Unified Preventive and Reactive Cyber Defense Dynamics Is Still Globally Convergent

Zongzong Lin, Wenlian Lu, *Senior Member, IEEE*, and Shouhuai Xu

***Abstract*— A class of the preventive and reactive cyber defense dynamics has recently been proven to be *globally convergent*, meaning that the dynamics *always* converges to a unique equilibrium whose location only depends on the values of the model parameters (but not the initial state of the dynamics). In this paper, we unify the aforementioned class of preventive and reactive cyber defense dynamics models and the closely related class of N-intertwined epidemic models into a single framework. We prove that the unified dynamics is still globally convergent under some mild conditions, which are naturally satisfied by the two specific classes of dynamics models mentioned above and are inevitable when analyzing a more general framework. We also characterize the convergence speed of the unified dynamics. As a corollary, we obtain that the N-intertwined epidemic model and its extension are globally convergent, together with a *full* characterization on their convergence speed, which is only partially addressed in the literature.**

***Index Terms*— Cybersecurity dynamics, cybersecurity foundation, cyber epidemics, preventive and reactive cyber defense dynamics, global convergence, network science.**

I. Introduction

MANY studies in cybersecurity focus on understanding or designing *building-block* mechanisms and analyzing their properties. For example, security of cryptographic primitives and protocols can now be rigorously proven in the modern cryptography framework, owing to the community effort during the last decades [11]. While necessary, the building-block perspective is not sufficient to understand and characterize cybersecurity because cybersecurity is also about properties of cyber systems when treated as a whole. This matter is important because it has been shown that cybersecurity can exhibit emergent behaviors [47], meaning that some cybersecurity properties cannot be derived from the properties of the underlying building-blocks or sub-systems because a system is more than the sum of its parts.

The situation mentioned above highlights the importance of investigating cybersecurity from a holistic perspective. This importance has inspired research efforts towards modeling, understanding, characterizing, and analyzing cybersecurity by treating the entire cyber system in question as a whole. Along this direction, a particular approach, dubbed *cybersecurity dynamics*, has been proposed and extensively investigated [46], [48]. Intuitively, this approach aims to understand, characterize and control the *evolution* of the global security state of a cyber system in question, where "evolution" is caused by the interaction between attacks and defenses over the course of time. A cybersecurity dynamics model can be used to characterize what will happen when the attacker wages a particular set of attacks and the defender employs a particular set of defenses (e.g., whether or not the global security state converges to a unique equilibrium). These kinds of understanding will pave a way for cyber defenders to orchestrate optimal cyber defense strategies to minimize the damage caused by cyber-attacks in the long run (see, e.g., [27]).

In order to achieve the ultimate goal of the cybersecurity dynamics approach, three major research thrusts have been proposed: *first-principle modeling*, which aims to describe the evolution of the global security state via first principles (i.e., building "as-simple-as-possible models with as-few-as-possible parameters, while making as-weak-as-possible assumptions" [48]); *cybersecurity data analytics*, which aims to validate/invalidate first-principe models and extract the values of parameters used by first-principle models; and *cybersecurity metrics*, which defines cybersecurity metrics and studies their measurements. We refer to [48] for a systematic treatment on the cybersecurity dynamics approach.

The present study falls into the first-principle modeling effort, which is inspired by methodologies in multiple disciplines [46]–[48], including: biological epidemiology [1], [2], [14], [19], [29] and its adaptation to the Internet setting as initiated by [17], [18], [34], [42]; interacting particle systems [26], which investigate the behaviors that can emerge from interacting components; and microfoundation in economics [16], which aims at connecting microeconomic

Manuscript received September 30, 2018; accepted March 31, 2019; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor K. Ren. Date of publication May 29, 2019; date of current version June 14, 2019. The work of W. Lu was supported in part by the Natural Sciences Foundation of China under Grant 61673119, in part by the Key Project of Shanghai Science and Technology under Grant 16JC1420402, in part by the Shanghai Municipal Science and Technology Major Project under Grant 2018SHZDZX01 and ZJLAB, and in part by the Shanghai Committee of Science and Technology under Grant 14DZ1118700. The work of S. Xu was supported in part by ARO under Grant W911NF-17-1-0566 and in part by the NSF under Grant 1814825 and Grant 1736209. *(Corresponding author: Shouhuai Xu.)*

Z. Lin is with the School of Mathematical Science, Fudan University, Shanghai 200433, China, and also with the Department of Computer Science, The University of Texas at San Antonio, San Antonio, TX 78249 USA.

W. Lu is with the School of Mathematical Sciences, Fudan University, Shanghai 200433, China, also with the Shanghai Center for Mathematical Sciences, Fudan University, Shanghai 200433, China, and also with the Shanghai Key Laboratory for Contemporary Applied Mathematics, Shanghai, China.

S. Xu is with the Department of Computer Science, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: shxu@cs.utsa.edu).

This paper has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors. This includes a PDF containing the Appendix.

Digital Object Identifier 10.1109/TNET.2019.2912847

models and macroeconomic models. While inheriting some insights from these inspiring methodologies, first-principle cybersecurity dynamics distinguishes itself from them with a unique set of technical barriers that have yet to be tackled [46], [48].

One of the barriers is to accommodate the rich semantics of cyber-attacks and cyber defenses, components of which may not have counterparts in the other settings mentioned above. This indeed has led to the establishment of families of first-principle cybersecurity dynamics models, which describe different types of cyber-attack-defense interactions, including: (i) preventive and reactive cyber defense dynamics, which accommodates the interaction between push- and pull-based attacks and preventive and reactive defenses (which will be elaborated below) [6], [7], [24], [25], [44], [45], [50], [52], [58]; (ii) adaptive cyber defense dynamics, which accommodates adaptive defenses against cyber-attacks [8], [51]; (iii) proactive cyber defense dynamics, which accommodates proactive cyber defenses (e.g., moving-target defense) against cyber-attacks [13]; and (iv) active cyber defense dynamics, which accommodates active cyber defenses against cyber-attacks [27], [49], [57].

In this paper, we focus on first-principle preventive and reactive cyber defense dynamics [24], [25], [44], [45], [50], [52], [58]. In this type of dynamics, the defender aims at (i) using *preventive* defense mechanisms (e.g., access control, host-based and network-based intrusion prevention) to prevent cyber-attacks from succeeding or causing any damages, and (ii) using *reactive* defense mechanisms (e.g., anti-malware tools, host-based and network-based intrusion detection) to detect successful attacks and clean up the damages. On the other hand, the attacker launches two kinds of cyber-attacks in the threat model: (i) *push-based* attacks, such as malware-like spreading behaviors (i.e., compromised computers actively attempt to attack other computers), and (ii) *pull-based* attacks, such as "drive-by download"-like [36] behaviors (e.g., a malicious webserver attacks browsers when they access it). A first theoretical result about the preventive and reactive cyber defense dynamics is presented in [50], which gives a *sufficient condition* under which the dynamics converges to a unique equilibrium — not necessarily the zero equilibrium (or the "dying out" equilibrium in the terminology of epidemics).

The aforementioned sufficient condition given in [50] corresponds to a specific parameter regime, rather than the entire parameter universe, of the preventive and reactive cyber defense dynamics. This means that the dynamics beyond this specific parameter regime is not understood. This problem is recently resolved in [58], which proves that the preventive and reactive cyber defense dynamics is globally convergent in the *entire* parameter universe (i.e., the dynamics always converges to a unique equilibrium whose location only depends on the values of the model parameters, but not the initial state of the dynamics). It is also shown in [58] that this global-convergence result still holds when the model parameters are node-dependent (meaning the employment of different host-based intrusion prevention and/or detection tools) and/or edge-dependent (meaning the employment of different network-based intrusion prevention and/or detection tools). It is further proven in [58] that the dynamics converges exponentially except for a very special parameter regime, in which the dynamics converges polynomially. For ease of reference, we call the preventive and reactive cyber defense dynamics studied in [50], [58] the "$\prod$-dynamics" or interchangeably the "$\prod$-model" because as we will elaborate later, "$\prod$" is the core component in the mathematical expression for describing the collective effect of multiple compromised nodes (or computers) waging push-based attacks against a vulnerable node.

In parallel to the preventive and reactive cyber defense dynamics model mentioned above, there is a closely related model that is called the N-intertwined epidemic model [39], [41], which is further extended to the so-called ϵ-SIS model [30]. These models have been studied in, for example, [4], [9], [20], [23], [37]. The state-of-the-art regarding these models is summarized in [21], [22], [33] and will be further reviewed in Section II. For ease of reference, we will call these two models the "$\sum$-dynamics" or interchangeably the "$\sum$-model" because "$\sum$" is the core component in their mathematical expression for describing the collective effect of multiple compromised nodes (or computers) waging push-based attacks against a vulnerable node.

Since the aforementioned $\prod$-model and $\sum$-model are closely related to each other, it makes one wonder whether or not they can be unified into a single framework such that properties of these models, which have been studied in the literature, and other models, which may be relevant but have not been studied in the literature, can be investigated altogether. This is important not only because it deepens our understanding (e.g., two different families of models actually can be instantiated from a more general model), but also because the results obtained in the unified model can be immediately applied to any relevant, special-case models. In this paper, we answer this question affirmatively.

Our Contributions: In this paper, we unify the $\prod$-model and the $\sum$-model into a single framework, which is dubbed the *unified dynamics* or interchangeably the *unified model*. As highlighted in Figure 1, our results are summarized as follows:

- Global convergence (Theorem 3): We show that under some *mild conditions* (Properties 1-3), the unified dynamics in the general case of $\alpha \geq 0$ is globally convergent while making no restrictions on the connectivity of the attack-defense graph structure, where "$\alpha \geq 0$" means that some nodes may be vulnerable to pull-based attacks (or self-infection) but the others may be not. It is worth mentioning that the global convergence property is a "nice" property because the fraction of compromised nodes in a network always converges to a unique equilibrium regardless of the initial state (i.e., regardless when the defender starts measuring the global security state) [50], [58].
- Convergence speed (Theorem 4): We characterize the convergence speed of the unified dynamics, which is exponential in most cases and at least polynomial in the other cases. Understanding the convergence speed is important because as demonstrated in [50], faster convergence would make it quicker for the defender to estimate

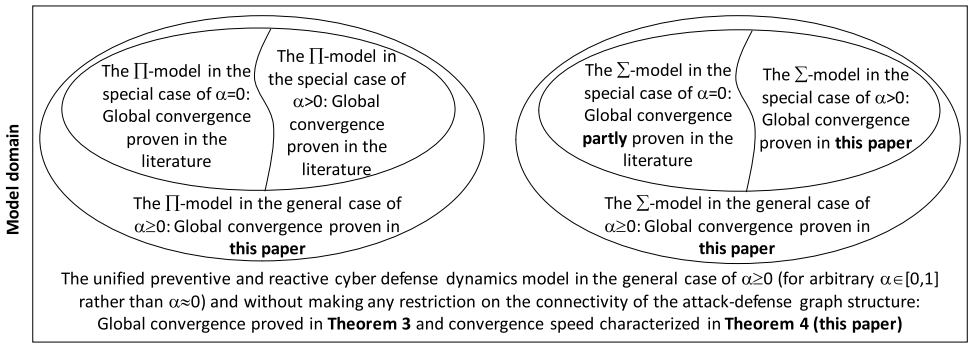

Fig. 1. Overview of our results and their relationship to the literature results, where the "$\prod$-model" refers to the preventive and reactive cyber defense dynamics model [24], [50], [58] and the "$\sum$-model" refers to the N-intertwined model [41] and its extension to accommodate the self-infection probability [30], $\alpha = 0$ means that no nodes are vulnerable to pull-based attacks (analogous to self-infection), $\alpha > 0$ means that all nodes are vulnerable to pull-based attacks, and $\alpha \geq 0$ means some nodes may be vulnerable to pull-based attacks and the others may be not.

the global security state even when the model parameters are not known.

In addition to the contribution that the unified model can accommodate other models than the $\prod$-model and the $\sum$-model, Corollaries 1 and 2 of our main result advance the state-of-the-art as follows.

Given that the aforementioned mild conditions (i.e., Properties 1-3) naturally hold in the $\prod$-model, Corollary 1 supersedes the state-of-the-art understanding of the $\prod$-dynamics as follows. From a global convergence point of view, we now know that the $\prod$-dynamics is globally convergent in the general case of $\alpha \geq 0$. In contrast, the state-of-the-art understanding is that the global convergence holds either in the special case of $\alpha = 0$ (i.e., no nodes are vulnerable to pull-based attacks) or in the special case of $\alpha > 0$ (i.e., all nodes are vulnerable to pull-based attacks) [58]. As shown by Theorem 5, our convergence speed result (Theorem 4) also supersedes the state-of-the-art convergence speed result presented in [58].

