applied sciences

MDPI

Article

An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users Against Cyberattacks

N'guessan Yves-Roland Douha *, Masahiro Sasabe, Yuzo Taenaka and Youki Kadobayashi

Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma 630-0192, Japan; sasabe@is.naist.jp (M.S.); yuzo@is.naist.jp (Y.T.); youki-k@is.naist.jp (Y.K.)

* Correspondence: douha.nguessan_yves-roland.dn6@is.naist.jp

Abstract: In the digital era, smart-home users face growing threats from cyberattacks that threaten their privacy and security. Hence, it is essential for smart-home users to prioritize cybersecurity education and training to secure their homes. Despite this, the high cost of such training often presents a barrier to widespread adoption and accessibility. This study aims to analyze the costs and benefits associated with various cybersecurity investment strategies for smart-home users in the context of cyberattacks. The study utilizes evolutionary game theory to model a game comprised of three populations: smart-home users, stakeholders, and attackers. We derive and analyze the replicator dynamics of this game to determine the evolutionarily stable strategy (ESS). Furthermore, we investigate the impacts of the costs and benefits of cybersecurity investment and cyberattack costs on the ESS. The findings indicate that incurring costs for cybersecurity training is beneficial for smart-home users to protect their homes and families. However, the training costs must be low and affordable for smart-home users in order to ensure their participation and engagement. Additionally, providing rewards for commitment to cybersecurity is crucial in sustaining interest and investment over the long term. To promote cybersecurity awareness and training for smart-home users, governments can incorporate it as a priority in national cybersecurity plans, provide subsidies for training costs, and incentivize good cybersecurity practices.

Keywords: cybersecurity investment; cost–benefit analysis; evolutionary game theory; replicator dynamics; smart-home users

Citation: Douha, N.Y.-R.; Sasabe, M.; Taenaka, Y.; Kadobayashi, Y. An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users Against Cyberattacks. *Appl. Sci.* **2023**, *13*, 4645. https://doi.org/ 10.3390/app13074645

Academic Editors: Ying Weng, Alexandro Baldassin, Kecheng Liu and Zhuo Chen

Received: 31 January 2023
Revised: 2 April 2023
Accepted: 3 April 2023
Published: 6 April 2023

1. Introduction

Smart homes—houses that mainly incorporate internet-of-things (IoT) devices (e.g., smart meters, smart fridges, and smart speakers) that collect various data and perform autonomous tasks to improve the quality of life at home through remote control and monitoring via the internet—are one of the fastest-growing markets, with worldwide revenue of USD 115.7 billion in 2022 expected to increase to USD 222.9 billion by 2027 [1]. The users of smart homes are of all age groups, i.e., children, adults, and senior citizens, who may face cybersecurity literacy issues leading to human errors and data breaches. This security vulnerability exposes both users and their smart homes to potential cyberattacks. Indeed, existing research [2] seems to agree that the human factor plays a critical role in cybersecurity breaches.

Previous studies investigating home users have shown a need for cybersecurity training. Furnell, Bryant, and Phippen [3] reported that home users lack deep knowledge about cybersecurity. Similarly, Furnell, Tsaganidi, and Phippen [4] reported a need for automatic safeguards to protect home users. Moreover, Łukasz and Potyrała [5] demonstrated the low competence of parents in handling the risks of the digital world. It is well known that user awareness of security countermeasures directly influences information system misuse [6]. Thus, cybersecurity awareness education is a solution that can empower smart-home users by providing them with the knowledge and skills required to reduce the success

rate of cyberattacks in smart homes that exploit human vulnerabilities. However, the financial costs of cybersecurity education programs are a crucial constraint [7]. For example, Morrison, Coventry, and Briggs [8] revealed that older adults might not engage in security behaviors because they believe that the costs of cybersecurity outweigh the benefits and do not want to do something wrong due to limited skills.

Solving the problem of the costs of cybersecurity training is necessary for home users who have limited resources for daily life expenditures. Many studies have investigated the costs and benefits of cybersecurity education training. For example, Zhang et al. [9] conducted a cost–benefit analysis of cybersecurity awareness training programs to determine a company's optimal degree of security. Unfortunately, previous research has not considered trainees' perspectives and constraints. Additional cost–benefit analyses are needed to examine the typical case of smart-home users. By demonstrating that cybersecurity training can provide tangible benefits to smart-home users, they can be motivated to engage in cybersecurity training and security behaviors at home.

