Toward a Self-Adaptive Cyberdefense Framework in Organization

Kuan-Jui Huang1,2 and Kuo-Huie Chiang1

Abstract
Organizations suffer more than ever from the inability to securely manage the information system, despite their myriad efforts. By introducing a real cyberattack of a bank, this research analyzes the characteristics of modern cyberattacks and simulates the dynamic propagation that makes them difficult to manage. It develops a self-adaptive framework that through simulation, distinctly improves cyberdefense efficiency. The results illustrate the discrepancies of the previous studies and validate the use of a time-based self-adaptive model for cybersecurity management. The results further show the significance of human and organizational learning effects and a coordination mechanism in obtaining a highly dependable cyberdefense setting. This study also provides an illuminating analysis for humans to position themselves in the collaborations with increasingly intelligent agents in the future.

Keywords
cybersecurity, multiagent systems, actor model, self-adaptive systems, human–machine collaboration

Introduction
A London graph server took control of 41 automatic teller machines (ATMs) from 10,000 kilometers away to dispense cash to waiting bagmen at 22 different branches. Without ATM cards, passwords, or the ATMs ever being touched, the cash was automatically allotted to the money mules at the scheduled time. This real cyberattack occurred in Taiwan in 2016. The criminals stole more than NT$83 million (US$2.5 million) in a few hours, and the international syndicate was based far away in Russia. The syndicate used this method to launch coordinated attacks that stole millions of U.S. dollars in a few years. In addition to Taiwan, other affected regions included Britain, Estonia, Malaysia, the Netherlands, Poland, Russia, Spain, and Thailand (Ferry, 2017; Huang, 2016). This cyberattack was initially confusing because the victim bank not only is a state-owned cyber-secure model but also has ISO 27001 and ISO 20000 dual certification, which indicates that it has implemented necessary security such as antivirus software, an intrusion detection and prevention (IDP) system, and advanced firewalls and has also conducted periodic cyberattack exercises. Even its third-party information security auditing was inspected every year by authoritative professionals. Although the intrusion might have hidden in the system for a long time and collected all required data for its “D day,” the relevant files were not recognized as harmful until the police traced the attacker’s activities and classified them as mutated malware. Intranets, traditionally considered secure and closed, are designed for limited communication with reliable connections. But in this case, they became paths of invasion and even help malware spread to another isolated, closed network—the ATMs. For system architects, the aforementioned infiltration clearly revealed a serious warning sign: the intrusion successfully penetrated the closed environment and then acquired sufficient privilege to learn the system’s hierarchical structure, and deceived the monitoring mechanism to engage in more espionage activities. Throughout this time, it remained unnoticed. At least three lessons can be learned from this attack. First, the many preventive measures put in place by professionals in the financial system did little to resist today’s intelligent cybercriminals. Second, even a closed system was not immune to cyberattack or system vulnerability. Third, without the occurrence of such attacks, people would not be conscious of hidden adversaries.

This type of attack is triggered by an advanced persistent threat (APT), which exploits vulnerability and employs various techniques to penetrate a system at a slow pace and hide for a long period to get high system privileges (Cole, 2012). Cybercriminal organizations with members with high intelligence and comprehensive skills may seek preys from anywhere in the world, attempting to penetrate the information

1National Chengchi University, Taipei
2National Taiwan University, Taipei

Corresponding Author:
Kuan-Jui Huang, Department of Management Information Systems, National Chengchi University, Taipei 11605, and Department of Electrical Engineering, National Taiwan University, Taipei 10617.
Email: guanruey@icloud.com
and communications technology (ICT) systems of these valuable targets. As long as cyberdefense mechanisms of these targets are not strong enough, they are likely to become the next victims of these sophisticated attacks.

To confront modern cyberattacks, this article presents an interdisciplinary study that melds organizational learning, epidemiology, artificial intelligence (AI), distributed computing, and control theory to advance organization adaptability to cyberattacks. It first exemplifies and summarizes the characteristics of modern intelligent cyberattacks and then discusses and simulates malware propagation using the concept of an epidemic as an analogy. Through the anatomy of a dynamic process, this article explains the deficiency and inapplicability of non-temporal, static analysis in the cyberdefense decision-making. It develops a distributed self-adaptive framework in simulation and distinctly improves the efficiency of cyberdefense. By extending from the simulation results, this research contemplates the significance of learning effects and the human–machine collaboration by incorporating the dynamic configuration into a fault-tolerant distributed cyberdefense framework that is new to the literature.

The remainder of this article is organized as follows: In next section, “Challenges forthcoming” depicts the characteristics and challenges of modern cyberattacks and brief overview of literature and research gaps. Section “Dimension of cyberdefense” describes cyberdefense layers with detection, recovery, and immunity functions. “Methodology” section illustrates the detail modeling and simulation of the malware propagation. “Discussion” section summarizes the findings from the simulations, identifies the discrepancies of past studies, and deduces the self-adaptive cyberdefense framework. In the final section, it concludes the research with the limitation and future directions.

As modern cyber threats mostly derive from cyberspace, this article uses the term “cyberattack” as a general term to include similar intrusions and vulnerability exploitations. Computer viruses are only parts of malicious software in a strict sense, although in many cyberattacks, “virus infection” usually becomes general terms that summarizes intrusive behaviors from worms, Trojan horses, ransomware, backdoor programs, or other malicious software. In this article, these harmful programs or automation scripts are collectively referred to as malwares and their active subroutines are named as “virus,” which can be detected, immunized, and recovered through certain methods.

**Challenges Forthcoming**

In the earlier stages of information technology, the situation appeared to be simpler: Engineers designed systems to work for people, efficiency and effectiveness were the priorities, and any other functions or mechanisms that could decrease the performance or usability of the system were neglected. As these systems were in a closed form managed only by a few persons who knew certain procedures, protection issues were much simpler and required only an examination and restoration of functionality when necessary. Infiltration suspects were easy to recognize because every login could be traced back to a limited set of operators. In this era, most conditions in the computer world were predefined and predictable, and anomalies were manifest. However, the situations became different after the late 1980s. The evolution of communications technology and the internet boom meant that information security was no longer an independent issue in a standalone system. Currently, people face new battles in which the operating environments are too complicated, and the antagonists are too smart and too fast.

**Undefined, Unprecedented, and Unstoppable Threats**

Global interconnectivity has enhanced the convenience of data-sharing and has led to the rapid spread of cyberthreats. The outbreak of modern cyberattacks, similar to powerful contagious epidemics, could infect global computers in just several hours and paralyze them instantly. Most cyberattacks use automatic and recursive programs to find, test, and penetrate systems with no regard to the size or types of organization. In the 2018 Global Risk Landscape (Collins et al., 2018), cyberattacks and data fraud or theft were listed as top risks with a high impact and high likelihood. Juniper’s report (Moar, 2018) predicted that from 2018 to 2023, the global estimated cost of cybersecurity might exceed US$9 trillion, and nearly 3 billion records could be exposed by criminal breaches per year. It is no news that cyberattacks intrude into seemingly secure cyber spaces or infrastructures to steal intellectual property, acquire unauthorized access, or implant malicious processes for political or business purposes.

**Associative Architecture With Reciprocal Effect**

From a microcontroller that is designed as a self-contained device for specific purposes to a large system that serves complex coordinated functions, a complete system is often integrated from many subsystems. It is nearly impossible to ensure security as the top priority in the entire supply chain or to ask for everyone’s responsiveness to all vulnerabilities in a timely manner. The trade-off between convenience and risk often challenges engineers. The tight schedules of product launches and the reality of resource allocation to function-oriented services often prioritize fast iterations. In fact, even without concerns about economic returns, it is currently more difficult to design a 100% secure ICT system than it was in the past. In the First Bank ATM heist, the intrusion was from a London offshore subsidiary server that then controlled the ATM patching software. The malware was then implanted into the ATM software during updating and allowed the hackers to control ATM subroutines and to ask the machines to dispense deposited cash. The cybercrimes investigator stated, “Banks have been paying many attention
to account data, particularly in regard to account transfers, but not to the physical ATM.” (Ferry, 2017). In this case, the missing links clearly became the breaking points.