Corollary 2 says that the $\sum$-dynamics is globally convergent in the general case of $\alpha \geq 0$ with certain convergence speeds, and thus advances the state-of-the-art understanding about the $\sum$-dynamics in the special case of $\alpha = 0$ (i.e., no nodes are vulnerable to pull-based attacks or self-infection) and $\alpha > 0$ (i.e., all nodes are vulnerable to pull-based attacks or self-infection). More specifically, given that the aforementioned mild conditions (i.e., Properties 1-3) naturally hold in the $\sum$-model, we have the following in regards to the $\sum$-dynamics.

- In the special case of $\alpha = 0$, the state-of-the-art understanding is scattered in a set of publications. The convergence to the zero equilibrium (i.e., spreading dying out) in the parameter regime below the epidemic threshold is studied in [20], [41] and earlier in [9], [23] for the biological setting; the convergence to a non-zero equilibrium in the parameter regime corresponding to the epidemic threshold is studied in [9], [23] for the biological setting; and the convergence to a non-zero equilibrium in the parameter regime above the epidemic threshold is studied in [9], [20], [23]. All of these results are obtained by assuming that the attack-defense graph structure is strongly connected. This strong connectivity assumption is later weakened to the weak connectivity assumption [21], [22]. In contrast, we do not make *any* assumption on the connectivity.
  From a convergence speed point of view, our Theorem 5 shows that our convergence speed result supersedes the state-of-the-art convergence speed result, namely (i) the global exponential convergence to the zero equilibrium in the parameter regime below the epidemic threshold [40], [41] and (ii) the *local* exponential convergence to a non-zero equilibrium in the parameter regime above the epidemic threshold [20]. Note that for the parameter regime above the epidemic threshold, the *local* exponential convergence obtained in [20] is weaker than our *global* exponential convergence result, which holds except for some parameter areas with a Lebesgue measure zero. Note further that for the parameter regime corresponding to the epidemic threshold, we show that the global convergence speed is exponential in some situations and is polynomial in other situations; the convergence speed in this parameter regime is not characterized until now.
- In the special case of $\alpha > 0$, the state-of-the-art understanding is the existence of a steady state in the ϵ-SIS model from a continuous-time Markov Chain point of view [30]. In contrast, we systematically investigate the corresponding dynamical system model, and show that the $\sum$-dynamics in the special case of $\alpha > 0$ is globally convergent and give a characterization on its convergence speed. Note that our Corollary 3 for the $\sum$-model in the special case of $\alpha > 0$ is in parallel to the aforementioned studies [9], [20]–[23], [41] for the $\sum$-model in the special case of $\alpha = 0$.

Paper Organization: The rest of the paper is organized as follows. Section II reviews the $\prod$-model and the $\sum$-model. Section III presents and investigates the unified model. Section IV uses numerical examples to illustrate the generality of our global convergence result and the necessity of some mild condition underlying the global convergence result. Section V discusses the limitations of the present study, which are open problems for future research. Section VI reviews

TABLE I
SUMMARY OF NOTATIONS

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$	The attack-defense structure where $(u, v) \in \mathcal{E}$ means node u can attack node v, where $\mathcal{V} = \{1, \ldots, n\}$
$i_v(t)$, $s_v(t)$	The probability that node v is in the *compromised* and *secure* at time t, where $s_v(t) + i_v(t) = 1$
α_v	The probability that node $v \in \mathcal{V}$ gets compromised because of pull-based attacks or self-infection
$\mathcal{V}_{\alpha=0}$	$\mathcal{V}_{\alpha=0} = \{v : v \in \mathcal{V} \wedge \alpha_v = 0\}$
$\mathcal{V}_{\alpha>0}$	$\mathcal{V}_{\alpha>0} = \{v : v \in \mathcal{V} \wedge \alpha_v > 0\}$
γ_{vu}	The probability that node v gets compromised because of push-based attacks launched from a compromised node u, where $(u, v) \in \mathcal{E}$
β_v	The probability a compromised node v becomes secure
$i(t), s(t)$	$i(t) = [i_1(t), \ldots, i_n(t)]$; $s(t) = [s_1(t), \ldots, s_n(t)]$
$\mathbb{0}, \mathbb{1}$	$\mathbb{0} = [0, \ldots, 0]_n$; $\mathbb{1} = [1, \ldots, 1]_n$
$\mathbb{0}_d$, $\mathbb{1}_d$	$\mathbb{0}_d = [0, \ldots, 0]_d$; $\mathbb{1}_d = [1, \ldots, 1]_d$
$\mathcal{N}_v, N(v)$	$\mathcal{N}_v = \{u : u \in \mathcal{V} \wedge (u, v) \in \mathcal{E}\}$; $N(v) = \lvert\mathcal{N}_v\rvert$
$f_v(\cdot)$	Dynamics function of node v
$h_v(\cdot)$	The probability node v changes from the *compromised* state to the *secure* state
$g_v(\cdot)$	The probability node v changes from the *secure* state to the *compromised* state
$f(\cdot)$, $h(\cdot)$, $g(\cdot)$	Compact form of $f_v(\cdot)$, $h_v(\cdot)$, $g_v(\cdot)$ for $v \in \mathcal{V}$, respectively; e.g., $f(\cdot) = [f_1(\cdot), \ldots, f_n(\cdot)]$
$\overline{h_v}$, $\overline{g_v}$	supremum of $h_v(\cdot)$ and $g_v(\cdot)$, respectively
$\underline{h_v}$, $\underline{g_v}$	infimum of $h_v(\cdot)$ and $g_v(\cdot)$, respectively
$H(\cdot)$	Diagonal matrix $\mathsf{diag}(h_1(\cdot), \ldots, h_n(\cdot))$
$G(\cdot)$	Diagonal matrix $\mathsf{diag}(g_1(\cdot), \ldots, g_n(\cdot))$
C^k	Differentiable function with k-order continuous derivative
$D[\cdot]$	Differential operator: $C^1 \times \mathbb{R}^n \to \mathbb{R}^n$.
$D_i[\cdot]$	Differential operator with respect to variable i.
$s(A)$	The maximum among the real parts of the eigenvalues of matrix A
Γ, B	$\Gamma = [\gamma_{vu}] \in \mathbb{R}^{n\times n}$, $B = \mathsf{diag}(\beta_1, \ldots, \beta_n)$

related prior studies. Section VII concludes the paper. Proof of Theorem 3 is lengthy and thus deferred to the Supplementary Material.

II. PRELIMINARIES

Table I summarizes the major notations that are used throughout the paper.

A. Mathematical Preliminaries

For two n-dimensional vectors $x_1, x_2 \in \mathbb{R}^n$, let $x_1 \geq x_2$ mean that $x_{1,v} \geq x_{2,v}$ for $1 \leq v \leq n$; let $x_1 > x_2$ mean that $x_1 \geq x_2$ and that there exists a v^* such that $x_{1,v^*} > x_{2,v^*}$; and let $x_1 \gg x_2$ mean that $x_{1,v} > x_{2,v}$ for $1 \leq v \leq n$.

A matrix $M = [m_{vu}] \in \mathbb{R}^{n\times n}$ is reducible if there exists a permutation matrix P such that $P^\top M P = \begin{bmatrix} M'_{11} & M'_{12} \\ 0 & M'_{22} \end{bmatrix}$ for any dimension-splitting between M'_{11} and M'_{22}; otherwise, M is irreducible. A matrix $M \in \mathbb{R}^{n\times n}$ is *block-wise irreducible* if M is a block-diagonal matrix with each diagonal-block being irreducible.

We consider an arbitrary graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with a finite node set $\mathcal{V} = \{1, \ldots, n\}$ and without loss of generality, directed edge set $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. Let $A = [a_{vu}] \in \mathbb{R}^{n\times n}$ be the adjacent matrix of $\mathcal{G}$ with weight $a_{vu} = 1$ if and only if $(u, v) \in \mathcal{E}$. Let $\mathcal{N}_v = \{u : (u, v) \in \mathcal{E}\}$ denote the neighborhood nodes belonging to $\mathcal{V}$ and pointing to v (i.e., the "in-neighbors" of v) and $N(v) = \lvert\mathcal{N}_v\rvert$ (i.e., the number of in-neighbors of v).

We consider n-dimensional autonomous dynamical system:

$$\frac{di(t)}{dt} = f(i(t))$$

where $i(t) = [i_1(t), \ldots, i_n(t)]^\top$ with $i_v(t) \in [0, 1]$ for $v = 1, \ldots, n$ (representing the probability that a node v in the *compromised* state at time t), $f(i(t)) = [f_1(i(t)), \ldots, f_n(i(t))]^\top$ with $f_v(i(t)), v = 1, \ldots, n$ being a function of $i(t)$ (representing the probability that a *secure* node becomes *compromised* at time t).

Definition 1 (Cooperative Dynamical System [15]): For a region $\Omega^n \subset \mathbb{R}^n$, let $x = [x_1, \ldots, x_n]^\top \in \Omega^n$ and $\psi(\cdot) = [\psi_1(\cdot), \ldots, \psi_n(\cdot)]^\top : \Omega^n \to \Omega^n$. An autonomous dynamical system $\frac{dx}{dt} = \psi(x)$ is said to be a cooperative *system if $\frac{\partial \psi_v(x)}{\partial x_u} \geq 0$ holds for all $u, v = 1, \ldots, n$ and $u \neq v$.*

Definition 2 (Subhomogeneity [55]): For a region $\Omega^n \subset \mathbb{R}^n$ contains $\mathbb{0} = [0, \ldots, 0]^\top$, a continuous mapping $\zeta(\cdot) : \Omega^n \to \Omega^n$, for any $\delta \in (0, 1)$ and $z \in \Omega^n$ with $z \gg \mathbb{0}$,

- *$\zeta(z)$is said to be* subhomogeneous *if $\zeta(\delta z) \geq \delta\zeta(z)$;*
- *$\zeta(z)$ is said to be* strictly subhomogeneous *if $\zeta(\delta z) > \delta\zeta(z)$;*
- *$\zeta(z)$ is said to be* strongly subhomogeneous *when $\zeta(\delta z) \gg \delta\zeta(z)$;*

Definition 3 (Monotone [55]): For a region $\Omega^n \subset \mathbb{R}^n$, a continuous map $\phi(\cdot) : \Omega^n \to \Omega^n$ is said to be monotone if $x \geq y$ implies that $\phi(x) \geq \phi(y)$.

B. The $\prod$-Model: The Preventive and Reactive Cyber Defense Dynamics Model

This model [24], [50], [58] describes the interaction of push-based attacks and pull-based attacks versus preventive defenses and reactive defenses. As mentioned above, push-based attacks accommodate malware-like attacks, namely that a compromised node or computer actively seeks to attack other nodes or computers; pull-based attacks accommodate "drive-by download"-like attacks (e.g., a malicious webserver attacks vulnerable browsers when they access the webserver); preventive defenses accommodate the defense mechanisms that aim to prevent cyber attacks from succeeding (e.g., host-based and network-based intrusion prevention); and reactive defenses accommodate the defense mechanisms that aim to detect successful attacks and clean up the damages (e.g., anti-malware tools, host-based and network-based intrusion detection).

Formally, push-based attacks take place on what is known as *attack-defense structure*, denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ as mentioned above, where $\mathcal{V} = \{1, 2, \ldots, n\}$ represents a network of n computers, $(u, v) \in \mathcal{E}$ means that a compromised computer u can launch push-based attacks directly against a secure but vulnerable computer v. Without loss of generality, $\mathcal{G}$ can be an arbitrary directed graph. Note that $\mathcal{G}$ is *not* necessarily the underlying physical network, and that $\mathcal{G}$ can be extracted from network security policies (e.g., which computer is allowed to communicate, or is blocked from communicating with, which other computers). This kind of access control policies is widely enforced in the real world (e.g., only authorized people can have access to certain government facilities), and can be

leveraged to mitigate the cyber attack-defense *asymmetry* that befits the attacker (i.e., the consequence of push-based attacks is amplified by a network effect) [49], [57].