To determine whether it is worthwhile for smart-home users to invest in cybersecurity, in this work we analyze smart-home environments, including many IoT devices, smart-home users, and multiple stakeholders (e.g., manufacturers) subject to cyberattacks. As mentioned in [10], attackers have a wide range of interests and potential targets in a dynamic and complex smart-home environment. We adopt evolutionary game theory (EGT) to model realistic attack scenarios based on direct attacks and supply chain attacks, which are indirect attacks in which an attacker compromises a part or parts of a supply chain in order to reach and compromise its primary target. We analyze the costs and benefits of the decision-making of three populations, i.e., smart-home users, smart-home stakeholders, and attackers, with regard to smart-home security.

Previous research has used formal methods to address cybersecurity issues in IoT-based smart environments. For example, Krichen and Alroobaea [11] used attack trees to represent attack scenarios on IoT systems and transformed a given attack tree into a network of priced timed automata to test the security of IoT systems. Tabrizi and Pattabiraman used model checking to automatically analyze and identify possible attacks on smart-home devices known as smart meters [12]. Similarly, Kumar et al. [13] used model checking to address authentication, anonymity, and integrity in a smart-home environment. In addition to these formal methods, EGT can be used to analyze decision-making in smart environments.

The choice of EGT in the present study is motivated by its effectiveness in studying the decision-making of large populations of agents who repeatedly engage in strategic interactions [14]. Similar formal methods, such as classical game theory and agent-based modeling, have limitations when modeling the evolution of populations over time. Classical game theory assumes that all players are rational and make decisions based only on their payouts, which is often unrealistic in real-world scenarios. While agent-based modeling can be used to simulate the behavior of individual agents and their interactions with each other and the environment, it may not capture the strategic interactions between agents as effectively as EGT. In contrast, EGT focuses specifically on strategic interactions among agents and describes the outcomes of these interactions as payoff distributions.

Using EGT, we can examine how the different costs and benefits of cybersecurity investment influence the behavior of smart-home users and stakeholders as well as how attackers might adapt to these changes. EGT allows us to study the evolution of different strategies and their effects on the population over time, which is important for understanding how to design effective cybersecurity measures. Several previous studies have used EGT to study cybersecurity issues, demonstrating its effectiveness and relevance in this field. For example, Tosh et al. [15] used EGT to examine a Cybersecurity Information Exchange (CYBEX) framework, while Abass et al. [16] used EGT to analyze advanced persistent threats. These studies highlight the value of EGT in addressing cybersecurity challenges and advancing our understanding of how strategic interactions shape the evolution of populations over time.

This journal paper is an extended version of our earlier conference paper [17]. That paper used a classical game-theoretic approach to analyze the security investment costs and benefits of smart-home users. In that paper, we studied a game based on agents and analyzed the pure and mixed Nash equilibria of a four-player game comprising three types of smart-home users (i.e., adults, children, and senior citizens) along with an attacker. In the present journal paper, we focus on a population game to investigate the evolution of agents' strategy choices on a large scale and over time. We propose an asymmetric non-cooperative game describing the strategic sets of three populations: smart-home users, manufacturers (an instance of smart-home stakeholders), and attackers. Figure 1 illustrates our proposed approach, outlining our investigation of the evolutionarily stable strategy (ESS) and the properties of the evolutionary dynamics in the game. Additionally, we analyze the impacts of cybersecurity investment costs, benefits, and cyberattack costs on the ESS.