**Ubiquitous and Invisible Threat**

No news might not be good news. Some vulnerabilities are rarely known but have been exploited by hackers; some are known but are not repaired. A zero-day vulnerability is a typical case, which refers to an attack that occurs after a weakness is discovered and publicized; as the developer has no time to fix it, it could become a new weakness to be exploited. As Figure 1 depicts, during stages (a), (b), and (c), people need to defend themselves because there is not yet an effective packet release. Obviously, traditional antivirus protection is useless at these stages, and the situation will worsen until stage (d), when it becomes the job of system administrators and users to install updates. After the confirmation of update completeness at stage (e), the threat should be cleared. Resisting a zero-day threat is normally a long struggle and may last months. In fact, long wait-times for improvements are well known in cybersecurity. It took 10 years for transport layer security (TLS) to evolve from version 1.2 to 1.3 (lasting until 2018) despite version 1.2 being found to be vulnerable to many flaws during that period.

![Figure 1. Zero-day threats lifespan: (A) Few know, (B) Many know, (C) Window period, self-defense period, (D) Update is available, and (E) Update is implemented. Note. The threat lasts longer than expected.](image)

**Structural Weakness**

Vulnerability can result from infrastructure design and the inherited complexity of computer architecture and networking. The internet, the contraction of interconnected networks, was preliminarily designed for packet switching among reliable members and trusted environments. These credible members, called the autonomous system (AS), adopted the border gateway protocol (BGP) to find one another and form the global internet. However, BGP is vulnerable to deliberate behavior or manipulated pathways. Advanced criminals may change the interdomain routing table or purposely (or accidentally) advertise new paths to become a strong intermediate AS, which enables them to hijack the original routing, truncate and alter this path. The threats in this example are referred to as “eavesdropping” and “man-in-the-middle,” which can cause the leakage of nonencrypted payloads. With this type of unauthorized iteration, which may be combined with serial coordinated attacks, endpoint systems are hardly aware of being penetrated. BGP hijacking is a typical example of native vulnerability that is not well known by end users. These attacks are often undertaken by larger groups with strong computing resources or a powerful infrastructure for reasons of politics (such as content censorship) or finance (such as cryptocurrency mining interception). Unfortunately, these types of attacks and similar higher-level attacks from more powerful users, such as state-sponsored groups or even some governments themselves, are not rare.

**Human Weakness**

Human-related factors can make this situation even more challenging. A system is no stronger than its weakest link (Jacobs, 2015), and humans are regarded as the least-dependable component in any system dedicated to ensuring the
security of an organization’s assets. Therefore, effective cybersecurity screens must address the human factor. Compared with malware-based attacks, social engineering is viewed as the shortest path for cyberattackers to penetrate a system or steal credentials. Social engineering tactics such as phishing, vishing, and impersonation using counterfeit identities, take advantage of human psychological or physiological weaknesses. The intrusion in the First Bank case originated from a phishing email with questionable Office attachments from a seemingly reliable sender. The London branch administrator worked as usual and accidentally clicked on an infectious email, which instantly opened the door to other systems.

**AI-Powered Cyberattacks**

AI-powered cyberattacks refer to the sophisticated penetration triggered or spread by context-specific malicious logics to exploit system vulnerabilities. An AI-enabled distributed denial-of-service attack could switch on new attack-initiating sources or mimic normal users to incessantly request services. The AI-powered impersonation mingled with the exploited vulnerability by the APT mode could lessen the alertness of existing defense systems. An implanted enhanced analyzing program could integrate system activity information, authorization directories, and user behavior patterns among related infrastructure for further exploitation.

**New Spectrum of Cyber War**

The battle extends to the entire line. Traditionally selected victims are often people without an awareness or alertness of intrusion patterns, which means that people with training or expertise tend to be immune to most cyberattacks. However, new sophisticated attacks by APT mode can be invisible during intrusion, undetectable during system compromising and data leaking. The period required to successfully find countermeasures may be unpredictable. Even the digital forensics may face unprecedented challenges due to the characteristics of big data, accompanying heterogeneous and distributed environments (Caviglione et al., 2017). Modern cyberattacks are too fast, delicate, and inclusive for humans. This situation will inevitably influence the defense strategy if we consider multiple scenarios altogether.

**Related Works**

Researchers and practitioners have been committed to strengthening systems through security engineering and enhanced defense-in-depth mechanisms (Cybenko et al., 2014). However, most of these kinds of defensive methods are static and may be disrupted by continuous penetration, or they may not be able to discern new attack types. In view of the shortcomings of static defense measures against unknown attack types, adaptive cyberdefense is a new research direction being raised in recent years, which aims to contain active threats, make the target of attack smaller, and response to an attack quickly (Montasari et al., 2018). Related techniques such as adaptive scoring (Amini et al., 2015), randomized compiling, dynamic virtualization, workload and service migration, and system regeneration (Jajodia et al., 2011) are proposed to help update the validation engine, maintain secrecy of system settings, slow down the speed of being penetrated, or increase the difficulty of being compromised. Nevertheless, facing mass deployment of modern ICT systems, such as the management of end-point devices in global enterprises, the issue of scalability raises new challenges to cybersecurity management. Self-adaptive security systems with adjustable defensive strategies is then developed and becomes an applicable solution to cover scalability issue in detecting and mitigating unforeseen threats (Tziakouris et al., 2018). The literature on self-adaptive cyberdefense covers research scope of self-configuration, self-healing process, self-protecting, and self-optimizing (Chigan et al., 2005; Ghosh et al., 2007; Salehie et al., 2012; Salehie & Tahvildari, 2009; Yuan et al., 2014; Yuan & Malek, 2012). Researchers in this field further suggest that topology awareness is the key to support adaptive cybersecurity, adaptive privacy, and adaptive digital forensics (Pasquale et al., 2014). Mastering the topology allows the defense mechanism to better manage the dynamic complexity of the system, which also means that the challenges and complexity of managing modern cybersecurity come from nonstatic uncertainty.

Even so, the distinction between adaptive cyberdefense and legacy static strategy is still very blurred for organizations. Literature does not elaborate on the fundamental reasons why traditional static strategies cannot be applied to new types of cyberattacks but only put forward intuitive conclusions and directly designed a set of dynamic strategies for certain hypothetical contexts or specific architecture layers. Probably due to this lack of effective systematic and pragmatic explanations, coupled with the almost invisible activity of malware transmission and the way it is contained, organizations are more confused than ever on the effectiveness, applicability, and operating principles of various cyberdefense approaches. Hence, a clear and concise generic framework of cyberdefense strategies should help organizations understand the nature of cyber threats and develop effective defense mechanisms to deal with increasingly powerful cyberattacks.

This research aims to these purposes. It uses simulation methods to observe the spread of highly contagious malware in different organizations, in an attempt to understand the interaction between defense mechanism and malware propagation, thereby proving the superiority of the dynamic adaptation structure. During the simulation, this research further introduces a learning variable and obtains more satisfactory results from the proposed self-adaptive cyberdefense framework. Main contributions of this article are threefold. It
incorporates interdisciplinary domains including epidemiology, AI, distributed computing, and control theory to cybersecurity research, and justifies the existence of system dynamics property in such a framework. It proves the importance of learning effects in distributed multiagents, and it illuminates the collaborative interaction model between human and machine in self-adaptive cyberdefense.

**Dimension of Cyberdefense**

A cyberdefense system can be seen as an integrated system used to oppose cyberattacks and that can provide organizations with a justifiably trusted service through detection, mitigation, and prevention. To achieve these goals, we need a chain of defense mechanisms. Inspired by biological system, literature indicates that the adaptive defense system should be distributed and multilayered with pattern recognition, protection, and immunity (Dasgupta, 2007). The immune system provides an intrusion barrier, which may come from the original protection mechanism that is sufficient to resist general damage, or it may be acquired and effective only in specific situations. The pattern recognizer identifies abnormalities that pass the immune system and generates signals to activate protection mechanism. Protection system assists in eliminating or neutralizing damages and gradually evolves the immune system. From perspective of ICT systems, these layers respectively represent functions of detection, recovery, and immunity.

**Detection**

The detection is the inception of the cyberdefense system. For this purpose, an antivirus process undertakes a virus check or packet filtering at which point the IDP and firewall match the characteristics of classified anomalies. Some modern on-premise solutions equip limited learning capability to adapt to mutant viruses or suspicious activities. However, an organized attack can learn how to pass these thresholds through processes such as the reduction of data transmission at a low and slow velocity. In that case, none of the activities will be deemed to be intrusions. This is how a smart invasion attempts to present itself as a normal process and acquires higher authorization to cover its further actions. Thus, the detection could be difficult as there could be thousands of processes working simultaneously. These processes, regardless of whether they are good or bad, are indifferently deemed to be normal. They will thus remain in place until the guardian upgrades its discrimination (or until D-day arrives).

When the vulnerability remedial measures or virus signatures are available, by updating the software and scheduling complete scans, we can detect anomalies and take action. These procedures to counter ordinary attacks are somewhat effective and easy to implement. A higher check frequency leads to earlier discovery of vulnerability and triggers the repairs that follow.

