stepanchenko, B.S. Development of the concept of predicting the time of the onset of a DDoS attack based on the study of the dynamics of the behavior of evolutionary equations. *Telecommun. Inf. Technol.* **2024**, *1*(*82*). 26–44. https://doi.org/10.31673/2412-4338.2024.012644
7. Rodriguez, H.S. Application of SIR Epidemiological Model: New Trends. *Int. J. Appl. Math. and Inf.* **2016**, *10*, 76–82. https://doi.org/10.48550/arXiv.1611.02565
8. Hethcote, H.W. Three Basic Epidemiological Models. In *Applied Mathematical Ecology. Biomathematics*; Levin, S.A., Hallam, T.G., Gross, L.J., Eds.; Springer, Berlin, Heidelberg, 1989, 18. https://doi.org/10.1007/978-3-642-61317-3_5
9. Rao, Y.S., Kesri, A.K., Mishra, B.K., Panda, Z.C. Distributed denial of service attack on target resources in a computer network for critical infrastructure: a differential-equation model. *Phys. Stat. Mech. Appl.* **2020**, *540*(*4*), 123240. https://doi.org/10.1016/j.physa.2019.123240

 doi:10.20944/preprints202602.1283.v1

10. Samoilenko, A.M., Perestyuk, N.A. Impulsive Differential Equations. In *World Scientific Series on Nonlinear Science Series A*, World Scientific: Singapore, 1995, 14; 472 p. https://doi.org/10.1142/2892
11. Pichkur, V., Sobchuk, V., Cherniy, D, Ryzhov, A. Functional Stability of Production Processes as Control Problem of Discrete Systems with Change of State Vector Dimension. *Bull. Taras Shevchenko Natl. Univ. Kyiv. Phys. Math. Sci.* **2024**, *1*(*78*), 105–110. https://doi.org/10.17721/1812-5409.2024/1
12. Barabash, O., Sobchuk, V., Sobchuk, A., Musienko, A., Laptiev, O. Algorithms for Synthesis of Functionally Stable Wireless Sensor Network. *Adv. Inf. Syst.* **2025**, *9*(*1*), 70–79. https://doi.org/10.20998/2522-9052.2025.1.08
13. Nosenko, T.V., Stanzhyts'kyi, O.M. Averaging method in some problems of optimal control. *Nonlinear Oscill* **2008**, 11, 539–547. https://doi.org/10.1007/s11072-009-0049-5
14. Lavrova, O., Mogylova, V., Stanzhytskyi, O., Misiats, O. Approximation of the Optimal Control Problem on an Interval with a Family of Optimization Problems on Time Scales. *Nonlinear Dyn. Syst. Theory* **2017**, *17*(*3*), 303–314.
15. Zhuk, T., Kasimova, N., Ryzhov, A. Application of the Averaging Method to the Optimal Control Problem of Non-Linear Differential Inclusions on the Finite Interval. *Axioms* **2022**, *11*, 653. https://doi.org/10.3390/axioms11110653
16. Kasimova, N., Zhuk, T., Tsyganivska, I. Approximate solution of the optimal control problem for non-linear differential inclusion on the semi-axes. *Georgian Math. J.* **2023**, *30*(*6*), 883–889. https://doi.org/10.1515/gmj-2023-2054