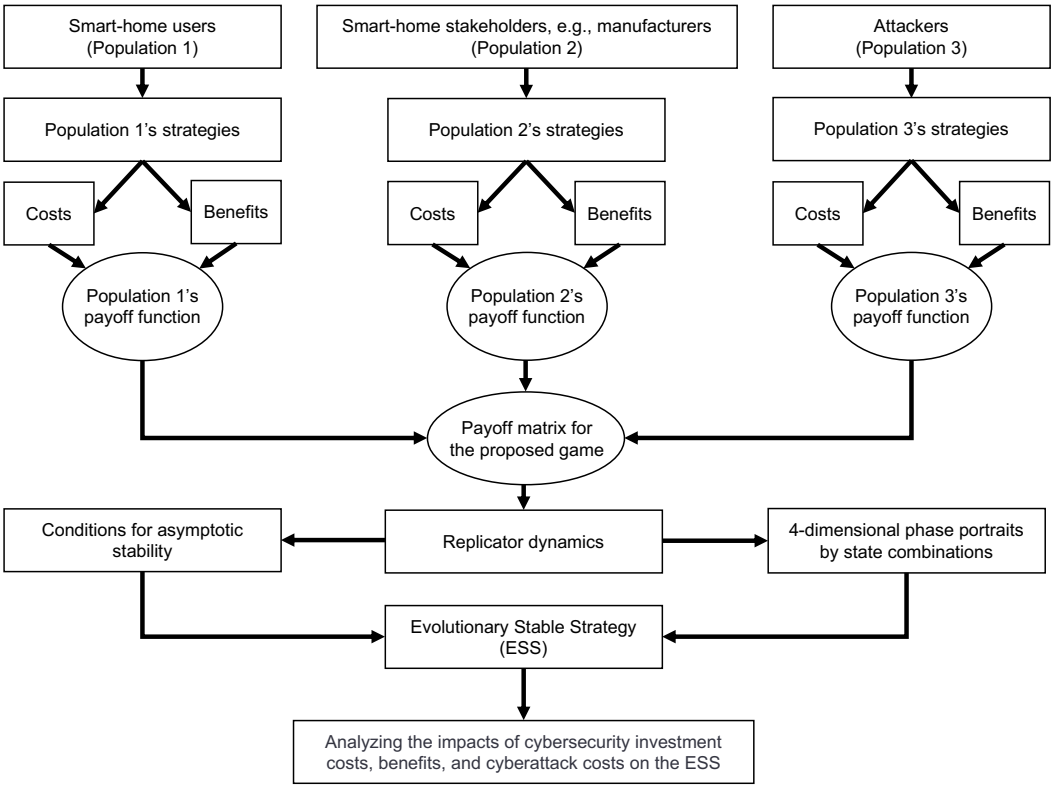


Figure 1. Flowchart of the proposed approach.

Contributions

The major contributions of the present journal paper are:

- Modeling the competition between cybersecurity investment and cyberattacks as a non-cooperative game among three populations: smart-home users, manufacturers, and attackers.
- Deriving the replicator dynamics of these three populations using EGT, analyzing the Nash equilibrium solutions of the proposed evolutionary game model, and identifying the conditions for asymptotic stability of equilibrium solutions.
- Validating our theoretical results using four-dimensional phase portraits with state combinations and plotting the evolution of population fractions to confirm the existence of a unique ESS in the proposed game.
- Analyzing and discussing the numerical results of the proposed game by investigating the impacts of costs and benefits of cybersecurity investment and cyberattack costs on the ESS.

We organize the remainder of the paper as follows: Section 2 presents the research background; Section 3 explains the proposed game model and illustrates the payoff matrix; Section 4 derives replicator dynamic equations and identifies the ESS; Section 5 presents the numerical results; Section 6 discusses the findings of the paper; finally, Section 7 concludes the work.

2. Related Work

This section presents related works in three subsections. Section 2.1 presents previous articles that have covered cybersecurity awareness for home users, Section 2.2 describes works that have used a game-theoretic approach to analyze security investment costs and benefits, and Section 2.3 introduces the background of evolutionary game theory.

2.1. Cybersecurity Awareness for Home Users

In the present paper, we differentiate home users from smart-home users. We consider home users as conventional internet users who use internet services through terminals (e.g., desktops, laptops, smartphones, and tablets) in the home. Smart-home users, on the other hand, are new-generation users who, in addition to internet services, use and remotely control IoT devices (e.g., smart thermostats, smart speakers) through terminals and voice commands to improve their comfort and quality of life at home.