**Recovery**

Compared to the past, recovery issues are more complicated due to the topology in cyberspace and malware polymorphism. A full recovery from a cyberattack by a single system scan is no longer a guaranteed result. Recovery patches can be left unresolved due to unconsciousness on the part of developers or the difficulty involved. Even worse, re-infection might occur because of incomplete decontamination. Under such circumstances, not every found vulnerabilities can be sterilized in each round. The recovery chance affects not only the system itself but also the probability of infection to other systems.

**Immunity**

In organic bodies, an immunogen must be recognizable as a nonself-component by the antibody to stimulate the immune mechanism and create a memory cell. A computer immunity system is also divided into innate immunity and adaptive immunity. Innate immunity, which is normally provided by the operating system or infrastructure, is a self-protection mechanism that limits abuse or system failure. Adaptive immunity is acquired from countermeasures to specific attacks. These subroutines often help systems to defend or mitigate attacks and create long-lasting memory in systems such as a vaccination for defense malware. Occasionally, mutant malware can reverse-develop resistance and render such protective subroutines ineffective.

Immunity is a complex issue. The literature (Forrest et al., 1997) has proposed the principles of computer immunology as: multilayered, distributed, diverse, sensitive, and with inexact matching, which involve the management of dependable distributed system. An important feature of cyberattack immunity is its pairwise relationship, similar to antigens and antibodies, which means that there is no cure-all for all situations. Most prescriptions only provide adaptive immunity to specific threats. Therefore, the likelihood of attaining resistance is probabilistic.

**Methodology**

To better understand the malware propagation and determine the proper countermeasures for a quick recovery, this article adopts a stochastic simulation with math modeling through epidemiology, actor model, and control theory.

**Modeling**

To constitute a conceptual protection screen, the outside-in oriented perspective begins with the segregation of malicious packets, recognition and protection of known malware, awareness of misbehavior and handling of malware; from the inside-out perspective, these steps map to the immune system, the recovery system, and the detection
system. The portrayed cyberdefense system with a hierarchical structure is illustrated in Figure 2. The variables of “Virus Check Frequency,” “Recovery Chance,” and “Gain Resistance Chance” are parameters to be used for the subsequent simulation.

To observe the property of malware propagation, we choose the commonly used models for simulation: The Agent-based Modeling (ABM), the Erdős–Rényi Network, the Compartmental model of epidemics and the Monte Carlo method.

First, cybersecurity is a monolithic issue in organizations that covers the collective behavior of individuals under a given set of rules. ABM handles the collective behavior of autonomous entities and addresses emergent phenomena whereby the whole is more than the sum of its parts (due to interactions) (Bonabeau, 2002). The components of ABM include agents and the environmental topology. Second, for the topology design, we need a model that satisfies a probabilistic setting because modern organizations have different internal social network topologies. The Erdős–Rényi model (ER model) provides a good universality of equal probability $p$ in $G = (N, E)$:

$$\begin{align*}
N_p^E (1 - p)^{\binom{N}{2} - E}
\end{align*}$$

where $N$ and $E$ denote the vertices and edges of graph $G$, respectively. Applying the ER model in each scenario helps control the equal probability of the various connections. The compartmental model from epidemiology (Kermack & McKendrick, 1927) is generally used to describe a disease (analog to a computer virus) that is spread under various situations whose basic form is a susceptible-infectious-recovered (SIR) model, which presents the healthy status on an agent-based system at each time $t$. The mode used here is without vital dynamics (without the factors of birth-join and death-leave), and the immunity state $M$ is lifelong for specific malware. Then, for all nodes $i \in \mathbb{N}$, the SIR model can be represented as follows:

$$\begin{align*}
S(t) + I(t) + R(t) &= N \\
S_i(t) \Rightarrow I_i(t) \Rightarrow R_i(t) \\
R_i(t) \Rightarrow M_i \\
P(E_S \text{ or } E_I \text{ or } E_R) &= P(E_S) + P(E_I) + P(E_R)
\end{align*}$$

where $E_S, E_I,$ and $E_R$ are the events of the states $S(t)$, $I(t)$, and $R(t)$, respectively, which represents the number of each state at time $t$, and $N$ is the number of nodes. Eq. 2 implies that we need to acquire only the relationships of either two of the three variables during analysis. Eqs. 3 and 4 depict the
trajectory of the state transition with a probability of $\beta$, $\gamma$, and $\delta$ under the respective impedance factors of $\Omega$. Eq. 4 means that the recovered node has a probability of $\delta$ to acquire time-invariant immunity $M$ for node $i$. Eq. 5 shows that $E_s$, $E_i$, and $E_p$ are mutually exclusive. Eqs. 6 to 8 are the ordinary differential equations of the SIR model.

The Monte Carlo method is commonly used in epidemiological studies and social network analyses. It uses repeated random sampling to approximate solutions to optimization where physical experiments are impractical. The Monte Carlo simulation has been shown to be able to quantify the sensitivity and uncertainty in nondeterministic situations (Demirtas et al., 2017), describe the reality and provide the approximate solution in complex systems, which suits the simulation of the malware propagation in an organization.

The simulation algorithm is composed according to the above. As illustrated in Figure 3, initially, the profile of the simulated target is created, which determines the number of agents and average degree of them, the initial outbreak size, the virus spread chance, the virus check frequency, the recovery chance, and the gain resistance chance on a randomly generated topology based on ER model. Except for topology, these parameters are all controlled based on required scenarios. The simulations proceed as follows. The infected nodes first run function(CheckNeighborState) to check if neighbors are the Infected. If not, they use function(tryInfectingNeighbor) to change the state of neighbors to the Infected. If they succeed, the neighbors will become the infected seeds and follow the same pattern to find the other victims. This procedure will continue until all nodes are infected. Defense process also starts from function(CheckNeighborState). Once anomaly is found, function(tryRemovingInfection) will attempt to repair the Infected so as to change the state of node to the Susceptible. During the repairing process, there is a probability for nodes to acquire immunity by function(tryGainingResistance). Nodes will continue to experience function(tryInfectingNeighbor) and function(tryGainingResistance) according to virus check frequency. There is a threshold $\Omega$ in each state constraining transition probability $\beta$, $\gamma$, and $\delta$. For example, if a node’s recovery chance $\gamma$ is larger than $\Omega(R)$ for a node, it becomes recovered and changes the state to the Susceptible, accompanying further chance of becoming the Resistant. Otherwise, it remains the Infected until next check. The left side of Figure 3 is the protection mechanism of an organization, and the right side is the propagation of malware. The algorithm emulates the competition between both sides and attempts to find the time elapsed from the infection to full recovery.

Simulation Cases

The first case is from the organizational perspective to simulate the interaction of the three quantifiable parameters of the protection screen, specifically, “Virus Check Frequency,” “Gain Resistance Chance,” and “Recovery Chance” via social network analysis. The second case applies distributed intelligence to emulate the human–computer collaboration under circumstances of powerful cyberattacks.

Case I  

ABM on SIR model. In the first case, we simulate the First Bank APT cyberattack where the infiltration begins with victims of phishing mails so that the malware has implanted to scan the network topology of the organization in search of additional victims and spreading patterns. We borrow from Python (ABM) packages—Mesa (2016) and adapt NetLogo Library (NetLogo, 1999) for the Monte Carlo simulation. Netlogo is a generally used programmable modeling tool to simulate the interactions among nodes. Mesa is an integrated library for ABM in the python programming language.

The simulation is conducted as follows. Initially, we set the outbreaks of the virus to 10 nodes (10% out of 100 total nodes) and the virus spread chance to 100% to observe the highly contagious status. The edge degree of the nodes is tentatively set to 3, which represents that each node has three connectors in its social network on average. The simulations are implemented under these conditions with different levels of “Virus Check Frequency” (VCF), “Recovery Chance” (RC) and “Gain Resistance Chance” (GRC) until the termination criteria are met at $t(i) = 0$, which indicates that the infectious node is 0 at time $t$. There are eight combinations of configuration, and each one is run three times to acquire the medium value of the time elapsed $Y(I = 0)$, where $Y(I = 0) = (t_{f0} - t_0)$. $Y(I = 0)$ represents the full recovery time required (excluding the origin point). The detailed experimental configurations are exhibited in the Appendices.

Result. The simulation results are summarized in Table 1, which shows that when holding other conditions constant, the combination of any two controlled variables significantly decreases the time required to full recovery. Furthermore, as demonstrated in Figure 4, if we must choose two out of the three to expedite the recovery, then the most effective mix is the “Virus Check Frequency” (VCF) and “Gain Resistance Chance” (GRC). Further details of the evolving lifecycles and propagation topology are shown in Figure A1 in the Appendix.