In this model, a node $v \in \mathcal{V}$ is in one of two states at any point in time t ($t \geq 0$): *secure*, meaning that the computer is secure (i.e., not compromised) but vulnerable to attacks (denoted by "0"); or *compromised*, meaning that the computer is compromised (denoted by "1"). Let $s_v(t)$ be the probability that node $v \in \mathcal{V}$ is in the *secure* state at time t, and $i_v(t)$ be the probability that node $v \in \mathcal{V}$ is in the *compromised* state at time t. Note that $s_v(t) + i_v(t) = 1$ for any $v \in \mathcal{V}$. The dynamics is described as follows: for $v \in \mathcal{V}$, we have

$$\frac{di_v(t)}{dt} = -\beta_v i_v(t) + \left[1 - (1-\alpha_v) \prod_{u \in \mathcal{N}_v} (1 - \gamma_{vu} i_u(t))\right] \times (1 - i_v(t)) \quad (1)$$

where $\beta_v > 0$ is the probability that a *compromised* node becomes *secure* at any point in time, $\alpha_v \geq 0$ is the probability that a *secure* node v becomes *compromised* because of pull-based attacks, and $0 \leq \gamma_{vu} \leq 1$ is the probability that a *compromised* node u successfully attacks a *secure* node v over $(u, v) \in \mathcal{E}$. Note that $\gamma_{vu} = 0$ for $(u, v) \notin \mathcal{E}$. Note further that the use of $\prod$ in system (1) explains the term of "the $\prod$-model." This dynamics has been characterized as follows:

Theorem 1 [58]: The $\prod$-dynamics or interchangeably the $\prod$-model (1) *is globally convergent when $\alpha_v = 0$ for all $v \in \mathcal{V}$ and when $\alpha_v > 0$ for all $v \in \mathcal{V}$.*

C. The $\sum$-Model: The N-Intertwined Epidemic Model and Its Extension

The N-intertwined epidemic model is introduced in [40], [41]. Using the same notations as the ones used in the $\prod$-model, the N-intertwined epidemic model can be written as

$$\frac{\mathrm{d}i_v(t)}{\mathrm{d}t} = -\beta_v i_v(t) + \sum_{u \in \mathcal{N}_v} \gamma_{vu} i_u(t)(1 - i_v(t)), \quad (2)$$

where $\beta_v > 0$ and $0 \leq \gamma_{vu} \leq 1$ respectively have the same meaning as mentioned above. We observe that the N-intertwined epidemic model (2) is different from the $\prod$-model (1) because the former contains a component $\sum_{u \in \mathcal{N}_v}$. The state-of-the-art understanding is:

Theorem 2 [9], [20], [23], [33], [41]: Consider system (2)*. Let $B = \mathsf{diag}(\beta_1, \ldots, \beta_n)$ and $\Gamma = [\gamma_{vu}]$ where $v, u \in \mathcal{V}$. For any initial state $i(0) \neq \mathbb{0}$ with a* strongly connected *attack-defense graph structure $\mathcal{G}$, the equilibrium $\mathbb{0}$ is globally asymptotically stable if and only if $s(-B + \Gamma) \leq 0$ [9], [23], [41]. For $s(-B + \Gamma) > 0$, there exists an $i^* \in (0, 1)^n$ such that i^* is globally asymptotically stable [9], [20], [23].*

As mentioned above, the N-intertwined epidemic model is extended to accommodate a node self-infection probability, leading to the ϵ-SIS model [30]. This model is explored in form of a continuous-time Markov Chain, where the "metastable" state can be approximately computed and characterized by the epidemic threshold when the self-infection probability ϵ is *small* — a limitation of the ϵ-SIS model, while noting that no such restriction is imposed by the $\prod$-model.

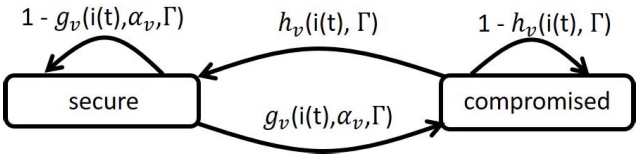

Fig. 2. State-transition diagram of node $v \in \mathcal{V}$ in the unified model, where $g_v(i(t), \alpha_v, \Gamma)$ and $h_v(i(t), \Gamma)$ depend on $i(t) = [i_1(t), \ldots, i_n(t)]^\top$ and the weighted adjacent matrix $\Gamma = [\gamma_{vu}]_{n \times n}$ of the attack-defense structure $\mathcal{G}$, and $g_v(i(t), \alpha_v, \Gamma)$ further depends on the pull-based attack or self-infection probability α_v.

From a dynamical system point of view, this extended N-intertwined epidemic model can be re-written as (using the same notations as in the $\prod$-model):

$$\frac{\mathrm{d}i_v(t)}{\mathrm{d}t} = -\beta_v i_v(t) + \left(\alpha_v + \sum_{u \in \mathcal{N}_v} \gamma_{vu} i_u(t)\right)(1 - i_v(t)), \quad (3)$$

where $\alpha_v = \alpha \in [0, 1]$ for $v \in \mathcal{V}$ can be arbitrary.

As mentioned above, for ease of reference, we call system (3) the "the $\sum$-dynamics" and interchangeably "the $\sum$-model," which accommodates the N-intertwined epidemic dynamics model (2) as a special example (by setting $\alpha_v = 0$ for all $v \in \mathcal{V}$). To the best of our knowledge, this dynamical system model (with arbitrary α) is not investigated until now.

III. Unified Preventive and Reactive Cyber Defense Dynamics

A. The Unified Model

This model unifies the $\prod$-model and the $\sum$-model reviewed above into a single framework. As in the $\prod$-model and the $\sum$-model, we let $s_v(t)$ be the probability that node $v \in \mathcal{V}$ is *secure* at time t and $i_v(t)$ be the probability that node $v \in \mathcal{V}$ is *compromised* at time t, where $s_v(t) + i_v(t) = 1$.

Figure 2 presents the state-transition diagram of node $v \in \mathcal{V}$ in the unified model, leading to:

$$f_v(i(t), \alpha_v, \Gamma) \stackrel{def}{=} \frac{di_v(t)}{dt} = -h_v(i(t), \Gamma) \times i_v(t) + g_v(i(t), \alpha_v, \Gamma) \times (1 - i_v(t)), \quad (4)$$

where $\alpha = [\alpha_1, \ldots, \alpha_n]^\top$ with α_v for $v \in \mathcal{V}$ being the probability that a secure node v becomes compromised because of pull-based attacks (reflecting the failure of preventive defense against pull-based attacks) or self-infection, γ_{vu} is the probability that an attack launched from node u against node v succeeds where $(u, v) \in \mathcal{E}$ (i.e., this probability reflects the failure of preventive defense against push-based attacks), $\Gamma = [\gamma_{vu}]_{n \times n}$ is the weighted adjacent matrix of the attack-defense structure $\mathcal{G}$, $h_v(i(t), \Gamma) : [0, 1]^n \times [0, 1]^{n,n} \to [0, 1]$ is the probability that a *compromised* node v becomes *secure* at time t because of the reactive defense, and $g_v(i(t), \alpha_v, \Gamma) : [0, 1]^n \times [0, 1] \times [0, 1]^{n,n} \to [0, 1]$ is the probability that a *secure* node v becomes *compromised* at time t because of

pull-based attacks (or self-infection) or push-based attacks. Hence, the compact form of the unified model (4) is

$$f(i(t),\alpha,\Gamma) \stackrel{def}{=} \frac{di(t)}{dt} = -H(i(t),\Gamma) \times i(t) + G(i(t),\alpha,\Gamma) \times (\mathbb{1} - i(t)), \quad (5)$$

where $\mathbb{1} = [1,\ldots,1]_n^\top$, diagonal matrix $H(i(t),\Gamma) = \mathsf{diag}(h_1(i(t),\Gamma),\ldots,h_n(i(t),\Gamma))$ has diagonal elements $h_1(i(t),\Gamma),\ldots,h_n(i(t),\Gamma)$, and diagonal matrix $G(i(t),\alpha,\Gamma) = \mathsf{diag}(g_1(i(t),\alpha_1,\Gamma),\ldots,g_n(i(t),\alpha_n,\Gamma))$ has diagonal elements $g_1(i(t),\alpha_1,\Gamma),\ldots,g_n(i(t),\alpha_n,\Gamma)$. The Jacobian matrix of $f(i(t),\alpha,\Gamma)$ with respect to i is denoted by $D_i[f] \in [0,1]^{n,n}$, where

$$D_i[f]_{vu}(i(t),\alpha,\Gamma) = \frac{\partial f_v}{\partial i_u}(i(t),\alpha_v,\Gamma). \quad (6)$$

B. Properties of Functions $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$

Functions $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$ in the unified model (4) should not be arbitrary but satisfy some mathematical properties to facilitate analysis and accommodate some real-world cybersecurity meanings. Of course, we must assure that these properties are satisfied by the $\prod$-model and the $\sum$-model (see Lemma 1 below). In what follows, we discuss three properties that represent the mild conditions mentioned above.

Property 1: Functions $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$ in the unified model (4) *have continuous and bounded derivatives with respect to vector variable i.*

Property 1 facilitates mathematical treatment. The validation of Property 1 requires to conducting cyber attack-defense experiments, which are orthogonal to the focus of the present study. This is reasonable because a characterization study, such as the present one, should consider as-general-as-possible classes of g_v's and h_v's to accommodate as-many-as-possible real-world scenarios.

Property 2: For any $u,v \in \mathcal{V}$ and $u \neq v$, $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$ in the unified model (4) *should satisfy*

- $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u} \geq 0$*: This is because in the context of preventive and reactive cyber defense dynamics, when everything else is fixed, a larger probability i_u leads to a higher probability $g_v(i(t),\alpha_v,\Gamma)$. That is, the more compromised nodes that can attack a secure node v, the higher the probability that v will be compromised. Moreover, we have $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u} > 0$ when $\gamma_{vu} > 0$ (because u can attack v) and $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u} = 0$ when $\gamma_{vu} = 0$ (because u cannot attack v).*
- $\frac{\partial h_v(i(t),\Gamma)}{\partial i_u} = 0$*: This is because in the context of preventive and reactive cyber defense dynamics, the reactive defense capability at a node is inherent to the node itself (i.e., independent of the neighboring nodes).*

Property 2 captures the cybersecurity meaning that the probability that node v gets compromised will increase with the probability that node u is compromised, namely $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u} > 0$, where $(u,v) \in \mathcal{E}$ and $\gamma_{vu} > 0$. When $(u,v) \notin \mathcal{E}$, meaning $\gamma_{vu} = 0$, the state of node u does not has any direct impact via (u,v) on the probability that node v gets compromised, namely $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u} = 0$. Moreover, the probability that a compromised node v becomes secure is independent of the state of node u, namely $\frac{\partial h_v(i(t),\Gamma)}{\partial i_u} = 0$ for all $u \in \mathcal{V}, u \neq v$.

Property 3: Functions $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$ in the unified model (4) *further satisfy: (i) $\underline{h_v} > 0$ where $\underline{h_v}$ is the infimum of $h_v(i(t),\Gamma)$; (ii) $D_i[h_v + g_v](i(t),\alpha_v,\Gamma) > \mathbb{0}$; and (iii) $g_v(i(t),\alpha_v,\Gamma)$ is subhomogeneous for all i in $[0,1]^n$ and all $v \in \mathcal{V}$.*

Property 3 captures that there is always a non-zero probability for a secure node v to become compromised at any point in time and that there is always a non-zero probability for a compromised node v becomes secure at any point in time. This property allows us to derive the strong subhomogeneity of the unified model (4); see Lemma 4 below.

C. Basic Properties of the Unified Model

In this subsection we discuss the basic properties of the unified model, including its generality, a non-trivial boundedness of $i_v(t)$, its cooperativeness, its strong subhomogeneity, and the properties of its equilibrium.

1) Generality of the Unified Model:

Lemma 1: (Generality of the Unified Model (4)): The unified model (4) *unifies, under Properties 1-3, the $\prod$-model* (1) *and the $\sum$-model* (3) *into a single framework.*

Proof: In order to prove the lemma, we need to show (i) the $\prod$-model and the $\sum$-model can be derived from the unified model with special instantiations of $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$, and (ii) the $\prod$-model and the $\sum$-model satisfy Properties 1-3.

To prove (i), we first observe that the unified model (4) can be instantiated as the $\prod$-model (1) by setting

$$g_v(i(t),\alpha_v,\Gamma) = 1 - (1-\alpha_v) \prod_{u \in \mathcal{N}_v} (1 - \gamma_{vu} i_u(t)) \quad (7)$$

and $h_v(i(t),\Gamma) = \beta_v$. Similarly, the unified model (4) can be instantiated as the $\sum$-model (3) by setting

$$g_v(i(t),\alpha_v,\Gamma) = \alpha_v + \sum_{u \in \mathcal{N}_v} \gamma_{vu} i_u(t) \quad (8)$$

and $h_v(i(t),\Gamma) = \beta_v$.

To prove (ii), we show the $\prod$-model and the $\sum$-model satisfy the three properties one-by-one.