The issue of home users' awareness of cybersecurity best practices is not new in itself. The first research dates back to the early 2000s with the accessibility of the internet and computers in the home. In 2007, Furnell, Bryant, and Phippen [3] investigated the security perceptions of internet users in the home using a survey of 415 home users. They found that home users, especially novice internet users, lacked deep knowledge regarding how to protect themselves and were not aware of initiatives that might help them. In 2008, Furnell, Tsaganidi, and Phippen [4] confirmed this finding in an additional investigation based on detailed interviews with 20 novice internet users. Moreover, the study revealed that safeguards should automatically be provided for home users. To this end, in 2010, Kritzinger and von Solm [18] proposed a theoretical e-awareness model that forces home users to absorb the required awareness content before venturing out into cyberspace in order to empower them with a better understanding of security risks and how to avoid threats. In 2012, Howe et al. [19] analyzed the psychology of security for home users. They reported that when home users do not understand the various security threats, they are sometimes unwilling or unable to incur the costs of defending against threats. An effective way to raise home user awareness of threats is to engage them in cybersecurity awareness training. In 2017, Alotaibi, Clarke, and Furnell [20] reviewed the existing security awareness tools for home users in terms of their timeliness, mechanisms, and effectiveness. They reported a need to implement a holistic information security management system that is easy to understand and not time-consuming in order to raise information security awareness among home users.

In 2019, Aldawood and Skinner [7] studied the challenges of implementing training and awareness programs targeting cybersecurity social engineering. They reported that the economic aspect of cybersecurity training was another challenge to consider. This finding corroborated the conclusions of Ricci, Breitinger, and Baggili [21], who surveyed 233 parents and reported that many did not want to spend money on cybersecurity education even though they were concerned about their children's safety and security from cyberattacks. In 2021, Łukasz and Potyrała [5] examined the level of knowledge and literacy held by 514 parents of primary school students. They reported that the majority of parents tended to overestimate their digital literacy level and had low cybersecurity skills. In addition, Morrison, Coventry, and Briggs [8] showed in 2021 that older adults, i.e., senior citizens, believed that the costs of cybersecurity training outweigh the benefits and did not want to engage in cybersecurity education.

The literature reveals that the cybersecurity literacy of children, adults, and senior citizens appears to be low. Despite this, home users are not willing to spend money on

cybersecurity education. Considering that smart-home users are even more at risk of cyberattacks because of security flaws in IoT devices, Douha et al. [17] analyzed the costs and benefits of cybersecurity awareness training for smart-home users. The authors used game theory to model the strategy choices of four agents: a child, an adult, and a senior citizen, each living in a smart home, and an attacker. They found that it is beneficial for smart-home users to incur costs to protect their homes and families against the threat of cyberattacks. One limitation of this study was the small number of agents and the static nature of the model. On the one hand, the results did not reflect the strategic choices of the smart-home users' population dynamic as a whole, only a sample of three agents living in a smart home. On the other hand, as an individual's choices may change over time, it is necessary to conduct a new study using evolutionary game theory to analyze the costs and benefits of cybersecurity education over time for the smart-home user population.

Finally, a recent review paper published in 2022 on home users' perspectives of security and privacy uncovered several research gaps [22]. The authors emphasized the need to take into account various interconnected home devices, the co-existence of diverse home user groups, and other stakeholders in future studies. We consider these aspects in our game theory-based approach.

2.2. Game-Theoretic Approaches for Cybersecurity Investment

Decisions about information technology (IT) security investment often involve weighing the costs and benefits. Thus, one might consider decision theory as an essential support for this purpose. However, Cavusoglu et al. [23] showed that game-theoretic approaches are more suitable than traditional decision-theoretic approaches regarding IT security investments, especially when considering that attackers are strategic. On the other hand, Douha et al. [24] presented an overview of potential cyberattacks on a smart home. Attackers can exploit different entry points, such as smart-home networks, IoT devices, mobile apps, and human vulnerabilities; thus, attackers are supposed to be strategic when planning to attack a smart home. This supports the idea that a game-theoretic approach can address the research problem addressed in our work.

Anna Nagurney and Ladimer Nagurney [25] presented a game model that determines optimal product transactions and cybersecurity investments for sellers competing to maximize their expected profits. Their model incorporates the preferences of buyers through demand price functions, which depend on product demand and the average level of security in the marketplace. Furthermore, Nagurney et al. [26,27] proposed supply chain network game theory models based on retailers and demand markets. However, their models do not account for attackers, a critical aspect in attack–defense models that is necessary for evaluating the costs and benefits of cybersecurity investment.