To validate the consistency, we conduct the sensitive analysis as in Table 2, which shows an interesting consequence. In the range $10\% \rightarrow 30\%$, an additional investment in “VCF + GRC” seems to provide the most gains in shortening $Y(I = 0)$, while in the range $50\% \rightarrow 70\%$, another choice is “VCF,” and in the range $70\% \rightarrow 90\%$, the best strategy becomes “RC+GRC.” The optimal solution seems to drift according to organization cybersecurity preparation and maturity, and the second place competes intensely.

According to the simulation result, there has been at least one assertion that, although it is possible for organizations to successfully defend against certain cyberattacks by adopting
predefined methods, the best measure is uncertain. What worked in the past may not be the most effective in the future. This finding challenges the adequacy of a static strategy in cyberdefense, which assumes that a noncontingent solution to cyberattacks exists. It further challenges the economical modeling based on discrete effectiveness (Arora et al., 2004;
In fact, the propagation and consequences evolve too fast for a single investment to take effect, especially under APT or AI-powered cyberattacks that do not remain static without more exploitation. Their actions might be latent and unpredictable, and they will not alert us of their presence or of what they have done. The moment that we observe a phenomenon at time \( t_0 \) is only a derivative result of a time function from a manifold trajectory \( \Phi_t \), and the phenomenon might have relocated itself to another position at the moment that we make an investment decision at time \( t_1 \). Previous

Gordon & Loeb, 2006) as its performance duration is too short to ascertain.

Table 1. Recovery Time Required for Different Scenarios.

| Ind. Var.                      | Scenario                  |
|-------------------------------|---------------------------|
|                               | 4-1 and 4-2 | 5-1 and 5-2 | 6-1 and 6-2 | 7-1 and 7-2 |
| Virus check frequency (VCF)   | 10%         | 20%         | 50%         | 50%         | 10%         | 20%         | 10%         | 20%         |
| Recovery chance (RC)          | 50%         | 50%         | 10%         | 20%         | 10%         | 20%         | 10%         | 20%         |
| Gain resistance chance (GRC)  | 10%         | 20%         | 10%         | 20%         | 50%         | 50%         | 10%         | 20%         |
| Full recovery time required, \( Y(I) = 0 \) | 683         | 156         | 587         | 139         | 965         | 121         | 2,897       | 380         |

Note. The combination of any two controlled variables will decrease \( Y(I = 0) \).

Figure 4. Recovery speed of a mixed strategy.

Note. The “VCF + GRC” strategy (in orange) helps recover the soonest. VCF = Virus Check Frequency; GRC = Gain Resistance Chance; RC = Recovery Chance.

Table 2. Sensitivity Test at Different Stages.

| Increment of investment | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% |
|-------------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Range                   | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% |
| VCF                     | 75  | 42  | 27  | 30  | 42  | 52  | 29  | 0   |
| GRC                     | 19  | 29  | 58  | 56  | 29  | 22  | 24  | 21  |
| RC                      | 81  | 14  | 35  | 42  | 17  | 38  | 30  | 0   |
| VCF, GRC                | 89  | 72  | 68  | 64  | 42  | 44  | 29  | 33  |
| RC, GRC                 | 76  | 47  | 53  | 31  | 17  | 5   | 58  | 0   |
| VCF, RC                 | 87  | 50  | 40  | 33  | 0   | 42  | 14  | 8   |

Note. The best and the second-best strategy appear to be contingent on different increments of investment. VCF = Virus Check Frequency; GRC = Gain Resistance Chance; RC = Recovery Chance.
literature might be built on a different background of fewer cyber connections and a simpler context without sophisticated persistent attacks and has been inclined to insufficiently emphasize on the topology of dynamical systems, the uncertainty of measurement performance, and the fast transient states of malware, although some have sensed the necessities and attempted to rectify previous deficiencies (Nazareth & Choi, 2015). Unfortunately, it is not uncommon for organizations to frequently obtain proposals of single solutions to the syndrome that demonstrates the greatest need for them, contrary to how prescriptions for flu seldom contain only one curative effect.

This process is very similar to computer virus propagation and is widely used in cybersecurity studies (which is also well-known in epidemiology). Recall in Eqs. 6 to 8 that every state over time is affected by the number of the previous state and the transition coefficient. In this vein, the identification of infected nodes is the prerequisite condition to manage the recovery process, regardless of how it occurs. Similarly, under the SIR model, the node is first susceptible to a virus prior to being infected (thus, prevention from known vulnerability is the first line of defense), and it is recovered and immune from the infectious state. The SIR model provides fundamental explanation of the major epidemic pattern and is helpful to cybersecurity studies. Researchers then propose more extensions of the compartmental model such as SIRS and SEIR ($E = \text{exposed}$) to demonstrate more interim variations of the epidemic propagation.

Case 2

Adaptation model. Cyberattacks can be seen as cybersecurity system faults that are, either caused by the design incompleteness of a functional specification, implementation procedures, or changes in contextual thresholds. In Case 2, we consider inducing the self-adaptive mechanism to simulate the intelligent nodes (smarter agents) in addressing serious cyberattacks. We expand the actor model and adaptive control system to a distributed framework to determine if an organization equipped by concurrent computing agents will make more differences based on the same parameters as Case 1.

Distributed self-adaption. Modern cyberattacks are often distributed through multiple penetrating approaches. The extent of the damage among the distributed devices can be different according to various intrusion patterns. The literature thus applies self-adaptive systems to manage these threats. Beginning by setting protection scopes, the abnormal behavior can be monitored, analyzed, identified, anticipated, and isolated without much intervention of the centralized system administrator (Chen et al., 2014; Claudel et al., 2006; Dean et al., 2012; Qu et al., 2010). The distributed agents, if provided with proper decision capability, can monitor lower-level or front-line signals and react accordingly. The required abilities are not only the technical deployments but also the behavioral and managerial arrangement. To equip the distributed agents with suitable knowledge, this article borrows from the disciplinary domain of AI.

Actor model. The actor model (Hewitt et al., 1973), which originated from AI, is an abstract process of concurrent computing widely used in software programming, communications, and distributed operating systems. It helps distributed computing run smoothly without problems from a single point of failure (SPOF). Actors, which are equivalent to the aforementioned nodes or smart agents, are the primitive units and are responsible for different jobs. The key infrastructure for an effective actor model is a common interface for communication so that message transformation and job integration can be easily executed. The principles of the actor model are threefold: light job, independent decision, and message passing. The “light” principle indicates that as each actor owns limited resources, an actor must work efficiently on its assigned job. “Independent decision” represents the essence of a distributed multiagent system so that the actor should, at its discretion, determine its own next steps. “Message passing,” is the direct transmission of a message to predetermined actors.

These three principles collaboratively create a fault-tolerant mechanism that allows a system to continue its operation, even when some of the actors are in failure states. Fault tolerance mitigates the occurrence of a SPOF and helps foster the design of redundancy, which is fundamental to disaster recovery for modern systems. The three principles of the actor model make it effective for strong cybersecurity, especially under APT or AI-powered attacks, which either paralyze systems or impersonate users to spread malware.

Under these circumstances, a cybersecurity system might have to retain the most important property—availability—and sometimes retain it by sacrificing information integrity (or precisely, by searching for eventual consistency). The actor model specializes in fault tolerance and helps achieve this target. When there are many unreliable resources, a good distributed consensus algorithm among actors helps meet the distributed consistency. With smart agents, we still need a robust control system to orchestrate the cybersecurity framework.

Control system. Cyberdefense can be regarded as a control system. There are two types of control loops: open and closed. Systems that demands real-time or high responsiveness suit closed-loop control to environmental changes, such as autonomous cars or the autopilot on airplanes; systems that demand external signals for operation require open-loop control, such as most lighting switches (Chun et al., 2013). A distributed cyberdefense scheme should have closed-loop control with feedback information so it would be comparatively safe under threats or uncertainty. A typical closed-loop control process of cyberdefense is illustrated in Figure 5. It consists of a series of chain reactions of states. Intuitively, given that state $s$ is in a closed-loop,
That is, if $\exists \Delta_0$ degree of stability by limiting $\Delta$ to an oscillation amplitude. Then, $E(t)$ is the equilibrium solution to the asymptotically stable function $E(s)$ in Eqs. 12 to 15, $\eta$ acts as a bounded stable factor that provides a constrained probability (Willems, 2012) of the stochastic system $E(s)$ in $\Delta$.