First, by substituting $g_v(i(t),\alpha_v,\Gamma)$ as the right-hand side of Eq. (7) and $h_v(i(t),\Gamma) = \beta_v$ into the unified model, we find that $g_v(i(t),\alpha_v,\Gamma)$ is a continuous differentiable function of $i_v(t)$ for any $v \in \mathcal{V}$ in the range of $[0,1]$ and that $h_v(i(t),\Gamma)$ is constant. This means that $g_v(i(t),\alpha_v,\Gamma)$ and $h_v(i(t),\Gamma)$ in the $\prod$-model have continuous and bounded derivatives, and therefore satisfy Property 1. Similarly, by substituting $g_v(i(t),\alpha_v,\Gamma)$ as the right-hand side of Eq. (8) and $h_v(i(t),\Gamma) = \beta_v$ into the unified model, we can draw a similar conclusion.

Second, the $\prod$-model and the $\sum$-model satisfy Property 2 because $h_v(i(t),\Gamma)$ in both cases is constant, whose derivation

is zero. Moreover, in $\prod$-model we have,

$$\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u}=(1-\alpha_v)\prod_{k\in\mathcal{N}_v\setminus\{u\}}(1-\gamma_{vk}i_k(t))\gamma_{vu}\geq 0 \tag{9}$$

and in $\sum$-model, we have

$$\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u}=\gamma_{vu}\geq 0. \tag{10}$$

Therefore, the $\prod$-model and the $\sum$-model satisfy Property 2.

Third, in the $\prod$-model and the $\sum$-model, $h_v(i)$ is a positive constant (meaning $\underline{h_v}>0$) and $\frac{\partial g_v(i(t),\alpha,\Gamma)}{\partial i_u}>0$ when $i(t)\gg\mathbb{0}$ for any $t\geq 0$. Therefore, we have $D_i[h_v+g_v](i(t),\alpha_v,\Gamma)>\mathbb{0}$ for $i(t)\gg\mathbb{0}$ and any $t\geq 0$. What remains to be shown is the subhomogeneity of $g_v(i(t),\alpha_v,\Gamma)$. For this purpose, we consider the two models separately.

For the $\prod$-model (1), we prove the subhomogeneity by using induction. When $N(v)=1$, $g_v(i(t),\alpha_v,\Gamma)$ is subhomogeneous with respect to i because for any $\delta\in(0,1)$ and $i\gg\mathbb{0}$, we have $g_v(\delta i,\alpha_v,\Gamma)-\delta g_v(i,\alpha_v,\Gamma)=1-(1-\alpha)(1-\gamma_{vu}\delta i_u)-\delta(1-(1-\alpha)(1-\gamma_{vu}i_u))\geq 0$. Suppose $g_v(i(t),\alpha_v,\Gamma)$ is subhomogeneous with respect to i when $N(v)=k$. For $N(v)=k+1$, we have

$$\begin{aligned}
&g_v(\delta i,\alpha_v,\Gamma)-\delta g_v(i,\alpha_v,\Gamma)\\
&=1-(1-\alpha)(1-\gamma_{vu_{k+1}}\delta i_{u_{k+1}})\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{vu_s}\delta i_{u_s})\\
&\quad-\delta(1-(1-\alpha)(1-\gamma_{vu_{k+1}}i_{u_{k+1}})\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{vu_s}i_{u_s}))\\
&=1-(1-\alpha)\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{vu_s}\delta i_{u_s})\\
&\quad-\delta[1-(1-\alpha)\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{vu_s}i_{u_s})]\\
&\quad+\delta(1-\alpha)\gamma_{vu_{k+1}}i_{u_{k+1}}[\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{vu_s}\delta i_{u_s})\\
&\quad-\prod_{u_s\in\mathcal{N}_v\setminus\{u_{k+1}\}}(1-\gamma_{u_sv}i_{u_s})]\geq 0.
\end{aligned}$$

That is, $g_v(i(t),\alpha_v,\Gamma)$ is subhomogeneous with respect to i in the $\prod$-model.

For the $\sum$-model (3), we have

$$g_v(\delta i,\alpha_v,\Gamma)=\alpha_v+\delta\sum_{u\in\mathcal{N}_v}\gamma_{vu}i_u\geq\delta g_v(i,\alpha_v,\Gamma),$$

which means $g_v(i(t),\alpha_v,\Gamma)$ is subhomogeneous with respect to i in the $\sum$-model. □

Lemma 1 can be summarized informally as:

Insight 1: The unified preventive and reactive cyber defense dynamics model accommodates the extensively-studied $\prod$-model (1) *and $\sum$-model* (3) *as special cases.*

2) Non-Trivial Boundedness of $i_v(t)$ When $t\to\infty$:

Lemma 2 (Non-Trivial Boundedness of the Unified Model (4)): Let $\underline{g_v}$ be the infimum of $g_v(\cdot)$, $\underline{h_v}$ be the infimum of $h_v(\cdot)$, $\overline{g_v}$ be the supremum of $g_v(\cdot)$, and $\overline{h_v}$ be the supremum of $h_v(\cdot)$, where $0\leq\underline{g_v}\leq\overline{g_v}\leq 1$ and $0\leq\underline{h_v}\leq\overline{h_v}\leq 1$. The unified model (4) *has the following properties: for each $v\in\mathcal{V}$,*

(i) *If $\underline{g_v}>0$, then there exist $\epsilon_{v,1}>0$ and $T_1>0$ such that $\inf_{t\geq T_1}i_v(t)\geq\epsilon_{v,1}$ and $\sup_{t\geq T_1}i_v(t)\leq 1$.*

(ii) *If $\underline{h_v}>0$, then there exist $\epsilon_{v,2}>0$ and $T_2>0$ such that $\inf_{t\geq T_2}i_v(t)\geq 0$ and $\sup_{t\geq T_2}i_v(t)\leq 1-\epsilon_{v,2}$.*

(iii) *If $\underline{g_v}>0$ and $\underline{h_v}>0$, then there exist $\epsilon_{v,1}>0$, $\epsilon_{v,2}>0$ and $T_3>0$ such that $\inf_{t\geq T_3}i_v(t)\geq\epsilon_{v,1}$ and $\sup_{t\geq T_3}i_v(t)\leq 1-\epsilon_{v,2}$.*

Proof: From the unified model (4), we have $\frac{di_v(t)}{dt}|_{i_v=0}\geq 0$ and $\frac{di_v(t)}{dt}|_{i_v=1}\leq 0$. This and the fact that the unified model (4) is a continuous dynamical system imply that $i_v(t)$ is bounded within $[0,1]$.

In order to prove (i), we can choose an $\epsilon_{v,1}\in\left(0,\min\left\{\frac{1}{2},\frac{\underline{g_v}}{\underline{g_v}+\overline{h_v}}\right\}\right]$ such that

$$\frac{di_v(t)}{dt}|_{i_v=\epsilon_{v,1}}\geq-\overline{h_v}*\epsilon_{v,1}+\underline{g_v}*(1-\epsilon_{v,1})\geq 0.$$

Since $\frac{di_v(t)}{dt}|_{i_v\in[0,\epsilon_{v,1})}>0$, there is a $T_1>0$ such that $\inf_{t\geq T_1}i_v(t)\geq\epsilon_{v,1}$ and $\sup_{t\geq T_1}i_v(t)\leq 1$.

In order to prove (ii), we can choose an $\epsilon_{v,2}\in\left(0,\min\left\{\frac{1}{2},\frac{h_v}{\underline{h_v}+\overline{g_v}}\right\}\right]$ such that

$$\frac{di_v(t)}{dt}|_{i_v=1-\epsilon_{v,2}}\leq-\underline{h_v}*(1-\epsilon_{v,2})+\overline{g_v}*\epsilon_{v,2}\leq 0.$$

Since $\frac{di_v(t)}{dt}|_{i_v\in(1-\epsilon_{v,2},1]}<0$, there is a $T_2>0$ such that $\inf_{t\geq T_2}i_v(t)\geq 0$ and $\sup_{t\geq T_2}i_v(t)\leq 1-\epsilon_{v,2}$.

In order to prove (iii), we choose $\epsilon_{v,1}$ as in case (i), choose $\epsilon_{v,2}$ as in case (ii), and choose $T_3=\max\{T_1,T_2\}$. Then, we have $\inf_{t\geq T_3}i_v(t)\geq\epsilon_{v,1}$ and $\sup_{t\geq T_3}i_v(t)\leq 1-\epsilon_{v,2}$. □

3) Cooperativeness of the Unified Model:

Lemma 3 (Cooperativeness of the Unified Model (4)*): The unified model* (4) *under Properties 1-2 is a cooperative dynamical system (according to Definition 1) and thus its solution is monotone (according to Definition 3).*

Proof: For any $i\in[0,1)^n$, Property 1 gives the differentiable property of $h_v(i)$ and $g_v(i)$ in the unified model (4). Then,

$$\begin{aligned}
\frac{\partial f_v(i(t),\alpha_v,\Gamma)}{\partial i_u}=&-\frac{\partial h_v(i(t),\Gamma)}{\partial i_u}i_v(t)\\
&+\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u}(1-i_v(t))
\end{aligned}$$

for any $u\in\mathcal{V}$ and $u\neq v$ is a convex linear combination of nonnegative items $-\frac{\partial h_v(i(t),\Gamma)}{\partial i_u}$ and $\frac{\partial g_v(i(t),\alpha_v,\Gamma)}{\partial i_u}$ by using Property 2. This means $\frac{\partial f_v(i(t),\alpha_v,\Gamma)}{\partial i_u}\geq 0$, namely that the unified model (4) is a cooperative system. Then, Theorem 1.7 in reference [15] and the fact that region $[0,1]^n$ is convex imply that the solution of the unified model (4) is monotone. □

4) Strong Subhomogeneity of the Unified Model:

Lemma 4 (Strong Subhomogeneity of the Unified Model (4)): The unified model (4) *under Properties 1 and 3 is strongly subhomogeneous in $[0,1]^n$ according to Definition 2.*

Proof: For any $\delta \in (0,1)$ and $i \in [0,1]^n$ with $i \gg \mathbb{0}$, we have

$$\begin{aligned} &f_v(\delta i,\alpha_v,\Gamma)-\delta f_v(i,\alpha,\Gamma)\\ &=[-h_v(\delta i,\Gamma)+h_v(i,\Gamma)]\delta i_v\\ &\quad+g_v(\delta i,\alpha_v,\Gamma)(1-\delta i_v)-g_v(i,\alpha_v,\Gamma)\delta(1-i_v)\\ &=[(h_v(i,\Gamma)+g_v(i,\alpha_v,\Gamma))-(h_v(\delta i,\Gamma)-g_v(\delta i,\alpha_v,\Gamma))]\delta i_v\\ &\quad+g_v(\delta i,\alpha_v,\Gamma)-\delta g_v(i,\alpha_v,\Gamma). \end{aligned} \tag{11}$$

Since Property 1 gives the differential property of $h_v(i,\Gamma)$ and $g_v(i,\alpha_v,\Gamma)$ in the unified model (4) with respect to i, by Taylor's theorem, there exists an $\alpha^* \in (\delta,1)$ such that

$$\begin{aligned} &(h_v(i,\Gamma)+g_v(i,\alpha_v,\Gamma))-(h_v(\delta i,\Gamma)+g_v(\delta i,\alpha_v,\Gamma))\\ &\qquad=D_i[h_v+g_v](\alpha^* i,\alpha_v,\Gamma)^\top(1-\delta)i>0. \end{aligned}$$

This means $f_v(\delta i)-\delta f_v(i) > g_v(\delta i)-\delta g_v(i) \geq 0$ because $g_v(i,\alpha_v,\Gamma)$ is subhomogeneous according to Property 3. Thus, the unified model (4) is strongly subhomogeneous. □

5) Properties of Equilibria in the Unified Model: We observe that when $\alpha_v = 0$ for all $v \in \mathcal{V}$, $\mathbb{0} = [0,\ldots,0]^\top$ is an equilibrium of the unified model (4). The convergence property of this equilibrium is characterized as follows:

Lemma 5: (Property of the Equilibrium $\mathbb{0}$ in the Unified Model (4) *When $\alpha_v = 0$ for all $v \in \mathcal{V}$): Suppose $\alpha_v = 0$ for all $v \in \mathcal{V}$, which means that $\mathbb{0}$ is an equilibrium of the unified model* (4)*. Suppose the attack-defense structure $\mathcal{G}$ is strongly connected in the unified model* (4)*. Under Properties 1-3,*

- *if $s(D_i[f](\mathbb{0},\alpha,\Gamma)) \leq 0$, then equilibrium $\mathbb{0}$ is globally asymptotically stable,*
- *if $s(D_i[f](\mathbb{0},\alpha,\Gamma)) > 0$, there exists a unique equilibrium $i^* \gg \mathbb{0}$ that is globally asymptotically stable,*

where $s(D_i[f](\mathbb{0},\alpha,\Gamma)) = \max\{R(\lambda) : det(\lambda I - D_i[f](\mathbb{0},\alpha,\Gamma)) = 0\}$.

