2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Analysis of Contagion Dynamics with Active Cyber Defenders

Keith Paarporn, Philip N. Brown, Shouhuai Xu

Abstract— **In this paper, we analyze the infection spreading dynamics of malware in a population of cyber nodes (i.e., computers or devices). Unlike most prior studies where nodes are reactive to infections, in our setting some nodes are *active defenders* meaning that they are able to clean up malware infections of their neighboring nodes, much like how spreading malware exploits network connectivity properties in order to propagate. We formulate these dynamics as an Active Susceptible-Infected-Susceptible (A-SIS) compartmental model of contagion. We completely characterize the system's asymptotic behavior by establishing conditions for the global asymptotic stability of the infection-free equilibrium and for an endemic equilibrium state. We show that the presence of active defenders counter-acts infectious spreading, effectively increasing the epidemic threshold on parameters for which an endemic state prevails. Leveraging this characterization, we investigate a general class of problems for finding optimal investments in active cyber defense capabilities given limited resources. We show that this class of problems has unique solutions under mild assumptions. We then analyze an Active Susceptible-Infected-Recovered (A-SIR) compartmental model and explicitly derive the peak infection level of any trajectory.**

I. Introduction

The spread of computer malware and viruses remains a major cause for concern, despite the tremendous amount of effort by academia, industry, and government. This is true despite the substantial progress in certain areas of cybersecurity such as cryptography, intrusion detection, firewalls, and anti-malware tools. These traditional cyber defense approaches are *preventive* and *reactive* in nature because they strive to prevent attacks from succeeding and react to recognized attacks [1], [2]. However, it is known that cyber attacks cannot be be completely prevented, for reasons that include undecidability [3] and human factors [4]. Moreover, reactive defenses are limited because there may be substantial delays before attacks are detected and cleaned up.

The limitation of traditional defenses is characterized by an asymmetry that benefits attackers. Namely, the effect of attacks is amplified by the network's connectivity (malware spreading), but the effect of preventive and reactive defenses is not [1], [2], [5]–[7]. This asymmetry has led to an emerging class of countermeasures called *active cyber defenses* [5]–[9], which leverage the same interconnections exploited by attacks to actively identify and clean up compromised nodes. This is achieved by endowing uncompromised nodes the ability to "hunt" compromised nodes to clean up their infection status (or "remotely delivering cures").

This work was supported in part by Colorado State Bill 18-086, NSF Grants #2122631, #2115134, and #2013779, and the Air Force Office of Scientific Research under award number FA9550-23-1-0171. The authors are with the Department of Computer Science at University of Colorado, Colorado Springs. Contact: {kpaarpor,pbrown2,sxu}@uccs.edu

This paper investigates the impact that active defenders have on the spread of malware. The spreading dynamics of malware draws parallels to the spread of an infectious disease in a human population, and as such, basic models in epidemiology are often utilized to study cybersecurity dynamics [2], [10]–[14]. The dynamics of these models often follow an epidemic threshold, such that parameter instances that lie below the threshold exhibit an infection-free equilibrium, and instances above the threshold exhibit an endemic equilibrium, where a constant fraction is infected over long periods of time. In this paper, we formulate cybersecurity dynamics as the A-SIS compartmental model, where nodes are either *susceptible* to, or *infected* by, the malware, and some nodes are *active* defenders.

There have been studies on characterizing the effectiveness of active defenders, mainly from a holistic (i.e., network-oriented) perspective [5]–[7]. A main focus has been on studying their advantage over preventive and reactive cyber defenses [5], and their potential side-effects [7]. These characterization works study mean-field approximations and provide conditions for the existence or absence of equilibria. A prescriptive study has derived optimal control strategies for active cyber defenses in a population contagion model [6], where it is assumed that *every* node in the network has active defense capabilities and no nodes are equipped with reactive defenses. This motivates us to consider more realistic scenarios, where nodes are equipped with reactive defense capabilities and some nodes can be equipped with active defense capabilities. From a practical standpoint in terms of materializing the potential of active defenses in the real world, ongoing work explores competent architectures for implementing active defense approaches [9], and systematizing the challenges that must be tackled before its full potential can be realized [15].

In relation to the literature on epidemics, our work is similar to the dynamics of competitive bi-virus models [16]–[18], though the mathematical equations differ in two respects. First, there are only two compartments (susceptible and infected) in our model of active defenses, whereas bi-virus models must account for three compartments. Second, active cyber defenses have inherent asymmetries, since it is possible that only a fraction of the nodes implement them. In bi-virus models, any node that is infected with a given virus type may spread it.