From a management perspective, $\eta$ can be analogous to the learning rate of smart agents who have the mental buffer to judge the appropriate variables in partially controllable $C(s)$. Here, $C(s)$ is the Human–Computer interface to be managed by people.

Case 2 is formulated according to additional parameter $\eta$ and the controllable $C(s)$. To observe the effect of the learning rate, Case 2 becomes the treatment group, and Case 1 is the control group. As stated, there are three milestones in the trajectory: $G_1$ at $Y(R > I)$, $G_2$ at $Y(S > I)$, and a termination point $G_3$ at $Y(I = 0)$. Figure 6A to D illustrates their trajectories under different factors $\eta$. The blue line is indeed Case 1, where $\eta = 0$, that is, Case 1 is a limiting, special condition of Case 2.

Learning matters. We can observe from Figure 6A to D that $Y(I = 0)$ (time required to full recovery) is proportional to $1/\eta$, which means that when the agents are smarter, the recovery time is the shorter. Interestingly, from Figure 6C, we also observe that the intelligence levels contribute less to $Y(I = 0)$ under a strong “Gain Resistance Chance.” This implies that as long as the collective immune capability (as measured by the “Gain Resistance Chance”) is sufficiently high (in Figure 6C, GRC is set at 100%), we might then skip the factor of agents’ learning capability. If not, enabling them to learn can contribute to a safer environment. The effect of learning on stability is even significant in a more complex network. Under another experiment with $N = 500$ and edge $= 8$, the learning effects contribute to the improvements in the range from 28% ($\eta = 5\%$) to 68% ($\eta = 15\%$).
Discussion

Based on the experiments above, we abstract the findings and consolidate them into a unified self-adaptive framework.

Self-Adaptation Setting

In a control system, a self-adaptive scheme includes the four indicators of self-configuration, self-optimization, self-healing, and self-protection (Kephart & Chess, 2003). Autonomic systems can reconfigure and update themselves automatically according to high-level policies: they tune and upgrade themselves to obtain better performance, detect and repair local problems, protect themselves from attacks and perform graceful degradation when a large portion of functions is ineffective.

The simulations in this article cover the discussion of self-configuration, self-healing, and self-protection. In terms of optimization, we provide the referential weights, combinatorial effects, sequential order conditions, learning factor, stabilizer, and ratios of distributed deployment for constraint optimization. An agent-based model is used to simulate the complex, infectious, recovered, immune evolution of autonomous agents in an ER-modeled social network. In general, the discussed framework meets a high self-adaptive level of autonomy. The purpose of the two simulations is to obtain insights into an effective cyberdefense management framework under powerful cyberattacks.

Through multiple rounds of practical simulations and mathematical inferences, we conclude the following:

1. A distributed multiagent framework for cyberdefense, which can be layered by detection, recovery, and immunity, helps quick recovery in the classic SIR model. Adaptive autonomy will expedite this process.
2. The identification of infected nodes is the prerequisite condition to activate remediation and adaptive immunity.
3. The propagation of malware under the SIR model is a dynamic process. No static approach is able to produce a cure-all for all contexts.
4. The optimal strategy is contingent at least on the properties of organization and time factor.
5. A combination of strategies performs better than single strategies. (Cost efficiency is not discussed here.)
6. The golden cross-points (the turning points, as are elaborated in Figure A1) and the patterns that approaches them are worth exploring for time-dependent decision-making.

Figure 6. Learning effect with mix strategy on recovery.

Note. A complete resistance capability (GRC = 100%) might replace the importance of learning to some degree as 6(C) shows. Otherwise, the higher learning rate the agents possess, the shorter the recovery time requires. VCF = Virus Check Frequency; RC = Recovery Chance; GRC = Gain Resistance Chance.
7. Within a certain large range, distributed intelligence that applies to concurrent cyberattacks appears to be more efficient than centralized deployment. When the organization owns more complex topology, the self-adaptive framework appears to be more efficient.

8. The human factor could be relevant to stabilize the imperfect closed-loop controls. Learning helps increase the reliability of such systems.

These findings echo some cybersecurity practices. For example, the notorious DDOS paralyzes the service of a centralized system; however, it can be restrained by the distributed, multilayered defense framework of a Content Delivery Network (CDN) or a Domain Name Service (DNS). The findings also match some interdisciplinary theories such as self-adaptation in control theory, organizational learning (Cytt & March, 1963), and double-loop learning (Argyris, 1997). To extend the above to management insights, the following sections elaborate the related interfaces and components.

Contingency and System Dynamics

Contingency theory suggests the evaluation of multiple approaches to fit an organization (Van de Ven & Drazin, 1984). In our experiments, the dynamic property particularly indicates the relation between the time factor and organizational cybersecurity health because the propagation in motion changes the state of the nodes. Specifically, the determination of parametric weighting for decision-making should be a function of time, and a universal static setting throughout the entire process is not applicable to all conditions. Cybersecurity appears to be more resource-consuming than most organizations presume. The cybersecurity system is more than a one-time solution procurement, a policy statement, or an auditing system.

As discussed earlier, the probability of system awareness, recovery, or immunity is indefinite under modern cyberattacks. We can acquire the same evidences from the simulations. Let weights \( \omega_1, \omega_2, \text{ and } \omega_3 \) denote the strategic weight of “Recovery Chance,” “Check Frequency,” and “Gain Resistance Chance” at time \( t \). The objective is to minimize \( Y(x) \) by selecting optimal arguments. According to Case 1’s result, the suggested priorities for a single strategy under different learning factors are:

\[
\begin{align*}
\text{if } \eta &= 0, \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(R > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(S > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(I = 0)
\end{align*}
\]

else if \( \eta = 10\% , \)

\[
\begin{align*}
\arg \min_{\omega > \omega_i > \omega_j} & Y(R > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(S > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(I = 0)
\end{align*}
\]

else if \( \eta = 15\% , \)

\[
\begin{align*}
\arg \min_{\omega > \omega_i > \omega_j} & Y(R > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(S > I) \\
\arg \min_{\omega > \omega_i > \omega_j} & Y(I = 0)
\end{align*}
\]

We can learn from the above that in a dynamic propagation, the importance of each parameter in countering cyberattacks varies based on the time of observation. For example, when \( \eta = 10\% , \) to reach the first golden cross-point \( G_1 \) \((Y(R > I))\), organizations should be invested in recovery measures to shorten the time exposed to threats. However, if an organization has \( \eta = 15\% \) over a cyberattack, it can invest in gain resistance measures to arrive at \( G_2 \) earlier.

It can be seen from the simulation results that the spread of malware contains the property of system dynamics. Also, the result demonstrates that there is no panacea for all situations. Under intelligent cyberattacks, system administrator or end users can no longer easily perceive every system alteration. Humans should adjust their expectation that their systems are always clean, that intrusions or malware are easy to detect, and that once these anomalies are detected, they will be immediately and completely eliminated.

Luckily there are some symptoms, and clues such as the slowdown of connections or response, pop-ups or strange programs, abnormal crashes or event logs, among which some are not recognized as malware but can be classified as suspicious activities. Normally, these activities can be detected by a modern cloud-based endpoint protection system prior to being classified as cyberattacks, but the responsiveness depends on discretion of these subsystems. These self-managements can be collectively described as:

\[
g(t) = \sum_{j=1}^{n} \phi_j
\]

\[
G(t) = \sum_{j=1}^{N} g_j(t)
\]

where \( \phi_j \) is the dynamic verification process of the \( i \)th symptom of \( n \) known malware at time \( t \), \( g(t) \) is the self-configuration of an agent, and \( G(t) \) is the collective cyberdefense configuration in an organization. With \( G(t) \), we can estimate referential check points of \( G_1, G_2, \text{ and } G_3 \).
on dynamic propagation trajectory $\varphi$. Each agent should be inspected for various symptoms in each round of examination prior to prescription. For system administrators or intrusion analysts, when modeling, we should consider time-based functions such as an evolution function $\varphi'$ in manifold as the foundation upon which to conduct the analysis. After all, the permeation is continuous, wide, and diffusing along the organizational topology. This finding emphasizes the necessity of a contingency strategy in cyberdefense because a function of time carries continuous signals that are often nonlinear and requires multiple (integral) analysis over different regions. We should avoid evaluating the nonlinear function just at a single point. This also explains why no single parameter in experiments will always dominate the others and no investing scope should be predefined prior to system scrutiny. From viewpoint of research, we may instead suggest replacing linear optimization with dynamical systems or cybernetics models and solve them by simulation or soft computing. The time factor is central in cyberdefense, especially when counteracting intelligent cyberattacks. The longer cybercriminals are allowed to remain inside a system, the more information they will be able to collect.