Proof: This lemma can be derived by directly applying Lemma 2.1 in [56] or Corollary 3.2 in [43]. □

In the case $\alpha_v > 0$ for all $v \in \mathcal{V}$, $\mathbb{0}$ is not an equilibrium of the unified model (4), Lemmas 6 below characterizes the property of the equilibrium in $(0,1)^n$.

Lemma 6 (Property of the Equilibrium of the Unified Model (4) *When $\alpha_v > 0$ for all $v \in \mathcal{V}$): Under the condition Properties 1-3 holds and $\alpha_v > 0$ for all $v \in \mathcal{V}$ in the unified model* (4)*, there is a unique equilibrium $i^* \in (0,1)^n$ is globally asymptotically stable in $[0,1]^n$.*

Proof: The proof is divided into three parts, respectively showing the uniqueness, existence, and global asymptotic stability of the equilibrium. The existence and uniqueness of the equilibrium can be proven by directly applying Theorem 2.3.2 in [55], where the nonempty compact invariant set $\mathcal{K} = [\epsilon_{v,1}, 1-\epsilon_{v,2}]$ is assured by Lemma 2 and the solution of the unified model (4) being monotone is assured by Lemma 3. The global asymptotic stability of the unique equilibrium can be proven by applying Theorem 2.2.6 in [55], which shows that $\mathcal{K}$ contains only one equilibrium and the equilibrium is globally asymptotically stable. □

D. Main Results of the Unified Model

Recall that $\alpha_v > 0$ means v is subject to pull-based attacks or self-infection, and that $\alpha_v = 0$ means v isn't. In the general case, we may have $\alpha_v > 0$ for some $v \in \mathcal{V}$ and $\alpha_v = 0$ for the other v's. Therefore, we further denote by $\mathcal{V}_{\alpha=0}$ the set of nodes with $\alpha_v = 0$ and by $\mathcal{V}_{\alpha>0}$ the set of nodes with $\alpha_v > 0$. This means that we can partition $\mathcal{V}$ into $\mathcal{V} = \mathcal{V}_{\alpha=0} \cup \mathcal{V}_{\alpha>0}$, where $\mathcal{V}_{\alpha=0}$ or $\mathcal{V}_{\alpha>0}$ may be empty.

1) Global Convergence of the Unified Dynamics: We can always divide the attack-defense structure $\mathcal{G}$, which is a directed graph, into K *Strongly Connected Components* (SCCs), denoted by $\mathsf{SCC}_1,\ldots,\mathsf{SCC}_K$, such that within each SCC_k there is always a path between any pair of nodes in SCC_k. Denote the set of nodes of $\mathsf{SCC}_1,\ldots,\mathsf{SCC}_K$ respectively by $\mathcal{V}_{\mathsf{SCC}_1},\ldots,\mathcal{V}_{\mathsf{SCC}_K}$, and their size respectively by $N_{\mathsf{SCC}_1} = |\mathsf{SCC}_1|,\ldots,N_{\mathsf{SCC}_K} = |\mathsf{SCC}_K|$.

Under Property 2, the Jacobian matrix of $f(i)$, which is defined in Eq. (6) as $D_i[f](i(t),\alpha,\Gamma)$, has the Perron-Frobenius form:

$$P^\top D_i[f](i(t),\alpha,\Gamma)P = \begin{bmatrix} Df_{11} & Df_{12} & \ldots & Df_{1K}\\ 0 & Df_{22} & \ldots & Df_{2K}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & \ldots & 0 & Df_{KK} \end{bmatrix} \tag{12}$$

where $P^\top$ is a permutation matrix, and Df_{kk} corresponding to SCC_k for $k = 1,\ldots,K$ is an irreducible matrix. Denote by

$$\begin{aligned} H_k(i(t),\Gamma) &= \mathsf{diag}(h_{v_{k,1}}(i(t),\Gamma),\ldots,h_{v_{k,N_{scc_k}}}(i(t),\Gamma)),\\ g_k(i(t),\alpha,\Gamma) &= [g_{v_{k,1}}(i(t),\alpha_{v_{k,1}},\Gamma),\ldots,g_{v_{k,N_{scc_k}}}(i(t),\\ &\qquad \alpha_{k,N_{scc_k}},\Gamma)]. \end{aligned}$$

Let SCC_{R_k} be the set of SCCs that have pathes arriving at SCC_k, meaning that if $\mathsf{SCC}_{R_k} \neq \emptyset$, then there is at least one path from a node in $\mathsf{SCC}_r \in \mathsf{SCC}_{R_k}$ to a node in SCC_k.

Theorem 3 (Global Convergence of the Unified Dynamics): Consider the unified model (4) *under Properties 1-3, where $\mathcal{V}$ is partitioned into $\mathcal{V} = \mathcal{V}_{\alpha=0} \cup \mathcal{V}_{\alpha>0}$ and the attack-defense structure $\mathcal{G} = (\mathcal{V},\mathcal{E})$ contains K strongly connected components SCC_k for $k = 1,\ldots,K$. For each SCC_k, the following holds*:

(i) *If $\mathcal{V}_{\mathsf{SCC}_k} \cap \mathcal{V}_{\alpha>0} \neq \emptyset$, then SCC_k has a unique equilibrium $i_k^* \in (0,1)^{N_{\mathsf{SCC}_k}}$ that is globally asymptotically stable in $[0,1]^{N_{\mathsf{SCC}_k}}$.*

(ii) *If $\mathcal{V}_{\mathsf{SCC}_k} \cap \mathcal{V}_{\alpha>0} = \emptyset$ and $s(-H_k(\mathbb{0}_{N_{\mathsf{SCC}_k}},\Gamma) + D_i[g_k](\mathbb{0}_{N_{\mathsf{SCC}_k}},\alpha,\Gamma)) > 0$, then SCC_k has a unique equilibrium $i_k^* \in (0,1)^{N_{\mathsf{SCC}_k}}$ that is globally asymptotically stable in $[0,1]^{N_{\mathsf{SCC}_k}} \setminus \{\mathbb{0}_{N_{\mathsf{SCC}_k}}\}$.*

(iii) *If $\mathcal{V}_{\mathsf{SCC}_k} \cap \mathcal{V}_{\alpha>0} = \emptyset$, $\mathsf{SCC}_{R_k} = \emptyset$ and $s(-H_k(\mathbb{0}_{N_{\mathsf{SCC}_k}},\Gamma) + D_i[g_k](\mathbb{0}_{N_{\mathsf{SCC}_k}},\alpha,\Gamma)) \leq 0$, SCC_k has an equilibrium $\mathbb{0}_{N_{\mathsf{SCC}_k}}$ that is globally asymptotically stable in $[0,1]^{N_{\mathsf{SCC}_k}}$.*

(iv) *If $\mathcal{V}_{\mathsf{SCC}_k} \cap \mathcal{V}_{\alpha>0} = \emptyset$, $\mathsf{SCC}_{R_k} \neq \emptyset$, $s(-H_k(\mathbb{0}_{N_{\mathsf{SCC}_k}},\Gamma) + D_i[g_k](\mathbb{0}_{N_{\mathsf{SCC}_k}},\alpha,\Gamma)) \leq 0$, and*

- *$\mathbb{0}_{N_{\mathsf{SCC}_r}}$ is a globally asymptotically stable equilibrium for every $\mathsf{SCC}_r \in \mathsf{SCC}_{R_k}$, then $\mathbb{0}_{N_{\mathsf{SCC}_k}}$ is a globally asymptotically stable equilibrium of SCC_k in $[0,1]^{N_{\mathsf{SCC}_k}}$;*
- *$\mathbb{0}_{N_{\mathsf{SCC}_r}}$ is not a globally asymptotically stable equilibrium for every $\mathsf{SCC}_r \in \mathsf{SCC}_{R_k}$, then SCC_k has*

an equilibrium $i_k^* \in (0,1)^{N_{\mathsf{SCC}_k}}$ *that is globally asymptotically stable in* $[0,1]^{N_{\mathsf{SCC}_k}} \setminus \{\mathbb{0}_{N_{\mathsf{SCC}_k}}\}$.

The proof of Theorem 3 is quite involved because the attack-defense structure $\mathcal{G}$ may not be strongly connected, in which case we need to, and always can, divide $\mathcal{G}$ into multiple strongly connected components. The proof is deferred to Supplementary Material for a better readability. Theorem 3 can be summarized informally as:

Insight 2: The unified preventive and reactive cyber defense dynamics (4) *is still globally convergent under the aforementioned mild conditions (i.e., Properties 1-3).*

2) Convergence Speed of the Unified Dynamics: We re-write the unified mode (4) in the parameterized form as:

$$\frac{di(t)}{dt} = f(i(t),\theta) = f_\theta(i(t)) \tag{13}$$

where $\theta = [\theta_1, \cdots, \theta_m] \in \Omega$ for $m = n+n^2$ and $\Omega \subseteq \mathbb{R}^m$, and $f_\theta = [f_{\theta,1}, \cdots, f_{\theta,n}]^\top$ is the parameterized form of $f(i,\theta)$.

Theorem 4 (Convergence Speed of the Unified Dynamics): Consider the parameterized form (13) *of the unified model* (4) *under Properties 1-3. Suppose the attack-defense structure* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ *contains* K *strongly connected components* SCC_k *for* $k = 1, \ldots, K$. *For each* SCC_k, *suppose* $f(i,\theta)$ *has continuous second-order partial derivatives with respect to* i *and continuous first-order partial derivatives with respect to* θ *and Jacobian* $D[f_\theta]$ *is always irreducible for all* $i \in [0,1]^n$ *and* $\theta \in \Omega$. *Then, the convergence speed of the dynamics corresponding to* SCC_k *is characterized as follows*:

(i) *In the case* $\alpha_v = 0$ *for all* $v \in \mathcal{V}$ *(meaning* $i^* = \mathbb{0}$*): if* $s(D_i[f_\theta](\mathbb{0})) < 0$, *then the convergence speed of* $\mathbb{0}$ *is exponential; if* $s(D_i[f_\theta](\mathbb{0})) = 0$, $\frac{\partial^2 f_{\theta_v}(i)}{\partial i_p \partial i_q} \le 0$ *at* $i = \mathbb{0}$ *for all* $v,p,q \in \mathcal{V}$ *with* $p \neq q$, *and* $\frac{\partial^2 f_{\theta_v}(i)}{\partial i_p^2} \le -a$ *at* $i = \mathbb{0}$ *for some* $a > 0$ *and any* $v, p \in \mathcal{V}$, *then the convergence speed is at least polynomial.*

(ii) *In the case* $\alpha_v \ge 0$ *for all* $v \in \mathcal{V}$ *other than the case treated above (meaning* $i^* > \mathbb{0}$*): if matrix* $D[f_\theta](i,\theta)$ *is of full rank for all* $i \gg 0$ *and* $\theta \in \Omega$, *then the convergence speed of* i^* *is exponential for any* $\theta \in \Omega \backslash P$, *where* $P \subset \mathbb{R}^m$ *is a set of Lebesgue measure zero.*

Moreover, the unified model is exponentially convergent if the convergence speed of the dynamics corresponding to each SCC is exponential, and is polynomially convergent if the convergence speed of the dynamics corresponding to one of the SCCs is polynomial.

Proof: We first consider the simple case $K = 1$, meaning that $\mathcal{G}$ is strongly connected, and then consider that } is composed of $K > 1$ strongly connected components.

First, we consider the case of $K = 1$ that has irreducible Jacobian.