Contributions: Our study abstracts away the underlying complex network structures originally considered in [5], [7]. Our A-SIS (Active SIS) model is based on a well-mixed population of nodes, where each node has the same rate of

2023 62nd IEEE Conference on Decision and Control (CDC) | 979-8-3503-0124-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CDC49753.2023.10384186

interaction with others. Under these assumptions, our pap provides a full characterization of the dynamical properti of the A-SIS contagion model. We precisely characteri its epidemic threshold, which increases in the fraction a effectiveness of active defenders (Theorem 3.1). We note th this is in contrast to many other studies of epidemic mod with reactive population behaviors, i.e. non-pharmaceutic interventions such as social distancing, where the epidem threshold remains unchanged from classic non-behavio models [19]–[21]. Additionally, we fully characterize t global stability properties of the equilibrium states of t system by identifying suitable Lyapunov functions (Secti III). Specifically, these equilibria are the infection-free equ librium (IFE) and the endemic equilibrium states, where we provide precise infection levels for the latter. Based on these characterizations, we then consider how a designer should optimize system security by investing monetary assets in increasing the fraction of active defense nodes and their effectiveness (Section IV). We show that there is a unique optimal investment profile, given concave return functions.

II. The A-SIS contagion model

Our model of active cyber defense is built upon the classic compartmental SIS model, which we first review below.

A. The SIS Epidemic Model

A malware spreads through a population of nodes, where each node is either susceptible or infected with the malware. We denote $s(t) \in [0,1]$ as the fraction of nodes in the network that are susceptible at time t, and $i(t) \in [0,1]$ as the fraction that are infected. The malware can only be transmitted from an infected node to a susceptible node upon contact. The per-contact infection rate is $\beta > 0$. Infected nodes are able to independently recover at the rate $\alpha > 0$ by using reactive defenses, e.g. by using recovery software, intrusion-detection system, or anti-malware tool. The states s and i evolve according to the following dynamical system:

$$\begin{aligned} \frac{ds}{dt} &= -\beta si + \alpha i \\ \frac{di}{dt} &= \beta si - \alpha i \end{aligned} \tag{1}$$

Under these dynamics, the mass of the population is invariant, and we must have $s(t) + i(t) = 1$ for all times t. Therefore, the SIS dynamics may be reduced to a single state variable,

$$\frac{di}{dt} = \beta i(1-i) - \alpha i \tag{2}$$

with initial condition $i(0) \in [0,1]$. The *infection-free equilibrium* (IFE) $i_{\text{IFE}} = 0$ is an equilibrium of the system. The *endemic* equilibrium $i^* = 1 - \frac{\alpha}{\beta} \in (0,1]$ is an equilibrium of the system if and only if $\frac{\beta}{\alpha} > 1$. The solution to this system is well-known. Its asymptotic properties are summarized.

Theorem 2.1 ([22]). *Consider the SIS model* (2).

- *If* $\frac{\beta}{\alpha} \leq 1$, *then* $i(t)$ *converges to* i_{IFE} *for any initial condition* $i(0) \in [0,1]$.

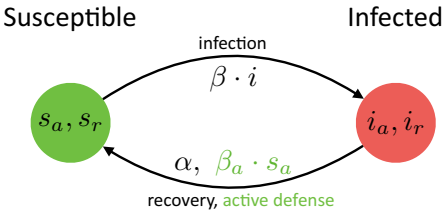

Fig. 1: State transition diagram under active cyber defense dynamics (A-SIS). Each node is one of two types that describe its equipped defense technology. Active nodes (subscript a) have both active and reactive defenses, whereas reactive nodes (subscript r) have only recovery capability. An infected node can transition to susceptible either through traditional recovery, or by interactions with active defenders that are susceptible.

- *If* $\frac{\beta}{\alpha} > 1$, *then* $i(t)$ *converges to the* endemic state $i^* = 1 - \alpha/\beta$ *for any initial condition* $i(0) \in (0,1]$.

From the above result, the dynamics of the SIS model follow a threshold on the parameter $\frac{\beta}{\alpha}$, which is often referred to as the basic reproduction number.

B. A-SIS: Active cyber defense dynamics

We now formulate our dynamical model of active cyber defense. Like in the SIS model, every node comes equipped with recovery software (and thus recovers from infection at rate α). Now, suppose a fixed fraction $x_a \in [0,1]$ of the nodes are *active defenders*. In addition to reactive defenses, they are able to employ active defenses against the spreading malware. Upon contact with any infected node, an active susceptible node is able to clean up the malware at the infected node with rate $\beta_a > 0$. We assume that an active defender can only clean up other infected nodes when it is itself not infected, which is natural. Thus, a susceptible state is required to implement active defenses. The remaining fraction $1 - x_a$ of the nodes are not active defenders. We refer to these nodes as *reactive* nodes.

Let $s_a(t)$, $s_r(t)$, $i_a(t)$, and $i_r(t)$ be the fraction of susceptible active, susceptible reactive, infected active, and infected reactive nodes, respectively. We denote $i(t) \triangleq i_a(t) + i_r(t)$ as the total infected fraction at time t. The dynamics are given by

$$\begin{aligned} \frac{ds_a}{dt} &= -\beta s_a i + \beta_a s_a i_a + \alpha i_a \\ \frac{di_a}{dt} &= \beta s_a i - \beta_a s_a i_a - \alpha i_a \\ \frac{ds_r}{dt} &= -\beta s_r i + \beta_a s_a i_r + \alpha i_r \\ \frac{di_r}{dt} &= \beta s_r i - \beta_a s_a i_r - \alpha i_r. \end{aligned} \tag{3}$$