Tosh et al. [28] proposed a sequential game model that involves three players: organization, attacker, and insurer. The authors used backward induction to determine the subgame perfect equilibrium and analyze the optimal self-defense investment strategy for organizations, the optimal attack rate for the adversary, and the optimal coverage level for insurers through numerical results. However, the proposed game assumes that each player is aware of the moves of other players, which may not be realistic in a real-world smart-home environment where users may not know if IoT devices available on the market are secure or if they are being targeted by attackers. This incomplete information can limit the effectiveness of the game model in capturing real-world scenarios. Therefore, in the present paper, we use a simultaneous game model to address this limitation.

Hyder and Govindarasu [29] proposed a game-theoretic approach for optimizing cybersecurity investment strategies in a smart grid. Their system model focuses on the costs of both attackers and defenders, with attackers seeking to minimize their costs while maximizing the costs of defenders, and vice versa for defenders. However, the authors did not include benefit parameters in their model, which are critical for evaluating the significance of cybersecurity investment. Therefore, our proposed model builds upon their framework by studying a non-cooperative game that analyzes both the costs and benefits

of attackers and defenders in the smart-home environment. Furthermore, we investigate the evolution of strategic choices by agents on a large scale and over time. This model extension contributes to a more comprehensive understanding of the strategic behavior of agents in cybersecurity investment decision-making.

Sun et al. [30] utilized evolutionary game theory to investigate information security investments in the mobile electronic commerce industry chain. They introduced a penalty parameter to discourage organizations from not investing in IT security, and showed that regulating such a parameter could encourage information security investments. In contrast, our study proposes a different approach that imposes higher costs of cyberattacks on populations that do not invest in cybersecurity, while offering a reward parameter for those who do. Although a recent study [17] used a similar approach, it only considered a static game model without analyzing the evolution of players' strategies over time. To address this limitation, our study uses an evolutionary game theory-based model to explore the dynamics of strategic behaviors over time, providing a deeper understanding of decision-making processes regarding cybersecurity investment in a smart-home environment.

2.3. Evolutionary Game Theory

Evolutionary game theory (EGT) was developed following the work of John Maynard Smith [31,32], with the aim of adapting the traditional game-theoretic approaches [33,34], in which players are assumed to be rational, to study natural biological selection. This investigation led to the development of the concept of "evolutionarily stable strategies" (ESS) to explain the existence of ritual conflicts between animals. In a game model comprising populations of individuals adopting different strategies and competing against each other, an ESS is a strategy that cannot be bettered (or invaded) by any other existing strategy that everybody else in the population chooses. The ESS describes the stability of the game dynamics over time. Note that this dynamic is often described using replicator dynamics [35]. Therefore, in the present study we derive and analyze the replicator dynamics of our proposed evolutionary game in order to identify the ESS.

While numerous previous studies have investigated cybersecurity challenges using evolutionary games, most have not focused on the central problem that our paper addresses. For example, Tosh et al. [15] examined a Cybersecurity Information Exchange (CYBEX) framework using an EGT-based approach to determine the condition under which players' self-enforced evolutionary stability (i.e., ESS) can be achieved. Abass et al. [16] analyzed the stability of defense and attack strategies in an evolutionary game based on the replicator dynamics criteria and identified the locally asymptotically stable points of the game. Sun et al. [30] used an EGT-based approach for cybersecurity investment, although they proposed a symmetric game and did not provide numerical results for their study.

Table 1 compares our study with previous research in the field. We note that the existing literature mainly focuses on the security of traditional internet users in their homes. However, with the increasing use of modern technologies such as IoT devices, the possibility of security breaches in smart homes is on the rise. There is a gap in the existing literature, as previous studies have not thoroughly explored the issue of cybersecurity investments for smart-home users. This motivates us to use an evolutionary game-theoretic approach to analyze the costs and benefits of cybersecurity investment over time for smart-home users in order to encourage them to invest in cybersecurity measures necessary to defend themselves against potential cyberattacks.

Table 1. Comparison between the present study and related works.