In case (i), we know $i^* = \mathbb{0}$. If $s(D_i[f_\theta](\mathbb{0})) < 0$, then the exponential convergence speed result can be derived from the stability theory of ordinary differential equations (see, e.g., [12]). If $s(D_i[f_\theta](\mathbb{0})) = 0$, then the Perron-Frobenius theorem [3] says that the geometric dimension of eigenvalue 0 of $D_i[f_\theta](\mathbb{0})$ is 1 and that the associated eigenvector $\xi = [\xi_1, \cdots, \xi_n]^\top$ have positive components and can be normalized as $\sum_v \xi_v = 1$. Let $\eta(t) = \xi^\top i(t)$. By the second-order Taylor expansion, we have

$$\begin{aligned}\frac{d\eta(t)}{dt} &= \xi^\top f_\theta(i(t)) = \xi^\top D_i[f_\theta](\mathbb{0}) i(t) \\ &\quad + \mu(i(t),\theta) + o(|i(t)|^2), \quad \text{and} \\ \mu(i(t),\theta) &= \sum_{v,p,q=1}^{n} \frac{\partial^2 f_{\theta_v}(\mathbb{0})}{\partial i_p \partial i_q} i_p(t) i_q(t) \xi_v.\end{aligned}$$

The condition $\frac{\partial^2 f_{\theta_v}(\mathbb{0})}{\partial i_p \partial i_q} \le 0$ for all $v,p,q \in \mathcal{V}$ with $p \neq q$ and the condition $\frac{\partial^2 f_{\theta_v}(\mathbb{0})}{\partial i_p^2} \le -a$ for some $a > 0$ and any $v, p \in \mathcal{V}$ imply $\mu(i(t),\theta) \le -c^*$, where $c^* = a \max_{v \in V} 1/(\xi_v)^2$. Thus, we have

$$\frac{d\eta(t)}{dt} \le -c\eta^2(t) + o(|\eta(t)|^2).$$

This inequality leads to the desired result of polynomial convergence speed, which means the converge speed is at least polynomial.

In case (ii), we have $i^* > 0$. The Sard Lemma [38] says that except for a set $P_1 \subset \mathbb{R}^n$ of Lebesgue measure zero, $D[f_\theta](i^*,\theta)$ is of full rank for all $\theta \notin P$, which implies that it does not have any zero eigenvalues. Since i^* is globally asymptotically stable, we conclude that $s(D_i[f_\theta](i^*)) < 0$, where $s(A)$ is the maximum among the real parts of the eigenvalues of matrix A. According to the stability theory of ordinary differential equations, we conclude that i^* is globally exponentially stable.

Second, consider the more general case of reducible Jacobian, meaning $K > 1$. The convergence speed of unified dynamics (4) depends on the SCC_k that has the slowest convergence speed. That is, if the convergence speed of the dynamics corresponding to some SCC_k is polynomial, then the convergence speed of the unified dynamics (4) is polynomial; otherwise, the convergence speed of the unified dynamics (4) is exponential.

This complete the proof of Theorem 4. □

Theorem 4 can be summarized informally as:

Insight 3: The unified preventive and reactive cyber defense dynamics (4) *converges, under the aforementioned mild conditions (i.e., Properties 1-3), at least polynomially but mostly exponentially.*

E. Relationship Between the Results in the Unified Model and the Literature Results in the $\prod$*-Model and the* $\sum$*-Model*

1) Instantiating Theorem 3 to $\prod$*-model and* $\sum$*-model:*

Corollary 1 (Corollary of Theorem 3 Corresponding to the $\prod$*-Model; Equivalent to Theorem 1 in Reference [58]): In the* $\prod$*-model* (1)*, the following two cases have been analyzed in the literature.*

- *In the case* $\alpha_v = 0$ *for* all $v \in \mathcal{V}$, *meaning that no node is subject to pull-based attacks, if* $s(-B+\Gamma) \le 0$ *where* $B = \mathsf{diag}(\beta_1, \ldots, \beta_n)$ *and* $\Gamma = [\gamma_{vu}], v, u \in \mathcal{V}$, *then* $\mathbb{0}$ *is globally asymptotically stable in* $[0,1]^n$*; otherwise, we have* $s(-B+\Gamma) > 0$ *and there is an equilibrium* $i^* \in [0,1)^n \setminus \{\mathbb{0}\}$ *that is globally asymptotically stable.*

- *If* $\alpha_v > 0$ *for* all $v \in \mathcal{V}$*, meaning that* every *node is subject to pull-based attacks, there is a unique equilibrium* $i^* \in (0,1)^n$ *that is globally asymptotically stable.*

Corollary 2 (Corollary of Theorem 3 Corresponding to the Special $\sum$*-Model (2); Equivalent to Theorem 2 in Reference [33]): In the special* $\sum$*-model* (2)*, where* $\alpha_v = 0$ *for* all $v \in \mathcal{V}$*, there are two cases.*

- *If* $s(-B+\Gamma) \leq 0$*, then* $\mathbb{0}$ *is globally asymptotically stable.*
- *If* $s(-B+\Gamma) > 0$*, then there is an equilibrium* $i^* \in [0,1)^n \setminus \{\mathbb{0}\}$ *that is globally asymptotically stable.*

Corollary 3 (Corollary of Theorem 3 Corresponding to the $\sum$*-Model (3); New Result): In the* $\sum$*-model* (3) *where* $\alpha_v > 0$ *for* all $v \in \mathcal{V}$*, there is a unique equilibrium* $i^* \in (0,1)^n$ *that is globally asymptotically stable.*

2) Convergence Speed of the $\prod$*-Model and the* $\sum$*-Model:*

Theorem 5 (Theorem 4 When Instantiated to the $\prod$*-Model and the* $\sum$*-Mode): Consider the* $\prod$*-model* (1) *and the* $\sum$*-model* (3)*. Suppose matrix* Γ *is irreducible. Then, we have the following results for the convergence speed of the globally stable equilibrium* i^* *in the* $\prod$*-model and the* $\sum$*-model*:

(i) *In the case* $\alpha_v = 0$ *for all* $v \in \mathcal{V}$ *(meaning* $i^* = \mathbb{0}$*), if* $s(-B+\Gamma) < 0$*, then the convergence speed of* $\mathbb{0}$ *is exponential; if* $s(-B+\Gamma) = 0$*, then the convergence speed is at least polynomial.*

(ii) *In the case* $\alpha_v \geq 0$ *for all* $v \in \mathcal{V}$ *other than the case treated above, meaning* $i^* > \mathbb{0}$*, the convergence speed of* i^* *is exponential when* $\beta = [\beta_1, \cdots, \beta_n]^\top \notin P_1$ *where* $P_1 \subset \mathbb{R}^n$ *is a set of Lebesgue measure zero, or when* $\alpha = [\alpha_1, \cdots, \alpha_n]^\top \notin P_2$ *where* $P_2 \subset \mathbb{R}^n$ *is a set of Lebesgue measure zero, or when* $\Gamma = [\gamma_{vu} : u, v \in \mathcal{V}] \notin P_3$ *where* $P_3 \subset \mathbb{R}^{n,n}$.

The proof of Theorem 5 is similar to the proof of Theorem 4 and therefore omitted. Summarizing Corollaries 1-3 and Theorem 5, we obtain the following:

Insight 4: Our results in regards to the unified preventive and reactive cyber defense dynamics (4) *supersede the literature results in regards to the* $\prod$*-dynamics* (1) *and the literature results in regards to the* $\sum$*-dynamics* (3)*.*

3) Summarizing the Relationship Between the Mathematical Properties, Lemmas, Theorems, and Corollaries: For better readability, we use Figure 3 to highlight the relationship between the mathematical properties, lemmas, theorems, and corollaries that have been discussed until the present section.

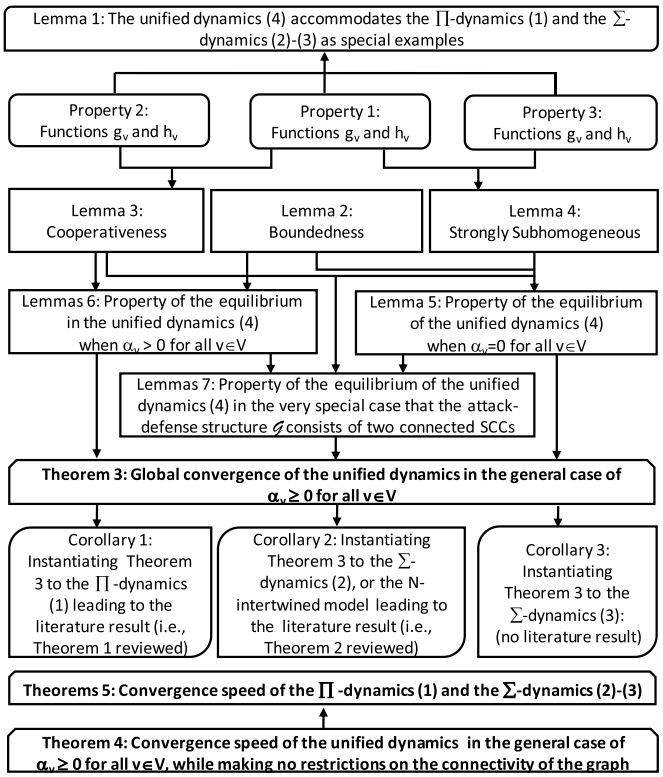

Fig. 3. Relationship between the mathematical properties, lemmas, theorem, and corollaries presented in the present paper (while noting that Lemma 7 is deferred to the Supplementary Material because it can be seen as a very special case of Theorem 3), and the relationship between the main theorem presented in this paper and the results presented in the literature.

IV. Numerical Illustrations

In this section, we use numerical examples to answer two questions. First, how general is our main result? In order to answer this question, we use numerical examples to show the following: Theorem 3 is applicable to the unified model (4) in the general case $0 \leq \frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} \leq 1$, which has not been considered in the literature even for the special $\prod$-model and $\sum$-model because the literature at most considers $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} = 0$ and $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} = 1$ separately. Second, is the mild condition (Property 3) required by Theorem 3 also necessary (while noting that Properties 1 and 2 naturally hold)?

For our numerical study, we treat the Internet peer-to-peer network called Gnutella06 in `http://snap.stanford.edu/data/index.html` as an example of the attack-defense structure $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. This is a plausible alternative because real-world attack-defense structures need to be derived from the topologies of real-world networks and their security configurations (e.g., access control and firewall policies), which are often sensitive and are not available to academic researchers. This means that as mentioned above, the attack-defense structure is in general different from the underlying physical network. This peer-to-peer network has $|\mathcal{V}| = 8,717$ nodes and $|\mathcal{E}| = 31,525$ *directed* edges. The security metric we use is $\bar{i}(t) \stackrel{def}{=} \frac{\sum_{v\in\mathcal{V}} i_v(t)}{|\mathcal{V}|}$, which is the fraction of compromised nodes at time t and succinctly represents the evolution of the dynamics.

A. Illustrating the Generality of the Main Result (Theorem 3)

For this purpose, we need to consider some concrete instantiation of the unified model (4). As an example, we consider the $\sum$-dynamics (3), which as mentioned above satisfies Properties 1-3 that are required by the main result. We conduct two experiments, each considering $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} \in \{0, 0.5, 1\}$ (i.e., 0%, 50%, and 100% of the nodes are subject to pull-based attacks or self-infection). The generality of our result is shown for the case $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} = 0.5$ because the literature results only cover the cases $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} \in \{0, 1\}$.

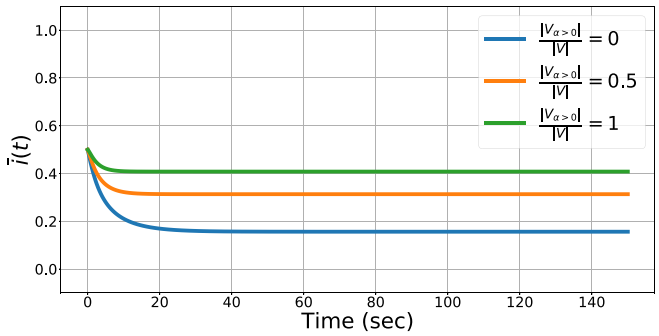

Fig. 4. Convergence of the $\sum$-dynamics (3) with $\alpha_v = 0.1$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.4$, and $\gamma_{vu} = 0.15$.

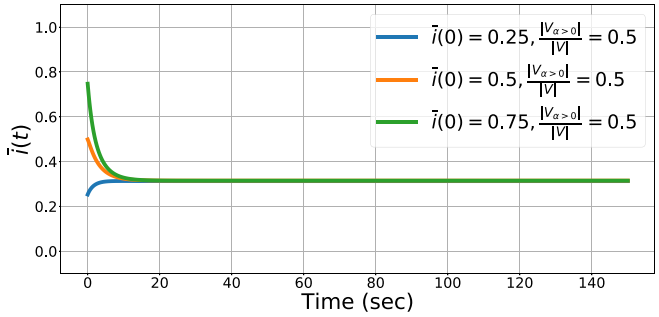

Fig. 5. Global convergence of the $\sum$-dynamics (3) with $\alpha_v = 0.1$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.4$, and $\gamma_{vu} = 0.15$.