A state transition diagram is shown in Figure 1. From the above equations, $\frac{ds_a}{dt} + \frac{di_a}{dt} = 0$ and $\frac{ds_r}{dt} + \frac{di_r}{dt} = 0$, and therefore we have $s_a(t) + i_a(t) = x_a$ and $s_r(t) + i_r(t) = 1 - x_a$ for any time $t \geq 0$. The dynamics in (3) is thus a planar system with state $\boldsymbol{i} \triangleq (i_a, i_r) \in [0, x_a] \times [0, 1 - x_a]$

governed by the dynamics

$$\begin{aligned}\frac{di_a}{dt} &= F_a(\boldsymbol{i}) \triangleq \beta(x_a - i_a)i - \beta_a(x_a - i_a)i_a - \alpha i_a \\ \frac{di_r}{dt} &= F_r(\boldsymbol{i}) \triangleq \beta(1 - x_a - i_r)i - \beta_a(x_a - i_a)i_r - \alpha i_r\end{aligned} \tag{A-SIS}$$

We will denote the state space as $\Gamma \triangleq [0, x_a] \times [0, 1 - x_a]$. The initial condition is specified by $\boldsymbol{i}_0 = (i_a(0), i_r(0)) = (i_{a0}, i_{r0}) \in \Gamma$. We seek to characterize the equilibria of system (A-SIS) and their stability properties. We immediately see that the infection-free equilibrium $\boldsymbol{i}_{\text{IFE}} \triangleq (0, 0)$ is an equilibrium point of system (A-SIS). We say an equilibrium $\boldsymbol{i}^*$ is *interior* if $\boldsymbol{i}^* \in (0, x_a) \times (0, 1 - x_a)$. We will study the stability properties of A-SIS in the next section.

III. Stability analysis of A-SIS dynamics

We consider the following stability notions. Let $\mathcal{E} = \{\boldsymbol{i} \in \Gamma : F(\boldsymbol{i}) = (0, 0)\}$ be the set of equilibrium points.

Definition 1. *An equilibrium point $\boldsymbol{i}^* \in \Gamma$ is* globally asymptotically stable (GAS) with respect to Γ *if for all $\boldsymbol{i}_0 \in \Gamma \backslash \mathcal{E}$, $\boldsymbol{i}(t)$ converges to $\boldsymbol{i}^*$.*

Since we are considering the particular system (A-SIS), we will simply say an equilibrium point is globally asymptotically stable (GAS). The stability properties of $\boldsymbol{i}_{\text{IFE}}$ is summarized in our main result below.

Theorem 3.1. *Consider system* (A-SIS)*.*

1) *The equilibrium $\boldsymbol{i}_{IFE}$ is globally asymptotically stable if and only if $\frac{\beta}{\alpha} \leq 1 + \frac{\beta_a x_a}{\alpha}$.*
2) *When $\frac{\beta}{\alpha} > 1 + \frac{\beta_a x_a}{\alpha}$, there exists a unique interior equilibrium $\boldsymbol{i}^* = (x_a \frac{\lambda_+}{\lambda_+ + \alpha}, (1 - x_a)\frac{\lambda_+}{\lambda_+ + \alpha})$ that is globally asymptotically stable, where*

$$\lambda_+ \triangleq \beta - \beta_a x_a - \alpha. \tag{4}$$

Here, $\boldsymbol{i}^*$ is referred to as the endemic equilibrium.

Note that Theorem 3.1 degenerates to Theorem 2.1 by setting $x_a = 0$, meaning that all nodes only have reactive defenses. The presence of active defenders increases the threshold for which the IFE is GAS in comparison to the condition in Theorem 2.1.

A. Global asymptotic stability of the IFE

Before establishing the GES result of $\boldsymbol{i}_{\text{IFE}}$, we first establish GAS of $\boldsymbol{i}_{\text{IFE}}$ in this subsection. The Jacobian is

$$J(\boldsymbol{i}) = \begin{bmatrix} \frac{\partial F_a}{\partial i_a} & \frac{\partial F_a}{\partial i_r} \\ \frac{\partial F_r}{\partial i_a} & \frac{\partial F_r}{\partial i_r} \end{bmatrix} \tag{5}$$

where

$$\begin{aligned}\frac{\partial F_a}{\partial i_a} &= (\beta - \beta_a)(x_a - 2i_a) - \beta i_r - \alpha \\ \frac{\partial F_a}{\partial i_r} &= \beta(x_a - i_a) \\ \frac{\partial F_r}{\partial i_a} &= \beta_a i_r + \beta(1 - x_a - i_r) \\ \frac{\partial F_r}{\partial i_r} &= \beta(1 - x_a - 2i_r - i_a) - \beta_a(x_a - i_a) - \alpha\end{aligned} \tag{6}$$

Evaluated at $\boldsymbol{i}_{\text{IFE}}$, we have

$$J(\boldsymbol{i}_{\text{IFE}}) = \begin{bmatrix} (\beta - \beta_a)x_a - \alpha & \beta x_a \\ \beta(1 - x_a) & \beta(1 - x_a) - \beta_a x_a - \alpha \end{bmatrix} \tag{7}$$

The eigenvalues are given by

$$\lambda_+ \triangleq \beta - \beta_a x_a - \alpha, \quad \lambda_- \triangleq -(\beta_a x_a + \alpha). \tag{8}$$

Since $\lambda_- < 0$, it is required that $\lambda_+ < 0$ for the IFE to be locally stable. This is the case under the condition

$$x_a > \frac{\beta - \alpha}{\beta_a}. \tag{9}$$

If $x_a < \frac{\beta - \alpha}{\beta_a}$, then the IFE is unstable.