Year	Reference	(Internet-Based) Home Users	(IoT-Based) Smart-Home Users	Cybersecurity Investment	Approach	Evolutionary Game Analysis
2007	Furnell, Bryant, and Phippen [3]	Yes	No	No	Empirical study of home users (survey)	No
2008	Furnell, Tsaganidi, and Phippen [4]	Yes	No	No	Empirical study of home users (interview)	No
2008	Sun et al. [30]	No	No	Yes	Game model using two-organization symmetric game	Yes, but no numerical results
2010	Kritzinger and von Solm [18]	Yes	No	No	Theoretical e-awareness model	No
2012	Howe et al. [19]	Yes	No	No	Literature review of factors that influence security decisions of home users	No
2015	Anna Nagurney and Ladimer Nagurney [25]	No	No	Yes	Game model using buyers and sellers	No
2015	Nagurney et al. [26]	No	No	Yes	Supply chain network game model using retailers and demand markets	No
2017	Alotaibi, Clarke, and Furnell [20]	Yes	No	No	Reviewing the existing security awareness tools for home users	No
2017	Nagurney et al. [27]	No	No	Yes	Supply chain network game model using retailers and demand markets with nonlinear budget constraints	No
2017	Tosh et al. [28]	No	No	Yes	Sequential game model using organizations, attackers, and insurers	No
2019	Ricci, Breitinger, and Baggili [21]	Yes	No	Yes	Empirical study of parents (survey)	No
2020	Hyder and Govindarasu [29]	No	No	Yes	Game model using attackers and defenders	No
2021	Łukasz and Potyrała [5]	Yes	No	No	Empirical study of parents (survey)	No
2021	Morrison, Coventry, and Briggs [8]	Yes	No	Yes	Empirical study of older adults (interview)	No
2021	Douha et al. [17]	Yes	Yes	Yes	Game model using an attacker and three categories of smart-home users	No

Table 1. *Cont.*

Year	Reference	(Internet-Based) Home Users	(IoT-Based) Smart-Home Users	Cybersecurity Investment	Approach	Evolutionary Game Analysis
2022	Pattnaik, Li, and Nurse [22]	Yes	Yes	No	Literature review of user perspectives on security and privacy in a home networking environment	No
2023	This work	Yes	Yes	Yes	Game model using three-population asymmetric game	Yes

3. Proposed Game Model

This section introduces our game model in three subsections; Section 3.1 describes the system, Section 3.2 defines the parameters of the game, and Section 3.3 presents the payoff matrix.

3.1. System Model

Our system comprises three populations: smart-home users ($population_1$), manufacturers ($population_2$), and attackers ($population_3$). Figure 2 illustrates our system. $Population_1$ uses the IoT devices (e.g., IP cameras, smart speakers, and smartwatches) manufactured by $population_2$ for conveniences such as house physical security, entertainment, and healthcare. The rise of cyberattacks on IoT devices may lead $population_1$ to invest in cybersecurity awareness training to learn how to protect IoT devices from cyberattacks and adopt good cybersecurity hygiene at home.

Recent cyberattacks have shown that manufacturing is among the most targeted industries. The IBM Security X-Force Threat Intelligence Index 2022 reported that manufacturing was the most attacked industry in 2021 [36]. It is worth noting that manufacturers do not always implement security best practices due to the effects of supply chain pressures and delays and the high costs of security. Thus, we consider that $population_2$ may comply with security best practices and implement them for smart-home devices.

Regarding attackers, they may gain interest in compromising smart homes for various motives, such as accessing private information, using IoT-based home devices to execute Distributed Denial-of-Service (DDoS) attacks, and the absence of resistance, such as that provided by a dedicated cybersecurity team. We consider that $population_3$'s attacks may target supply chains that include manufacturers (i.e., $population_2$). As a result, $population_3$ may deceive $population_1$ indirectly through the exploitation of IoT device vulnerabilities. Furthermore, $population_3$ may discern that $population_1$ is not aware of security countermeasures, such as changing default passwords, using multi-factor authentication, or recognizing and avoiding phishing links, which may provide various entry points. Thus, $population_3$ may succeed in deceiving $population_1$ directly, for instance through social engineering.

The proposed system model is designed to address the unique security challenges of smart-home environments. In such environments, IoT devices are prevalent and susceptible to many attacks, partly because manufacturers may produce insecure IoT devices in order to reduce production costs. Moreover, users may lack extensive knowledge of cybersecurity best practices, thereby making smart homes even more vulnerable to cybersecurity threats. As a result, the proposed system aims to enhance the security of smart homes by promoting investments in cybersecurity to mitigate the risks posed by insecure IoT devices, human factors, and other vulnerabilities.