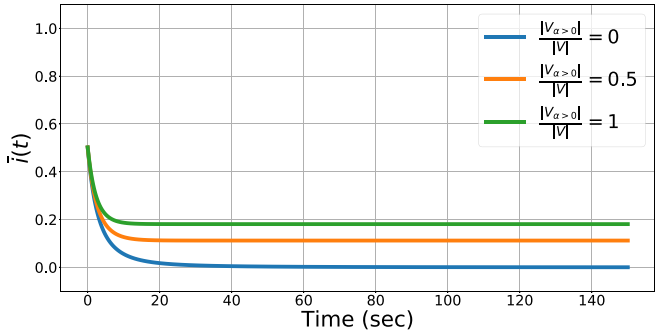

Fig. 6. Convergence of the $\sum$-dynamics (3) with $\alpha_v = 0.05$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.5$, and $\gamma_{vu} = 0.1$.

In the first experiment, we have $\alpha_v = 0.1$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.4$ for $v \in \mathcal{V}$, and $\gamma_{vu} = 0.15$ for $(u, v) \in \mathcal{E}$. Figure 4 plots the evolution of $\bar{i}(t)$, which is the fraction of the compromised nodes over time t, corresponding to the initial state that 50% of the randomly selected nodes are in the *compromised* state. We observe that $\bar{i}(t)$ in each of the three scenarios indeed converges to an equilibrium whose location depends on the parameter values. On the other hand, Figure 5 shows the global convergence when randomly-selected 50% of the nodes are subject to pull-based attacks.

In the second experiment, we set $\alpha_v = 0.05$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.5$ for $v \in \mathcal{V}$, and $\gamma_{vu} = 0.1$ for $(u, v) \in \mathcal{E}$. Figure 6 plots the evolution of $\bar{i}(t)$ with the initial state that 50% of the randomly selected nodes are in the *compromised* state.

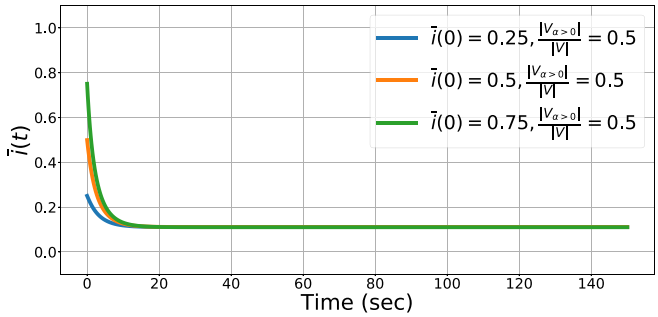

Fig. 7. Global convergence of the $\sum$-dynamics (3) with $\alpha_v = 0.05$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.5$, and $\gamma_{vu} = 0.1$.

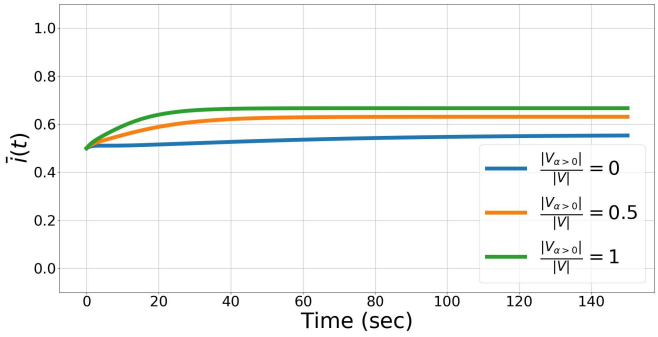

Fig. 8. Convergence of the unified model violate Property 3.

We observe that $\bar{i}(t)$ in each of the three scenarios indeed converges to an equilibrium. On the other hand, Figure 7 shows the global convergence when randomly-selected 50% of the nodes are subject to pull-based attacks.

B. Illustrating the Necessity of a Mild Condition

Since Properties 1-2 are naturally satisfied, we focus on the necessity of Property 3. We propose considering two examples of the unified model (4), one showing that the dynamics is still globally convergent even if Property 3 is violated, and the other showing that the dynamics is not globally convergent when Property 3 is violated. This empirically hints that Property 3 is necessary for global convergence under certain assumption, but its precise formulation is left an outstanding open problem.

1) Example Hinting That Property 3 May not be Necessary: In this example, we consider the unified model (4) while setting

$$h_v(i(t), \Gamma) = \beta_v$$
$$g_v(i(t), \alpha_v, \Gamma) = 0.5 \times \left(\frac{1}{N(v)} \sum_{u \in \mathcal{N}_v} \gamma_{vu} i_u(t) \right)^2 + 0.5 \times \alpha_v^2.$$

We observe that in this case Property 3 does not hold because $g_v(i(t), \alpha_v, \Gamma)$ is not subhomogeneous with respect to variable i. We conduct two experiments, each considering three scenarios of $\mathcal{V}_{\alpha>0}$: $\frac{|\mathcal{V}_{\alpha>0}|}{|\mathcal{V}|} \in \{0, 0.5, 1\}$.

In the first experiment, we set $\alpha_v = 0.2$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.1$ for $v \in \mathcal{V}$, $\gamma_{vu} = 0.9$ for $(u, v) \in \mathcal{E}$. Figure 8 shows

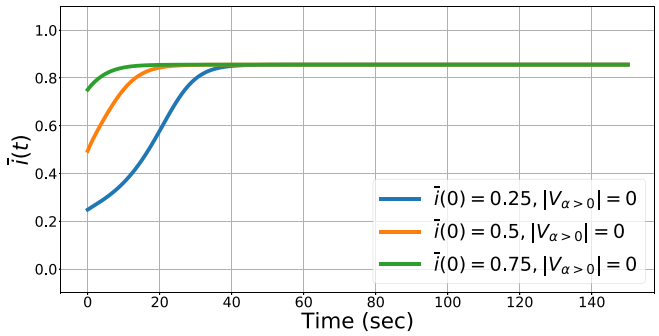

Fig. 9. Global convergence of the unified model that violate Property 3.

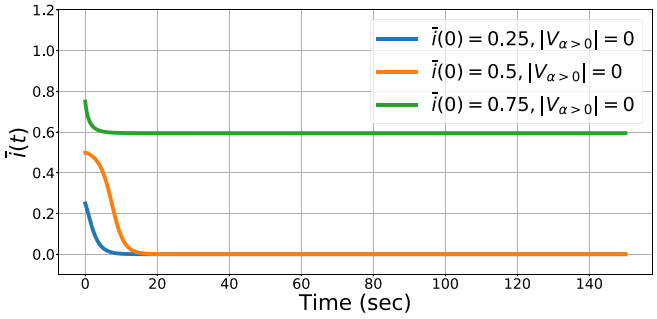

Fig. 10. Convergence of the unified model with functions $g_v(i(t))$ and $h_v(i(t))$ that violate Property 3.

that when the initial state is that 50% randomly selected nodes are in the *compromised* state, $\bar{i}(t)$ is still convergent in each of the three scenarios albeit the location of the equilibrium depends on the parameter values.

In the second experiment, we set $\alpha_v = 0.1$ for $v \in \mathcal{V}_{\alpha>0}$, $\beta_v = 0.05$ for $v \in \mathcal{V}$, and $\gamma_{vu} = 0.9$ for $(u, v) \in \mathcal{E}$ Figure 9 shows that $\bar{i}(0)$, despite three different initiate states, indeed converges to the same equilibrium, implying global convergence.

2) Example Hinting That Property 3 May be Necessary: In this example, we consider the unified model (4) while setting

$$h_v(i(t), \Gamma) = \beta_v$$
$$g_v(i(t), \alpha_v, \Gamma) = \begin{cases} 4x^3(t), & \text{if } x(t) \in [0, 0.5), \\ 1 - 4(1 - x(t))^3, & \text{if } x(t) \in [0.5, 1] \end{cases}$$

where $x(t) = \frac{1}{N(v)} \sum_{u \in \mathcal{N}_v} \gamma_{vu} i_u(t)$. We observe that Property 3 does not hold because $g_v(i(t), \alpha_v, \Gamma)$ is not sub-homogeneous with respect to variable i.

In the experiment, we set $\alpha_v = 0$ and $\beta_v = 0.5$ for $v \in \mathcal{V}$ and $\gamma_{vu} = 1$ for $(u, v) \in \mathcal{E}$, and consider different initial states. Figure 10 shows that $\bar{i}(0)$ converges to different equilibria with respect to different initial states, hinting that Property 3 is necessary for the global convergence result.

Insight 5: Our empirical experiment hints that Property 3 *is necessary for the global convergence result, but it is an open problem to prove the necessity rigorously.*

V. Limitations and Future Research Directions

The present study has several limitations. First, the unified dynamics is proven to be globally convergent under some mild conditions. It is an exciting future work to prove (or disprove) the necessity of Property 3.

Second, the present work focuses on characterization, assuming cyber-attack-defense structure $\mathcal{G}$ and model parameters α_v, β_v, and γ_{vu} are given (following [33], [41], [58] and the references therein). Although such characterization studies make no restrictions on the structure and model parameters, we need to design algorithms for extracting the cyber-attack-defense structure $\mathcal{G}$ and model parameters α_v, β_v, and γ_{vu} in real-world cyber environments. One challenge is that it is difficult for academic researchers to obtain such datasets, which are often sensitive (e.g., real-world network topologies and their security policies).

Third, much research needs to be conducted to show how to exploit the global convergence result to design practical sampling methods to estimate the global cybersecurity state, such as the fraction of compromised nodes $\bar{i}(t)$ even when the model parameters are not known. This is important because it may be costly to obtain the model parameters. An promising result in this direction is given in [50], which shows the possibility of designing sampling algorithms to derive $\bar{i}(t)$ by using a very small number of sensors *without* knowing the values of the model parameters.

Fourth, pull-based attacks and push-based attacks are assumed to be waged independently, and the *compromised* nodes are assumed to wage attacks independently. Although this assumption has been widely adopted (see, for example, [33], [41], [58] and the references therein), in the long-term this assumption needs to be weakened or eliminated. Initial results in this direction have been reported in [8], [44], [45], but much more remains to be done.

Fifth, in the present paper, the attack-defense structure $\mathcal{G}$ and the model parameters α_v, β_v and γ_{vu} are assumed to be time-independent. These assumptions might be valid for a small time scale or when the cybersecurity dynamics converge *exponentially*. The more general case of time-dependent attack-defense structures $\mathcal{G}(t)$ and time-dependent parameters $\alpha_v(t)$, $\beta_v(t)$ and $\gamma_{vu}(t)$ are left for future study.

VI. Related Work

The most closely related prior work is [50], [58], which characterize the preventive and reactive cyber defense dynamics (i.e., the $\prod$-model). This dynamics model is originally introduced in [24], which however does not give any satisfactory analytical treatment. The modeling approach adopted in [24] is initiated in [42] and later further studied, for example, in [5], [10]. However, these models [5], [10], [42] do not consider pull-based attacks (i.e., they only consider push-based attacks). Moreover, these studies [5], [10], [42] characterize the dynamics in the parameter regime below the epidemic threshold (i.e., the dynamics converges to the zero equilibrium or the spreading dies out). In contrast, [50] presents the first conditional convergence result for the case $\alpha > 0$ (i.e., all nodes are vulnerable to pull-based attacks). Moreover, [58] shows that the $\prod$-dynamics is globally convergent by eliminating the condition that is imposed in [50]. Nevertheless, [58] only considers the $\prod$-dynamics in the special cases of $\alpha = 0$

(i.e., no nodes are vulnerable to pull-based attacks) and $\alpha > 0$ (i.e., all nodes are vulnerable to pull-based attacks), but not in the general case of $\alpha \geq 0$ (i.e., some nodes may be vulnerable to pull-based attacks but the others aren't), which is resolved in the present paper.

A closely-related modeling approach is the N-intertwined model [41]. This approach is seemingly also rooted in [42], but uses a different method to model the aggregate effect of multiple nodes attacking a single node. This approach has been investigated in, for example, [4], [9], [20], [23], [33], [35], [37], [39]. The N-intertwined model is also extended to the ϵ-SIS model [30] by using a parameter ϵ to model the self-infection probability, which is analogous to the aforementioned pull-based attack probability α introduced in [24]. The parameter is assumed to be small (i.e., ≈ 0) in [30]. In contrast, we investigate the dynamical system version of the $\sum$-model with an *arbitrary* self-infection probability α.

From a broader point of view, preventive and reactive cyber defense dynamics is just one family of models in the cybersecurity dynamics framework [46], [48], which aims to systematically understand all kinds of cyber defense dynamics, including: adaptive cyber defense dynamics that aims to model the interaction between an attacker and an adaptive defender (e.g., [32], [51], [53], [54]); active cyber defense dynamics that aims to model the interaction between an attacker and an active defender who leverages a push-based defense mechanism (e.g., [27], [49], [57]); and proactive cyber defense dynamics that aims to model the interaction between an attacker and a proactive defender (e.g., [13], [28], [31]). Understanding these kinds of cybersecurity dynamics will pave the way for establishing a unified body of knowledge in understanding cybersecurity dynamics as a whole.