Now, let us consider the two nullclines of system (A-SIS),

$$\begin{aligned}\mathcal{I}_a &\triangleq \{\boldsymbol{i} \in \Gamma : F_a(\boldsymbol{i}) = 0\} \\ &= \left\{\boldsymbol{i} \in \Gamma : \left(\frac{\alpha}{\beta(x_a - i_a)} - \left(1 - \frac{\beta_a}{\beta}\right)\right) i_a = i_r \right\} \\ \mathcal{I}_r &\triangleq \{\boldsymbol{i} \in \Gamma : F_r(\boldsymbol{i}) = 0\} \\ &= \left\{\boldsymbol{i} \in \Gamma : i_a = \left(\frac{\alpha - \beta(1 - x_a - i_r) + \beta_a x_a}{\beta(1 - x_a - i_r) + \beta_a i_r}\right) i_r \right\}.\end{aligned} \tag{10}$$

The intersection of the nullclines yields the set of equilibrium points. Observe that $\boldsymbol{i}_{\text{IFE}}$ is always an equilibrium. We may define functions

$$\begin{aligned}I_a(i_a) &\triangleq \left(\frac{\alpha}{\beta(x_a - i_a)} - \left(1 - \frac{\beta_a}{\beta}\right)\right) i_a \\ I_r(i_r) &\triangleq \left(\frac{\alpha - \beta(1 - x_a - i_r) + \beta_a x_a}{\beta(1 - x_a - i_r) + \beta_a i_r}\right) i_r\end{aligned} \tag{11}$$

whose graphs $(i_a, I_a(i_a))$ and $(I_r(i_r), i_r)$ are the a- and r-nullclines, respectively. The following convexity properties hold.

Lemma 3.1. *Function $I_a(i_a)$ for $i_a \in [0, x_a)$ is convex and strictly increasing in i_a. Function $I_r(i_r)$ for $i_r \in [0, 1 - x_a)$ is convex in i_r. It is strictly increasing on $i_r \in [0, 1 - x_a)$ if $x_a \geq \frac{\beta - \alpha}{\beta + \beta_a}$, and on $i_r \in [\frac{\beta(1 - x_a) - \beta_a x_a - \alpha}{\beta}, 1 - x_a)$ if $x_a < \frac{\beta - \alpha}{\beta + \beta_a}$.*

Note that $I_a(i_a)$ ($i_a \in [0, x_a]$) and $I_r(i_r)$ ($i_r \in [0, 1 - x_a]$) are functions defined on different domains. It will be more convenient to have them on the same domain, $i_a \in [0, x_a]$. Such a representation for the r-isocline is given below.

Lemma 3.2. *The r-nullcline can explicitly be represented as a function of $i_a \in [0, x_a]$ with*

$$\begin{aligned}&\hat{I}_r(i_a) \triangleq \\ &\frac{1}{2}\left[-\left(\frac{d + i_a(\beta - \beta_a)}{\beta}\right) + \right. \\ &\qquad \left. + \sqrt{\left(\frac{d + i_a(\beta - \beta_a)}{\beta}\right)^2 + 4i_a(1 - x_a)}\right]\end{aligned} \tag{12}$$

where $d \triangleq \alpha + \beta_a x_a - \beta(1 - x_a)$.

The representation $\hat{I}_r(i_a)$ is the inverse function of $I_r(i_r)$. Because $I_r(i_r)$ is convex and strictly increasing with respect

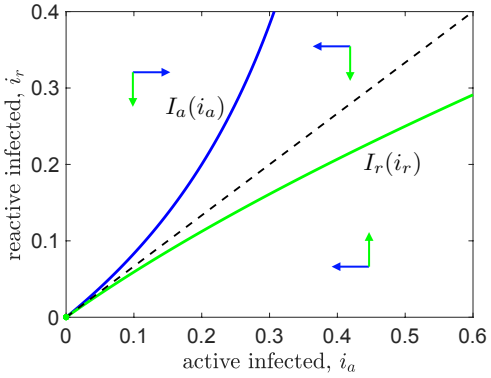

Fig. 2: Nullclines of system (A-SIS). The arrows depict the directions of the flow of system (A-SIS). The dashed line is $i_r = \frac{1-x_a}{x_a} i_a$. Here, we have set $\beta = 0.3$, $x_a = 0.6$.

to i_r, it follows that $\hat{I}_r(i_a)$ is concav in $i_a \in [0, x_a]$. These properties conditions for the existence of a uni