### Distributed Autonomous Actor

Researchers suggest high-level strategies with local tactics reinforcement learning hierarchy for distributed applications (Atighetchi et al., 2004). Such cyberdefense structures deploy homogeneous computing units in heterogeneous systems (Rodriguez & Castillo, 2018) and can be symbolized as the work specialization and collaboration relationships in modern organizations. This area is still quickly developing. Some studies design information sharing systems as communication pools that are efficient but subject to a SPOF at the interconnector. An improved approach emulates social insect colonies that share data with distributed decision-making (Korczynski et al., 2016) by devising a coordination overlay network on closed-loop control nodes. The evolving paradigm of the distributed framework for dependable computing corresponds with the reasoning process in this research.

For modern cyberattacks, defense must occur on all fronts because every contact point could serve as a point of entry of threat or beachhead of recovery. This is another difference of contemporary cyberdefense that distinguishes it from past cyberdefense. In engineering, the actor model provides fault tolerance capability such as fail-safe architecture and the least-privilege principle (Open Web Application Security Project, 2015) to help defend against sophisticated exploitation. The agents under the actor model should be autonomous knowledge workers characterized by empowerment, computing, and communication. “Empowerment” refers to the realization and maintenance of the stability of a self-adaptive defense system; it improves the knowledge system and the routine policies of cybersecurity. Actors’ “computing” should be comprised of feedback, detection, controller, and process functions that help promptly and accurately find the optimal solution to cyber-attack features through the standard procedures and available referral systems. The “communication” characteristic posits that the organization should intrinsically retain the collective consciousness and discipline to handle the non-deterministic problems of cyber threats.

### Learning and Human’s Role

Learning is the newly found latent variable in this distributed framework. The learning factor ($\eta$) is inferred from mathematics and has been placed into the simulation in Case 2, which helps even an efficient recovery. This factor is an exogenous variable outside the chained control functions and relates to the discretionary adjustment by the controller of a closed-loop system (see Eqs. 12–15). Learning in an organization has been widely discussed in the literature, and this research justifies its reliability functionality for a self-adaptive cyberdefense system.

Through the engineering lens, the learning factor works as a stabilizer that levels down the spreading speed against infection through the enlargement of a tolerance buffer. It constrains the error function in Eq. 15 and the state transition function in Eq. 3, and it could incur recovery and obtain immunity through the closed-loop control process in Eqs. 9 to 11. This learning buffer is not typically included in the design of computer cyberdefense infrastructure; however, it is common in many other control systems. Learning to control the input by evaluating errors and adjusting the default set of configurations is essential, even in a highly automatic and sophisticated environment, such as power plants or spacecrafts. These context-specific systems must account for human interactions to judge the inability and inefficacy of systems from the anomaly.

This observation sheds light on the human role in future cyberdefense framework. Currently, people who face smarter intelligence first worry about being replaced or the lack of control over these automatic agents. Increasing AI capability exacerbates this anxiety. However, as long as the applicable intelligence is context specific, such as so-called weak AI in playing games or identifying objects, the human factor is just a key (although not the only key) to increase the system generalizability whether good or bad. Humans can act as generalists, managing the interfaces between these systems and making up for their lack of functionality.

AI in a largely explored solution space will become almost invincible to humans, such as the race with AlphaGo. Some predefined automatic processes help us perform tasks more efficiently. However, for these processes in a dynamic and irregular environment, their ability appears clumsy. The machine reinforcement learning process, if it is enabled in a
cyberattack algorithm, will be considerably hampered because of the innate immunity of most operating systems, in which the anomaly logs transmitted to system administrators and IDP systems, seldom leave alone such repetitive and immense chain function to find their next steps unless the entire system has been captured and been forgotten. Cyberattacks can be powered by AI and human collaboration; however, it is impractical to exaggerate the capability and efficiency of pure machine-based intrusion into a large system.

Similarly, the predefined closed-loop controls of cyberdefense systems are expert systems within specific contexts. They can be specialists in endpoint protection, identity authentication, or software integrity verification, but they are still not generalists. A combination of several specialists still demands a strong generalist to obtain coherence, to coordinate and to control. Closed-loop controls can be regarded as powerful tool sets for a specific purpose, which can be the sufficient and/or necessary condition for other loops. Combining and integrating many closed-loop systems increases their applicability. However, we are still far from creating strong AI in the exhausted context of malware. Thus far, the plotting of large-scale DDOS or the sophisticated First Bank robbery that involves algorithmic computation is controlled by humans. AI simply aggravates the exploitation efficiency.

Effective learning. There has been a plethora of materials to teach people how to identify and react to vulnerabilities. Nevertheless, partially due to the technical involvements, the extent of the acceptance and adoption of correct cyberdefense should include both operational learning, in which one learns the procedures to securely use and control the system, and conceptual learning, which facilitates one’s understanding of the logical structure and basic principles. The lack of opportunities to practice with real cybersecurity events is another inevitable difficulty. Organizations will seldom face a continuous red alert of fatal cyberattacks where everyone must mobilize, and this hinders practical experiments and situated learning because of attenuation-of-stimulus effect (Allenmark et al., 2015) and the decay of working memory (Portrat et al., 2008). Therefore, the attentive and periodic rehearsal, meaning making and acceptance management should not be underestimated.

Double-Loop Reinforcement

An effective self-adaptation framework of cyberdefense may consider a double-loop reinforcement cycle on the organizational configuration of cyberdefense: one loop of global introspection and improvement capability (i.e., the improving loop, represented here by $\xi(s)$) to adapt various feedback from subsystems, and one loop to perform light jobs stably and quickly (i.e., the implementing loop, represented by $\tau(s)$). An entity is in the implementing loop if it executes the predefined cybersecurity procedures of a specific context, whereas it can sometimes account for the coordination mechanism in the improving loop. A self-adaptive cyberdefense system strives to minimize the recovery time with the implementing loop and to maximize the reflection effect with the improving loop alongside the propagation trajectory. The objective function of the reinforcement learning cycle can be depicted as:

$$\max_{\xi} \min_{\tau} G(t)$$

where $G(t)$, which is the same as in Eq. 18, is the group self-configuration function at time $t$.

External loop. One problem of closed-loop control is the local optimal. Generally discussed cyberdefense practices focus on the closed-loop functions—especially on the competency of the effective responsiveness from technical solutions such as the IDP, firewalls, or antivirus software. These measures are effective for signature-base cyberattack detection and recovery, and they contribute to limited immunity. However, considering advanced cyberattacks, the solutions are inevitably trapped in the dilemma of false positive and true negative after a period of time; eventually, they are likely to overreact to suspected symptoms and be disabled by humans. This situation would require the incorporation of information and solutions from the even larger external loops toward self-configuration.

The external loops can be constituted by government security agencies, antivirus solution providers, or security forums that provide useful and noteworthy information on cybersecurity development, which can help organizations with referential actions or self-examinations. Joining such a related community or activities to learn about state-of-the-art development, updated weakness and threat databases, unreliable third-party services, possible intrusive approaches and countermeasures, can provide organizations with information gains to operate the control loop of protection from general cyberattacks. These connections relate to the organizational learning factor ($\eta_o$) which attributes to the adaptability of an organization to the outer world. They also assist adaptive immunity with the help of third-party solutions
such as context envisaging and symptom diagnosis. For adaptability, organizational learning appears to be important in the entire framework. The optimal strategy empowered by learning capability can be expressed as:

$$\omega^t_\eta = \arg \max_{\eta} \max_{t} \min G(t)$$

where \(\omega^t_\eta\) is the weight matrix of the parameters at time \(t\) which offers an effective strategic planning of resources. \(\eta\) are the coefficients of organizational and individual learning, respectively. Eq. 19 can be customized with more constraints for contextual optimization for organizations.

The study on the importance between \(\eta\) in cybersecurity requires more evidence under different organizational settings, and we can conjecture that an internalization process and epistemic structure is necessary. In general, exogenous innovation is more time-consuming to take effect than an internal process. Therefore, organizations without much exterior resources can still make a difference by arranging inner reinforcement learning cycles for a cyberdefense framework.

### Self-Adaptive Framework

Accordingly, a self-adaptive cyberdefense strategy comprises individual learning on its controllable defense elements and appropriate implementation to minimize the exposure duration of vulnerability. On one hand, organizations should maximize such capability by continuous introspection and providing reinforcement learning feedback; on the other hand, organizations should bridge external innovative resources and trigger knowledge internalization. Above all, these approaches should adapt to the patterns of malware whose characteristics can be contingent on the moment of observation and require continuous monitoring and verification. The self-configuration \(G(t)\) can be enhanced by self-healing and self-protection and reinforced by self-optimization, as shown in Eqs. 18 and 19.