VII. Conclusions

We have unified two widely-investigated cyber defense dynamics models into a single framework, proved that the unified dynamics is globally convergent, and characterized the convergence speed of the unified dynamics. The unified framework gets rid of some unnecessary assumptions that are made in the literature (e.g., the connectivity of the attack-defense structure and the smallness of the self-infection probability). The unified dynamics framework accommodates more classes of preventive and reactive cyber defense dynamics models than the class of $\prod$-models and the class of $\sum$-models that have been investigated in the literature. We have also discussed the limitations of the present study, leading to open problems for future research.

Acknowledgment

The authors thank the reviewers for their comments that helped improve the readability of the paper. The opinions are those of the authors' and do not reflect any of the funding agencies in any sense.

References

[1] R. M. Anderson and R. M. May, *Infectious Diseases of Humans*. Oxford, U.K.: Oxford Univ. Press, 1991.

[2] N. T. Bailey, *The Mathematical Theory of Infectious Diseases*, 2nd ed. London, U.K.: Griffin, 1975.

[3] A. Berman and N. Shaked-Monderer, *Completely Positive Matrices*. Singapore: World Scientific, 2003.

[4] W. K. Chai and G. Pavlou, "Path-based epidemic spreading in networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 1, pp. 565–578, Feb. 2017.

[5] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 4, pp. 1–26, 2008.

[6] H. Chen, J.-H. Cho, and S. Xu, "Quantifying the security effectiveness of firewalls and DMZs," in *Proc. 5th Annu. Symp. Bootcamp Hot Topics Sci. Secur. (HoTSoS)*, 2018, pp. 9-1–9-11.

[7] H. Chen, J.-H. Cho, and S. Xu, "Quantifying the security effectiveness of network diversity: Poster," in *Proc. 5th Annu. Symp. Bootcamp Hot Topics Sci. Secur. (HoTSoS)*, 2018, Art. no. 24.

[8] G. Da, M. Xu, and S. Xu, "A new approach to modeling and analyzing security of networked systems," in *Proc. Symp. Sci. Security (HotSoS)*, 2014, pp. 6-1–6-12.

[9] A. Fall, A. Iggidr, G. Sallet, and J.-J. Tewa, "Epidemiological models and Lyapunov functions," *Math. Model. Natural Phenomena*, vol. 2, no. 1, p. 62– 83, 2007.

[10] A. Ganesh, L. Massoulie, and D. Towsley, "The effect of network topology on the spread of epidemics," in *Proc. IEEE Infocom*, Mar. 2005, pp. 1455–1466.

[11] O. Goldreich, *Foundations of Cryptography*, vol. 1. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[12] J. K. Hale, *Ordinary Differential Equations*. New York, NY, USA: Wiley, 1969.

[13] Y. Han, W. Lu, and S. Xu, "Characterizing the power of moving target defense via cyber epidemic dynamics," in *Proc. Symp. Sci. Secur. (HotSoS)*, 2014, pp. 10-1–10-12.

[14] H. W. Hethcote, "The mathematics of infectious diseases," *SIAM Rev.*, vol. 42, no. 4, pp. 599–653, 2000.

[15] M. W. Hirsch, "Systems of differential equations that are competitive or cooperative II: Convergence almost everywhere," *SIAM J. Math. Anal.*, vol. 16, no. 3, pp. 423–439, 1985.

[16] K. D. Hoover, "Idealizing reduction: The microfoundations of macroeconomics," *Erkenntnis*, vol. 73, no. 3, pp. 329–347, 2010.

[17] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Symp. Secur. Privacy*, May 1991, pp. 343–361.

[18] J. O. Kephart and S. R. White, "Measuring and modeling computer virus prevalence," in *Proc. IEEE Symp. Secur. Privacy*, May 1993, pp. 2–15.

[19] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. Roy. Soc. London A, Math. Phys. Sci.*, vol. 115, no. 772, pp. 700–721, 1927.

[20] A. Khanafer, T. Başar, and B. Gharesifard, "Stability properties of infected networks with low curing rates," in *Proc. Amer. Control Conf.*, Jun. 2014, pp. 3579–3584.

[21] A. Khanafer, T. Başar, and B. Gharesifard, "Stability of epidemic models over directed graphs: A positive systems approach," *Automatica*, vol. 74, pp. 126–134, Dec. 2016.

[22] A. Khanafer, T. Başar, and B. Gharesifard, "Stability properties of infection diffusion dynamics over directed networks," in *Proc. Decis. Control*, 2015, pp. 6215–6220.

[23] A. Lajmanovich and J. A. Yorke, "A deterministic model for gonorrhea in a nonhomogeneous population," *Math. Biosci.*, vol. 28, nos. 3–4, p. 221–236, 1976.

[24] X. Li, T. P. Parker, and S. Xu, "Towards quantifying the (in)security of networked systems," in *Proc. IEEE AINA*, May 2007, pp. 420–427.

[25] X. Li, P. Parker, and S. Xu, "A stochastic model for quantitative security analyses of networked systems," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 1, pp. 28–43, Jan. 2011.

[26] T. M. Liggett, *Interacting Particle Systems*. Berlin, Germany: Springer-Verlag, 1985.

[27] W. Lu, S. Xu, and X. Yi, "Optimizing active cyber defense dynamics," in *Proc. GameSec*, 2013, pp. 206–225.

[28] H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, and M. van Dijk, "Markov modeling of moving target defense games," in *Proc. ACM Workshop Moving Target Defense (MTD)*, 2016, pp. 81–92.

[29] A. G. M'Kendrick, "Applications of mathematics to medical problems," *Proc. Edinburgh Math. Soceity*, vol. 14, pp. 98–130, Feb. 1926.

[30] Van Mieghem, Piet, and Eric Cator, "Epidemics in networks with nodal self-infection and the epidemic threshold," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 86, no. 1, 2012, Art. no. 016116.

[31] R. Mitchell, "Epidemic-resistant configurations for intrusion detection systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 487–494.
[32] C. Nowzari, M. Ogura, V. M. Preciado, and G. J. Pappas, "Optimal resource allocation for containing epidemics on time-varying networks," in *Proc. 49th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 1333–1337.
[33] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Analysis and control of epidemics: A survey of spreading processes on complex networks," *IEEE Control Syst.*, vol. 36, no. 1, pp. 26–46, Feb. 2016.
[34] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 63, no. 6, p. 066117, 2001.
[35] V. M. Preciado and A. Jadbabaie, "Moment-based spectral analysis of large-scale networks using local structural information," *IEEE/ACM Trans. Netw.*, vol. 21, no. 2, pp. 373–382, Apr. 2013.
[36] N. Provos *et al.*, "The ghost in the browser analysis of Web-based malware," in *Proc. HotBots*, 2007, pp. 1–9.
[37] F. D. Sahneh, C. Scoglio, and P. V. Mieghem, "Generalized epidemic mean-field model for spreading processes over multilayer complex networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 5, pp. 1609–1620, Oct. 2013.
[38] A. Sard, "The measure of the critical values of differentiable maps," *Bull. Amer. Math. Soc.*, vol. 48, no. 12, pp. 883–890, 1942.
[39] P. Van Mieghem, "The N-intertwined sis epidemic network model," *Computing*, vol. 93, nos. 2–4, pp. 147–169, Dec. 2011.
[40] P. Van Mieghem and J. Omic, "In-homogeneous virus spread in networks," *Mathematics*, vol. 17, no. 1, p. 1– 14, 2013.
[41] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, Feb. 2009.
[42] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, "Epidemic spreading in real networks: An eigenvalue viewpoint," in *Proc. IEEE SRDS*, Oct. 2003, pp. 25–34.
[43] P. Weng and X.-Q. Zhao, "Spreading speed and traveling waves for a multi-type SIS epidemic model," *J. Differ. Equ.*, vol. 229, no. 1, pp. 270–296, 2006.
[44] M. Xu, G. Da, and S. Xu, "Cyber epidemic models with dependences," *Internet Math.*, vol. 11, no. 1, pp. 62–92, 2015.
[45] M. Xu and S. Xu, "An extended stochastic model for quantitative security analysis of networked systems," *Internet Math.*, vol. 8, no. 3, pp. 288–320, 2012.
[46] S. Xu, "Cybersecurity dynamics," in *Proc. Symp. Sci. Secur. (HotSoS)*, 2014, pp. 14-1–14-2.
[47] S. Xu, "Emergent behavior in cybersecurity," in *Proc. Symp. Sci. Secur. (HotSoS)*, 2014, pp. 13-1–13-2.
[48] S. Xu, "Cybersecurity dynamics," in *Proactive and Dynamic Network Defense*, Z. Lu and C. Wang, Eds. New York, NY, USA: Springer, 2019.
[49] S. Xu, W. Lu, and H. Li, "A stochastic model of active cyber defense dynamics," *Internet Math.*, vol. 11, no. 1, pp. 23–61, 2015.
[50] S. Xu, W. Lu, and L. Xu, "Push- and pull-based epidemic spreading in arbitrary networks: Thresholds and deeper insights," *ACM Trans. Auto. Adapt. Syst.*, vol. 7, no. 3, pp. 32-1–32-26, 2012.
[51] S. Xu, W. Lu, L. Xu, and Z. Zhan, "Adaptive epidemic dynamics in networks: Thresholds and control," *ACM Trans. Auto. Adapt. Syst.*, vol. 8, no. 4, p. 19, 2014.
[52] S. Xu, W. Lu, and Z. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 30–45, Jan. 2012.
[53] L.-X. Yang, P. Li, X. Yang, and Y. Y. Tang, "A risk management approach to defending against the advanced persistent threat," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2018.2858786.
[54] L.-X. Yang, X. Yang, and Y. Y. Tang, "A Bi-virus competing spreading model with generic infection rates," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 1, pp. 2–13, Jan. 2018.
[55] X.-Q. Zhao, J. Borwein, and P. Borwein, *Dynamical Systems in Population Biology*. Cham, Switzerland: Springer, 2017.
[56] X.-Q. Zhao and Z.-J. Jing, "Global asymptotic behavior in some cooperative systems of functional differential equations," *Can. Appl. Math. Quart*, vol. 4, no. 4, pp. 421–444, 1996.
[57] R. Zheng, W. Lu, and S. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proc. Symp. Bootcamp Sci. Secur. (HotSoS)*, 2015, pp. 2-1–2-12.
[58] R. Zheng, W. Lu, and S. Xu, "Preventive and reactive cyber defense dynamics is globally stable," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 2, pp. 156–170, Apr./Jun. 2018.

ZongZong Lin received the B.S. degree in mathematics from Zhejiang Normal University, Zhejiang, China, in 2014. He is currently pursuing the Ph.D. degree in applied mathematics with Fudan University, Shanghai, China. His current research interests include dynamical systems, cybersecurity dynamics, and neural networks.

Wenlian Lu (M'09–SM'15) received the B.S. degree in mathematics and the Ph.D. degree in applied mathematics from Fudan University, Shanghai, China, in 2000 and 2005, respectively. He was a Post-Doctoral Fellow with the Max Planck Institute for Mathematics in the Science, Leipzig, Germany, from 2005 to 2007, and a Marie-Curie International Incoming Research Fellow with the Department of Computer Sciences, University of Warwick, Coventry, U.K., from 2012 to 2014. He is currently a Professor with the School of Mathematical Sciences and the Institute for Science and Technology of Brain-Inspired AI, Fudan University. His current research interests include neural networks, cybersecurity dynamics, computational systems biology, nonlinear dynamical systems, and complex systems. He has served as an Associate Editor for the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS since 2013 and *Neurocomputing* from 2010 to 2015.

Shouhuai Xu received the Ph.D. degree in computer science from Fudan University. He is currently a Full Professor with the Department of Computer Science, The University of Texas at San Antonio. He is also the Founding Director of the Laboratory for Cybersecurity Dynamics. He coined the notion of cybersecurity dynamics as a candidate foundation for the emerging science of cybersecurity. His research interests include the three pillar thrusts of cybersecurity dynamics: first-principle cybersecurity modeling and analysis (the x-axis, to which the present paper belongs); cybersecurity data analytics (the y-axis); and cybersecurity metrics (the z-axis). He co-initiated the International Conference on Science of Cyber Security (http://www.sci-cs.net/) and the ACM Scalable Trusted Computing Workshop. He is/was a Program Committee Co-Chair of SciSec2019, SciSec2018, ICICS2018, NSS2015, and Inscrypt2013. He is/was an Associate Editor of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.