Lemma 3.3. *If $\lambda_+ \leq 0$, then $\boldsymbol{i}_I$ equilibrium in Γ. A unique interior only if $\lambda_+ > 0$.*

The proof is omitted due to spac

Now, let us consider the candidat $\Gamma \to \mathbb{R}_{\geq 0}$ defined by

$$V(\boldsymbol{i}) \triangleq \max \left\{ \frac{1-x_}{x_a} \right.$$

It holds that $V(\boldsymbol{i}) \geq 0$ for all $\boldsymbol{i}$, wit $\boldsymbol{i} = \boldsymbol{i}_{\text{IFE}}$. Observe that when $x_a > \frac{1-x_a}{x_a} i_a$ is a lower bound for $I_a(i_a)$ $\hat{I}_r(i_a)$. Therefore, when $\lambda_+ < 0$, w

$$\frac{dV}{dt} = \mathbb{1}_{\{i_r > \frac{1-x_a}{x_a} i_a\}} F_r(\boldsymbol{i}) + \mathbb{1}_{\{i_r \leq \frac{1-x_a}{x_a} i_a\}} F_a(\boldsymbol{i}) \leq 0 \quad (14)$$

with equality if and only if $\boldsymbol{i} = \boldsymbol{i}_{\text{IFE}}$. Hence, $V(\boldsymbol{i})$ serves as a Lyapunov function that establishes the global asymptotic stability (w.r.t. Γ) of $\boldsymbol{i}_{\text{IFE}}$. This concludes the proof of Theorem 3.1 part 1.

B. Global stability of the endemic equilibrium

The system possesses a unique interior equilibrium when $x_a < \frac{\beta-\alpha}{\beta_a}$ ($\lambda_+ > 0$) (Lemma 3.3), which is given by

$$i_a^* = x_a \cdot \frac{\lambda_+}{\lambda_+ + \alpha}, \quad i_r^* = (1-x_a) \cdot \frac{\lambda_+}{\lambda_+ + \alpha}. \quad (15)$$

We will refer to this interior equilibrium as the *endemic* equilibrium, $\boldsymbol{i}^* = (i_a^*, i_r^*)$. To establish global asymptotic stability (part 2 of Theorem 3.1), we will consider the candidate Lyapunov function $V_R : \Gamma \to \mathbb{R}_{\geq 0}$,

$$V_R(\boldsymbol{i}) \triangleq \max \{ |i_a - x_a f|, R \cdot |i_r - (1-x_a) f| \} \quad (16)$$

for some $R > 0$, where $f \triangleq \frac{\lambda_+}{\lambda_+ + \alpha} \in (0,1)$. We can write it more explicitly as

$$V_R(\boldsymbol{i}) = \begin{cases} x_a f - i_a, & \text{if } \boldsymbol{i} \in \Gamma_a^< \\ i_a - x_a f, & \text{if } \boldsymbol{i} \in \Gamma_a^\geq \\ R((1-x_a)f - i_r), & \text{if } \boldsymbol{i} \in \Gamma_r^< \\ R(i_r - (1-x_a)f), & \text{if } \boldsymbol{i} \in \Gamma_r^\geq \end{cases} \quad (17)$$

where the regions are defined as

$$\begin{aligned} \Gamma_a^< &\triangleq \{\boldsymbol{i} : V_R(\boldsymbol{i}) = |i_a - x_a f|,\ i_a - x_a f < 0\} \\ \Gamma_a^\geq &\triangleq \{\boldsymbol{i} : V_R(\boldsymbol{i}) = |i_a - x_a f|,\ i_a - x_a f \geq 0\} \\ \Gamma_r^< &\triangleq \{\boldsymbol{i} : V_R(\boldsymbol{i}) = R|i_r - (1-x_a)f|, i_r - (1-x_a)f < 0\} \\ \Gamma_r^\geq &\triangleq \{\boldsymbol{i} : V_R(\boldsymbol{i}) = R|i_r - (1-x_a)f|, i_r - (1-x_a)f \geq 0\} \end{aligned} \quad (18)$$

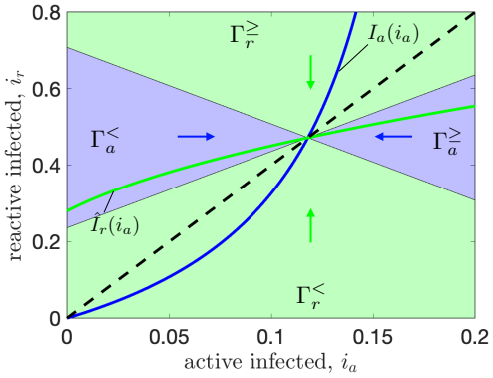

Fig. 3: The regions defined in the Lyapunov function V_R (17). We set $\beta = 0.3$, $\beta_a = 0.28$, $\alpha = 0.1$, $x_a = 0.2$, which is in the regime $x_a \leq \frac{\beta-\alpha}{\beta+\beta_a}$. Here we set $R = 0.5$, which satisfies the condition of (19), $0.25 \leq R < \min\{0.8746, 0.6143\}$.