The illustration of a self-adaptive cyberdefense framework is demonstrated in Figure 7. The implementing loop and improving loop run well separately and incorporate in a double-loop reinforcement learning cycle. The innovation loop enhances an organization’s adaptability according to innovation adoption and knowledge internalization through the improving loop and the implementing loop. This framework contains elements of high dependability that oppose cyber threats from operational error, design failure, and systematic incompleteness.

In a rapidly evolving environment, organizational activities occur concurrently in various areas. Without an implementing structure near the front and feedback for improvement, it is difficult for organizations to respond in time and create an organic, self-reinforcing mechanism. In addition, an effective cybersecurity mechanism cannot be built without considering human learning problems, including at both the individual and organizational levels. Humans in an organization have both individuality and conformity characteristics, and their interactions often cause time latency (Forrester, 1994; Senge, 1991), that affects the efficiency of addressing cyberattack and arouses structural inertia, which disables the sensitivity of extraordinariness. Accordingly, an introspective loop that links to the mental model of the reinforcing cycle is suitable for a continuously improving organization.

Cybersecurity has been classified as national security or even in terms of the battle between good and evil. Organizations should draw lessons from primeval instincts that learn from informative collective wisdom and cooperate with others to survive cyberattacks (Axelrod & Hamilton, 1981; Cosmides, 1989; Ein-Dor, 2014), in addition to inhouse resource optimization. Self-adaptation keeps an organization innovative and synchronizing with the outer world where more cybersecurity energy gathers to supplement the capacity of a single entity.

### Coordination

Recall in Experiment 2 that, the distributed smart agents require a good distributed consensus algorithm to help attain consistency. This coordination assigns the cyberdefense tasks to a distributed multiagent system. Functionally, such assignment requires an interface among the loops, that is, the coordination mechanism that bridges communication processes. Flexibility is necessary for the allowance of control discretion. In a self-adaptive cyberdefense system, the coordination mechanism is explicit to ensure self-actuation and implicit to facilitate self-optimization. The self-reinforcing helps foster the structural virtuous cycle of continuous improvement. In this regard, routines and standardized norms are helpful. Routines are self-reinforcing and provide organizational flexibility whose process can be seen as a continuous learning cycle (Feldman & Pentland, 2003) within the improving loops. Norm management includes policies and procedures that entail specific technical processes, techniques, checklists, and forms (Cichoniski et al., 2012). Organizational norms should provide referential principles with contingent examples in response to quick adaptation.

A self-adaptive cyberdefense system contains many smart agents that can perform several independent closed-loop controls. The scenario of the distributed cyberdefense framework is a collaborative model where multiple agents can operate independently and share high-level knowledge. As cyberattacks have multiple appearances, a single agent may have to manage multiple such closed loops, and often filter out abnormal events. Similar to developing employee working skills, a structured interpretation framework should be designed to assist user adoption, and the ontology alignment or knowledge mapping should be provided for effective communication. The heuristic buffers in the closed-loop (\(\Omega \times \eta\) in Eqs. 12–15) indicate that the interactions between...
humans and machines can influence the performance of a cyberdefense framework.

**Conclusion, Limitation, and Future Research**

Defending cyberattacks should be seen more as a survival strategy than as a solution procurement decision. A self-adaptive framework, whose distributed computing and fault-tolerant properties provide high service availability and the integral system can then mitigate complete failures and facilitate a quicker recovery from the beachheads. The strategic alignment of a self-adaptive framework comprises a contingency strategy on a dynamic configuration, autonomous agents, a learning episteme, double-loop reinforcement, and coordination mechanisms.

Unlike the extant research on information security that extends the discussion through information system theory, this research draws on various disciplines to develop a self-adaptive cyberdefense framework. This research begins with the introduction of a real APT attack and the coming challenges of cybersecurity. In an analogy to an epidemic SIR model, it prepares a layered structure with three dimensions of cyberdefense, namely, Detection, Recovery, and Immunity for simulation. In the first experiment, this research simulates the interaction of these factors that affect recovery velocity and identifies the inapplicability of a static analysis to cyberdefense strategy. In the second experiment, it then transforms the problem to the distributed system with intelligent and autonomous nodes through the actor model and control theory. In search of dependability, this research justifies the impact of learning effects, labels the importance of the human factor, and identifies the time-dependent property. Based on the experiments’ results, this study identifies the discrepancies of the previous studies and develops a time-based self-adaptive framework with management interpretation. From a theoretical perspective, this article develops a self-adaptive control organism to be used for cyberdefense management. This research advances cyberdefense analysis by creating a new dynamic configuration and learning factors in a human–machine collaborative, fault-tolerant distributed framework. From a practice viewpoint, this study offers both instrumental and managerial implications. The configurations in the simulations are based on general conditions with mostly adjustable variables. A subtler customization could generate further variations for multiple purposes. Besides, to enable a distributed cyberdefense, this paper exemplifies key elements for similar simulations including preparing for the propagation topology (by considering the relative position of critical facilities and the identification of...
functional loops), the self-examination of the strength of the current protection screen, an analysis of possible exposure, the construction of the cybersecurity epistemic, the facilitating arrangement for cyberdefense learning and adoption, and the coordination mechanism of routines, norms, and ontology alignment. This work also provides an illuminating analysis for humans to position themselves in the collaborations with increasingly intelligent agents.

Limited to the length of paper, this research does not explore the immediate runtime strategies for all types of cyberattacks. In addition, the modeling uses basic settings, in an attempt to gain generality for discussion. For this reason, further customization might be necessary when applying the framework to specific contexts. The authors encourage future research to continue to develop more responsive mechanisms on self-adaptive basis, and apply the framework proposed in this research to human–computer collaborative environments to obtain further parsimonious theory.

Appendix

- Simulation hypothesis:(adapt (12))
  1. Resistant nodes cannot be infected.
  2. Susceptible neighbors will be infected with a probability given by virus chance.
  3. Infected nodes are not immediately aware their infection until checking.
  4. Virus spreads in the connectivity of topology with regardless of the distance.

- Controlled variables and configuration of scenarios.
  - Scenario 1 to 3: VCF, GRC, RC
  - Scenario 4: VCF, GRC
  - Scenario 5: GRC, RC
  - Scenario 6: VCF, RC
  - Scenario 7: VCF, GRC, RC
  - Scenario 8: VCF, GRC, RC, Virus Spread Chance

Figure A1. Evolving life cycle and propagation trajectory.
Note. The red line is the number of the Infected, the green line is that of the Susceptible and the gray line represents the Resistant. We can observe that except in the emerging period, three lines will generally cross at another two points at $R(t) > I(t)$ and $S(t) > I(t)$. We refer to them as Golden Cross (turning points) $G_1$ and $G_3$, and $Y (I = 0)$ as $G_2$. The $Y (R > I)$ represents the elapse time by $(t_{R-I} - t_0)$ at $G_1$, the $Y (S > I)$ is the elapse time by $(t_{S-I} - t_0)$ at $G_2$, and the $Y (I = 0)$ is the elapse time by $(t_{I=0} - t_0)$ at $G_3$. After $G_1$, the number of resistant nodes has surpassed the number of the infected. After $G_2$, the number of susceptible has been larger than that of the infected. These turning points affect the convergence velocity.
Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Kuan-Jui Huang https://orcid.org/0000-0001-5178-3189

References

Allenmark, F., Hsu, Y.-F., Roussel, C., & Waszak, F. (2015). Repetition priming results in sensitivity attenuation. Brain Research, 1626, 211–217.

Amini, L., Christodorescu, M., Cohen, M. A., Parthasarathy, S., Rao, J., Sailer, R., & Verscheure, O. (2015). Adaptive cybersecurity analytics. Google Patents.

Argyris, C. (1997, September). Double loop learning in organizations. Harvard Business Review. https://hbr.org/1977/09/double-loop-learning-in-organizations

Arora, A., Hall, D., Piatto, C., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. IT Professional, 6(6), 35–42.

Atighetchi, M., Pal, P., Webber, F., Schantz, R., Jones, C., & Loyall, J. (2004). Adaptive cyberdefense for survival and intrusion tolerance. IEEE Internet Computing, 8(6), 25–33.

Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. Science, 211, 1390–1396.

Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. Proceedings of the National Academy of Sciences of the United States of America, 99(Suppl. 3), 7280–7287.

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. IEEE Security & Privacy, 15(6), 12–17.