In the case $x_a \leq \frac{\beta-\alpha}{\beta+\beta_a}$, we will select any R in the range

$$\frac{x_a}{1-x_a} \leq R < \min \left\{ \frac{1}{\hat{I}_r'(i_a^*)}, \frac{\beta x_a f}{d + \beta f (1-x_a)} \right\}. \quad (19)$$

The condition $R < 1/\hat{I}_r'(i_a^*)$ ensures that the graph of $\hat{I}_r$, for $i_a \geq x_a f$, is contained in $\Gamma_a^\geq$. The condition $R < \frac{\beta x_a f}{d + \beta f (1-x_a)}$ ensures that the graph of $\hat{I}_r$, for $i_a < x_a f$, is contained in $\Gamma_a^<$. The condition $\frac{x_a}{1-x_a} \leq R$ ensures that the graph of I_a in Γ is contained only in either $\Gamma_r^<$ (for $i_a < x_a f$) or $\Gamma_r^\geq$ (for $i_a \geq x_a f$). Under (19), the following properties hold:

- Any $\boldsymbol{i} \in \Gamma_a^<$ satisfies $F_a(\boldsymbol{i}) > 0$.
- Any $\boldsymbol{i} \in \Gamma_a^\geq$ satisfies $F_a(\boldsymbol{i}) \leq 0$ with equality if and only if $i_a = x_a f$.
- Any $\boldsymbol{i} \in \Gamma_r^<$ satisfies $F_r(\boldsymbol{i}) > 0$.
- Any $\boldsymbol{i} \in \Gamma_r^\geq$ $F_r(\boldsymbol{i}) \leq 0$ with equality if and only if $i_r = (1-x_a)f$.

We thus obtain

$$\frac{dV_R}{dt}(\boldsymbol{i}) = \begin{cases} -\frac{di_a}{dt}, & \text{if } \boldsymbol{i} \in \Gamma_a^< \\ \frac{di_a}{dt}, & \text{if } \boldsymbol{i} \in \Gamma_a^\geq \\ -R\frac{di_r}{dt}, & \text{if } \boldsymbol{i} \in \Gamma_r^< \\ R\frac{di_r}{dt}, & \text{if } \boldsymbol{i} \in \Gamma_r^\geq \end{cases} \leq 0, \tag{20}$$

with equality if and only if $\boldsymbol{i} = \boldsymbol{i}^*$. Similar arguments can be applied in the case $x_a > \frac{\beta-\alpha}{\beta+\beta_a}$. In this case, the arguments hold for the choice $R = 1$. This establishes global asymptotic stability (w.r.t. Γ) of $\boldsymbol{i}^*$, which concludes the proof of Theorem 3.1 part 2.

IV. Optimal investments in active defense

We have now fully characterized the global asymptotic behavior of system A-SIS. It may be summarized by the limiting infected fraction

$$L(x_a, \beta_a) \triangleq \lim_{t\to\infty} i(t) = \begin{cases} 1 - \frac{\alpha}{\beta - \beta_a x_a}, & \text{if } \beta_a x_a < \beta - \alpha \\ 0, & \text{else} \end{cases}. \tag{21}$$

In this section, we consider a system operator that makes investment decisions to promote the active defense capabilities of the network. Suppose the operator has a limited monetary budget $M > 0$. It decides to invest an amount of money $a \geq 0$ in increasing the total fraction x_a of active defenders, with a return function $h : \mathbb{R}_{\geq 0} \to [0, 1]$ that is increasing. This reflects a plausible scenario since active defenses are new tools and capabilities which would incur extra costs to install on network nodes. Likewise, it decides to invest an amount $b \geq 0$ in increasing the effectiveness of active defenders, with an expected return function $g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$. This reflects the costs associated with improving active defense tactics, where more advanced tactics incur higher costs (e.g., requiring the active defender to collect and process more data from its neighboring node it is trying to help out). The optimization problem that the operator faces is thus formulated as

$$\begin{aligned} \min_{y=(a,b)} \; & L(h(a), g(b)) \\ \text{s.t. } & a, b \geq 0 \\ & a + b \leq M \end{aligned} \tag{22}$$

This problem becomes trivial if there is a feasible pair (a, b) that satisfies $g(b)h(a) \geq \beta - \alpha$. In this case, the infection can be eradicated. As such, we will consider the cases where no feasible pair achieves this, i.e. $g(b)h(a) < \beta - \alpha$ for all a, b with $a + b \leq M$.

We will proceed by defining the following structural properties for the return functions.

Definition 2. *We denote the family of functions $\mathcal{D}$ as the set of single-variable functions $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ that are strictly increasing, twice continuously differentiable, concave, and satisfies $f(0) = 0$.*

For the formulation of optimization problem (22), we place the following assumptions on the return functions h, g.

Assumption 1. *The function $g \in \mathcal{D}$. The function $h(a)$ is of the form $h(a) = \min\{\hat{h}(a), 1\}$, where $\hat{h} \in \mathcal{D}$.*

Concavity is a common assumption that describes marginal diminishing returns on investment. For the function $h(a)$, there is a value $t > 0$ for which monetary investments larger than t will convert the entire population to become active defenders. It can be the case that $t = \infty$, in which case $h \in \mathcal{D}$. The assumption $h(0) = g(0) = 0$ asserts that zero investment yields zero returns. The following result establishes that there exists a unique optimal investment that solves (22).

Theorem 4.1. *Suppose g, h satisfy the properties of Assumption 1. Suppose $t \geq M$. Then* (22) *has a unique solution $y^* = (a^*, b^*)$, where $a^* \in (0, M)$ satisfies*

$$g(M - a^*)h'(a^*) = g'(M - a^*)h(a^*) \tag{23}$$

and $b^* = M - a^*$. Suppose $t < M$. If $g'(M - t) \geq g(M - t)\hat{h}'(t)$, then the unique solution is given by the same y^*. If $g'(M - t) < g(M - t)\hat{h}'(t)$, then the unique solution is given by $a^* = t$, $b^* = M - t$.

The proof follows from analyzing the KKT conditions of the associated optimization problem (22), and is omitted for space considerations. Below, we apply the result to examples of return functions.

Example 1. *For linear returns on investment, $h(a) = \min\{c_1 a, 1\}$ and $g(b) = c_2 b$ for constants $c_1, c_2 > 0$. From Theorem 4.1, if $1/c_1 > M$, we have $a^* = b^* = M/2$. If $M/2 \leq 1/c_1 < M$, we also obtain $a^* = b^* = M/2$. If $1/c_1 < M/2$, then $a^* = 1/c_1$ and $b^* = M - 1/c_1$.*

Example 2. *Suppose $h(a) = \frac{a}{a+c_1}$ and $g(b) = \bar{\beta}\frac{b}{b+c_2}$ for constants $c_1, c_2, \bar{\beta} > 0$. From* (23)*, we obtain $a^* = \frac{c_1(M+c_2)}{c_1-c_2}\left[1 - \sqrt{1 - \frac{(c_1-c_2)M}{c_1(M+c_2)}}\right] < M$ if $c_1 \neq c_2$, and $a^* = M/2$ if $c_1 = c_2$.*

V. A-SIR dynamics of active cyber defense

In this section, we investigate the impact of active defenders in the SIR (susceptible-infected-recovered) epidemics model. Here, a node that has been cleared of infectious malware obtains permanent protection against any future infection. The protection can be conferred either through reactive defenses (with rate α), or through active defenses (with rate β_a). As such, we keep track of the five states $s_a(t)$, $s_r(t)$, $i_a(t)$, $i_r(t)$, and $r(t)$. The dynamics are given as

$$\begin{aligned} \frac{ds_a}{dt} &= -\beta \cdot s_a i, \quad \frac{ds_r}{dt} = -\beta \cdot s_r i \\ \frac{di_a}{dt} &= \underbrace{\beta \cdot s_a i}_{\text{malware infection}} - \underbrace{\beta_a \cdot s_a i_a}_{\text{active defense}} - \underbrace{\alpha i_a}_{\text{reactive defense}} \\ \frac{di_r}{dt} &= \beta \cdot s_r i - \beta_a \cdot s_a i_r - \alpha i_r \\ \frac{dr}{dt} &= \beta_a \cdot s_a i + \alpha i \end{aligned} \tag{A-SIR}$$

with initial conditions $(s_{a0}, s_{r0}, i_{a0}, i_{r0}) \in [0,1]^4$ that satisfy $s_{a0} + s_{r0} + i_{a0} + i_{r0} = 1$. Here, we are assuming that no node is initially fully protected from the malware, meaning $r(0) = 0$. We consider the class of initial value problems with the above dynamics (A-SIR) parameterized by a fixed fraction of initially infected nodes i_0 and the fraction of active defenders in the population, namely s_{a0}. Observe that the roles of infected active or infected reactive nodes are indistinguishable (both types infect susceptibles at the same rate, and both attain protection at the same rates). Indeed, the total infected fraction i depends only on i, but not on (i_a, i_r):

$$\frac{di}{dt} = \beta \cdot si - \beta_a \cdot s_a i - \alpha i. \tag{24}$$

Therefore, we only consider the initial fraction of active susceptible nodes, namely s_{a0}. The following Theorem characterizes the peak infection level for any initial value problem of the A-SIP dynamics.

Theorem 5.1. *Consider any initial value problem of the A-SIP dynamics, and denote by $i(t)$, $t \geq 0$ the resulting state trajectory for the total infected fraction of nodes. Then $i_{pk} \triangleq \max_{t\geq 0} i(t)$ is characterized by*

$$i_{pk} = \begin{cases} 1 - \frac{\alpha}{\beta} - \frac{\beta_a}{\beta} s_{a0} + \frac{\alpha}{\beta} \log \frac{\alpha}{\beta s_0 - \beta_a s_{a0}}, & \text{if } s_{a0} < \frac{\beta s_0 - \alpha}{\beta_a} \\ i_0, & \text{if } s_{a0} \geq \frac{\beta s_0 - \alpha}{\beta_a} \end{cases}. \tag{25}$$

The above result indicates that the infection level will not exceed i_{pk} for any time $t \geq 0$. Thus, if the objective of a system operator is to ensure the network never reaches an infectivity level above a certain desired threshold τ, then equation (25) can help specify design parameters (e.g. β_a, s_{a0}, α) on defense that meet this requirement.