Chen, Q., Abdelwahed, S., & Erradi, A. (2014). A model-based validated autonomic approach to self-protect computing systems. IEEE Internet of Things Journal, 1(5), 446–460.

Chigan, C., Li, L., & Ye, Y. (2005, March). Resource-aware self-adaptive security provisioning in mobile ad hoc networks. In IEEE wireless communications and networking conference. https://doi.org/10.1109/WCNC.2005.1424845

Chun, I., Park, J., Lee, H., Kim, W., Park, S., & Lee, E. (2013). An agent-based self-adaptation architecture for implementing smart devices in Smart Space. Telecommunication Systems, 52(4), 2335–2346.

Cichoniski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Claudel, B., De Palma, N., Lachaize, R., & Hagimont, D. (2006). Self-protection for distributed component-based applications. In A. K. Datta & M. Gradinariu (Eds.), Symposium on self-stabilizing systems (pp. 184–198). Springer.

Cole, E. (2012). Advanced persistent threat: Understanding the danger and how to protect your organization. Newnes.

Collins, K. S. A., Brenda, B., Samans, R., Hanouz, M. D., & Howell, L. (2018). The global risks report. World Economic Forum 2018.

Cosmides, L. (1989). The logic of social exchange: Has natural selection shaped how humans reason? Studies with the Wason selection task. Cognition, 31(3), 187–276.

Cybenko, G., Jajodia, S., Wellman, M. P., & Liu, P. (2014). Adversarial and uncertain reasoning for adaptive cyber defense: Building the scientific foundation. In A. Prakash & R. Shyamasundar (Eds.), International conference on information systems security (pp. 1–8). Springer.

Cytet, R. M., & March, J. G. (1963). A behavioral theory of the firm. NJ: Prentice Hall.

Dasgupta, D. (2007). Immuno-inspired autonomic system for cyber defense. Information Security Technical Report, 12(4), 235–241.

Dean, D. J., Nguyen, H., & Gu, X. (2012). UBL: Unsupervised behavior learning for predicting performance anomalies in virtualized cloud systems. In Proceedings of the 9th international conference on autonomic computing (pp. 191–200). Association for Computing Machinery. https://doi.org/10.1145/2371536.2371572

Demirtas, H., Allozi, R., Hu, Y., Inan, G., & Ozbek, L. (2017). Joint generation of binary, ordinal, count, and normal data with specified marginal and association structures in Monte-Carlo simulations. In D. G. Chen & J. Chen (Eds.), Monte-Carlo simulation-based statistical modeling (pp. 3–15). Springer.

Ein-Dor, T. (2014). Facing danger: How do people behave in times of need? The case of adult attachment styles. Frontiers in Psychology, 5. Article 1452.

Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing organizational routines as a source of flexibility and change. Administrative Science Quarterly, 48(1), 94–118.

Ferry, T. (2017, February). Looking back at the First Bank’s ATM Heist. Taiwan Business TOPICS. https://topics.amcham.com.tw/2017/02/looking-back-at-the-first-banks-atm-heist/

Floch, J., Hallsteinsem, S., Stav, E., Eliassen, F., Lund, K., & Gjorven, E. (2006). Using architecture models for runtime adaptability. IEEE Software, 23(2), 62–70.

Forrest, S., Hofmeyr, S. A., & Somayaji, A. (1997). Computer immunology. Communications of the ACM, 40(10), 88–96.

Forrester, J. W. (1994). System dynamics, systems thinking, and soft OR. System Dynamics Review, 10(2–3), 245–256.

Fruhlinger, J. (2020). Top cybersecurity facts, figures and statistics for 2020. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Ghosh, D., Sharman, R., Rao, H. R., & Upadhyaya, S. (2007). Self-healing systems—Survey and synthesis. Decision Support Systems, 42(4), 2164–2185.

Gordon, L. A., & Loeb, M. (2006). Budgeting process for information security expenditures. Communications of the ACM, 49(1), 121–125.

Hewitt, C., Bishop, P., & Steiger, R. (1973). A universal modular actor formalism for artificial intelligence. In Proceedings of the 3rd international joint conference on artificial intelligence (pp. 235–245). Morgan Kaufmann Publishers.

Huang, Y. F. (2016). If you were the First Bank, can you defense the cyberattacks? In The analysis of First Bank hacking. iThome. https://www.ithome.com.tw/article/107291
Jacobs, S. (2015). Engineering information security: The application of systems engineering concepts to achieve information assurance. John Wiley.

Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., & Wang, X. S. (2011). Moving target defense: Creating asymmetric uncertainty for cyber threats. Springer Science & Business Media.

Keenan, J. M., Baillet, S. D., & Brown, P. (1984). The effects of causal cohesion on comprehension and memory. Journal of Verbal Learning and Verbal Behavior, 23(2), 115–126.

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. IEEE Computer, 36(1), 41–50.

Kermack, W. O., & McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. Proceedings of the Royal Society of London. Series A. Containing Papers of a Mathematical Physical Character, 115(772), 700–721.

Korczynski, M., Hamieh, A., Huh, J. H., Holm, H., Rajagopalan, S. R., & Fefferman, N. H. (2016). Hive oversight for network intrusion early warning using diamond: A bee-inspired method for fully distributed cyber defense. IEEE Communications Magazine, 54(6), 60–67.

Laprie, J. (1985). Dependable computing and fault tolerance: Concepts and terminology. In Proceedings of the 15th IEEE international symposium on fault-tolerant computing (pp. 2–11).

Mesa. (2016). Mesa: Agent-based modeling in Python 3+. https://mesa.readthedocs.io/en/master/

Moar, J. (2018). The future of cybercrime & security. Juniper Research.

Montasari, R., Hosseinian-Far, A., & Hill, R. (2018). Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. In H. Jahankhani (Ed.), Cyber criminology (pp. 71–93). Springer.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. Information & Management, 52(1), 123–134.

NetLogo. (1999). Virus on a network. https://ccl.northwestern.edu/netlogo/models/VirusOnANetwork

Open Web Application Security Project. (2015). OWASP annotated application security verification standard. https://owasp-aasvs.readthedocs.io/en/latest/index.html

Pasquale, L., Ghezzi, C., Menghi, C., Tsigkanos, C., & Nuseibeh, B. (2014). Topology aware adaptive security. In Proceedings of the 9th international symposium on software engineering for adaptive and self-managing systems (pp. 43–48). https://doi.org/10.1145/2593929.2593939

Portrat, S., Barrouillet, P., & Camos, V. (2008). Time-related decay or interference-based forgetting in working memory? Journal of Experimental Psychology: Learning, Memory, and Cognition, 34(6), 1561–1564.

Qu, G., Rawashdeh, O. A., & Che, D. (2010). Self-protection against attacks in an autonomic computing environment. International Journal of Computers and Their Applications, 17(4), 250–256.

Rodriguez, A., & Castillo, L. (2018). A first step towards a general-purpose distributed cyberdefense system. In Y. Demazeau, B. An, J. Bajo, & A. Fernández-Caballero (Eds.), Advances in practical applications of agents, multi-agent systems, and complexity: The PAAMS collection (pp. 237–247). Springer.

Salehie, M., Pasquale, L., Omoronyia, I., Ali, R., & Nuseibeh, B. (2012). Requirements-driven adaptive security: Protecting variable assets at runtime. In 2012 20th IEEE international requirements engineering conference (pp. 111–120). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/RE.2012.6345794

Salehie, M., & Tahvildari, L. (2009). Self-adaptive software: Landscape and research challenges. ACM Transactions on Autonomous and Adaptive Systems, 4(2), 1–42.

Senge, P. M. (1991). The fifth discipline, the art and practice of the learning organization. Currency.

Tziakouris, G., Bahsoon, R., & Babar, M. A. (2018). A survey on self-adaptive security for large-scale open environments. ACM Computing Surveys, 51(5), 1–42.

Van de Ven, A. H., & Drazin, R. (1984). The concept of fit in contingency theory. Strategic Management Research Center, University of Minnesota.

Willems, J. C. (2012, July). Constrained probability [Paper presentation]. The IEEE international symposium on information theory proceedings.

Yuan, E., Esfahani, N., & Malek, S. (2014). A systematic survey of self-protecting software systems. ACM Transactions on Autonomous and Adaptive Systems, 8(4), 1–41.

Yuan, E., & Malek, S. (2012, June). A taxonomy and survey of self-protecting software systems. In 2012 7th international symposium on software engineering for adaptive and self-managing systems (pp. 109–118). Institute of Electrical and Electronics Engineers. http://doi.org/10.1109/SEAMS.2012.6224397