VI. Conclusion

Active cyber defense is an emerging technology. We have proposed a novel active cyber defense model based on the epidemiological SIS population dynamics. We fully characterized the behavior of the dynamics, establishing global asymptotic stability of infection-free and endemic fixed points. We show that deploying active cyber defenses has an impact on the epidemic threshold, unlike other mitigation approaches studied in epidemic models such as reactive social distancing. We further leverage the characterization to determine optimal investments in active cyber defense. As a side-product, we also characterize the effect of deploying active cyber defense in an SIR model. We hope this study will inspire more investigations on the effectiveness of active cyber defense, which is a new paradigm in cyber defense that could be a game-changer in cybersecurity.

References

[1] S. Xu, W. Lu, L. Xu, and Z. Zhan, "Adaptive epidemic dynamics in networks: Thresholds and control," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 8, no. 4, pp. 1–19, 2014.

[2] R. Zheng, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics is globally stable," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 2, pp. 156–170, 2017.

[3] L. M. Adleman, "An abstract theory of computer viruses," in *Advances in Cryptology—CRYPTO'88: Proceedings 8*. Springer, 1990, pp. 354–374.

[4] R. Montañez, E. Golob, and S. Xu, "Human cognition through the lens of social engineering cyberattacks," *Frontiers in psychology*, vol. 11, p. 1755, 2020.

[5] S. Xu, W. Lu, and H. Li, "A stochastic model of active cyber defense dynamics," *Internet Mathematics*, vol. 11, no. 1, pp. 23–61, 2015.

[6] W. Lu, S. Xu, and X. Yi, "Optimizing active cyber defense," in *Decision and Game Theory for Security: 4th International Conference, GameSec 2013, Fort Worth, TX, USA, November 11-12, 2013. Proceedings 4*. Springer, 2013, pp. 206–225.

[7] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, 2015, pp. 1–12.

[8] P. Théron and A. Kott, "When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–7.

[9] P. Theron, A. Kott, M. Drašar, K. Rzadca, B. LeBlanc, M. Pihelgas, L. Mancini, and F. De Gaspari, "Reference architecture of an autonomous agent for cyber defense of complex military systems," *Adaptive Autonomous Secure Cyber Systems*, pp. 1–21, 2020.

[10] A. Ganesh, L. Massoulié, and D. Towsley, "The effect of network topology on the spread of epidemics," in *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2. IEEE, 2005, pp. 1455–1466.

[11] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Transactions On Networking*, vol. 17, no. 1, pp. 1–14, 2008.

[12] Y. Han, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics with ergodic time-dependent parameters is globally attractive," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2517–2532, 2021.

[13] V. S. Varma, Y. Hayel, and I.-C. Morărescu, "A non-cooperative resource utilization game between two competing malware," *IEEE Control Systems Letters*, vol. 7, pp. 67–72, 2022.

[14] V. S. Mai, R. J. La, and A. Battou, "Optimal cybersecurity investments using sis model: Weakly connected networks," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 6097–6102.

[15] S. Xu, "Aica development challenges," in *Building an Artificial Intelligence Cyber-Defense Agent*, A. Kott, Ed. Springer, 2022, vol. 74, pp. 1–31.

[16] J. Liu, P. E. Paré, A. Nedić, C. Y. Tang, C. L. Beck, and T. Başar, "Analysis and control of a continuous-time bi-virus model," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4891–4906, 2019.

[17] A. Santos, J. M. Moura, and J. M. Xavier, "Bi-virus sis epidemics over networks: Qualitative analysis," *IEEE Transactions on Network Science and Engineering*, vol. 2, no. 1, pp. 17–29, 2015.

[18] V. Doshi, J. Hu, and D. Y. Eun, "Bi-sis epidemics on graphs - quantitative analysis of coexistence equilibria," in *2022 IEEE 61st Conference on Decision and Control (CDC)*, 2022, pp. 5608–5613.

[19] K. Paarporn, C. Eksin, J. S. Weitz, and J. S. Shamma, "Networked sis epidemics with awareness," *IEEE Transactions on Computational Social Systems*, vol. 4, no. 3, pp. 93–103, 2017.

[20] C. Eksin, K. Paarporn, and J. S. Weitz, "Systematic biases in disease forecasting–the role of behavior change," *Epidemics*, vol. 27, pp. 96–105, 2019.

[21] T. C. Reluga, "Game theory of social distancing in response to an epidemic," *PLoS computational biology*, vol. 6, no. 5, p. e1000793, 2010.

[22] W. Mei, S. Mohagheghi, S. Zampieri, and F. Bullo, "On the dynamics of deterministic epidemic propagation over networks," *Annual Reviews in Control*, vol. 44, pp. 116–128, 2017.