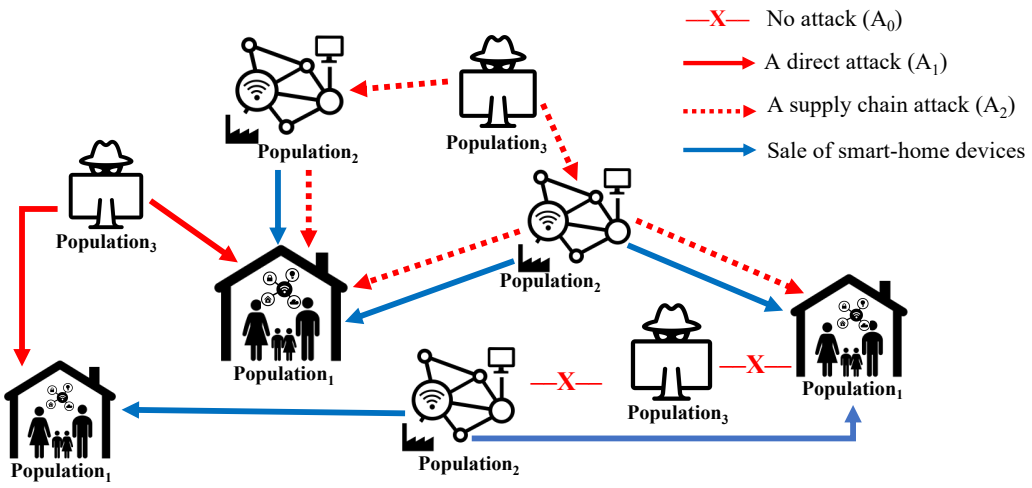


Figure 2. Illustration of the proposed system model.

3.2. Game Modeling

This subsection presents the parameters used to describe the proposed game, as shown in Table 2.

Table 2. List of parameters used in the proposed evolutionary game model.

Parameters	Descriptions
T	$population_1$ invests in cybersecurity awareness training.
$\bar{T}$	$population_1$ does not invest in cybersecurity awareness training.
S	$population_2$ implements security best practices.
$\bar{S}$	$population_2$ does not implement security best practices.
A_0	$population_3$ adopts the strategy of no attack.
A_1	$population_3$ deceives $population_1$ directly.
A_2	$population_3$ deceives $population_1$ after compromising $population_2$.
$P(A_1/T)$	Probability of $population_3$ compromising $population_1$ given the strategy T.
$P(A_1/\bar{T})$	Probability of $population_3$ compromising $population_1$ given the strategy $\bar{T}$.
$P(A_2/S)$	Probability of $population_3$ to compromise $population_2$ given the strategy S.
$P(A_2/\bar{S})$	Probability of $population_3$ compromising $population_2$ given the strategy $\bar{S}$.
C_{10}	Cost of smart-home adoption.
C_{11}	Households' expenditure.
C_{12}	Cost related to the strategy T.
C_{13}	Cost of a security breach given the strategy $\bar{S}$.
C_{14}	Cost of cyberattacks on $population_1$ involving interruption costs of smart-home services and affecting $population_1$'s comfort and safety.
C_{20}	Cost of security implementation related to the strategy S.
C_{21}	Cost of cyberattacks on $population_2$ involving loss of intellectual property and customer confidential information, and lost revenue.
C_{30}	Cost of conducting a cyberattack targeting $population_1$, given that $population_1$ takes the strategy T.
C_{31}	Cost of conducting a cyberattack targeting $population_1$, given that $population_1$ takes the strategy $\bar{T}$.
C_{32}	Cost of conducting a cyberattack targeting $population_2$, given that $population_2$ takes the strategy S.
C_{33}	Cost of conducting a cyberattack targeting $population_2$, given that $population_2$ takes the strategy $\bar{S}$.
I_{10}	Households' income.
P_{20}	Amount of profit obtained by $population_2$ from selling smart-home devices given the strategy S.
P_{21}	Amount of profit obtained by $population_2$ from selling smart-home devices given the strategy $\bar{S}$.

Table 2. *Cont.*

Parameters	Descriptions
R_{10}	The measure of the improved lifestyle that $population_1$ may enjoy by living in smart homes.
R_{11}	Reward of $population_1$ for noticing security countermeasures based on the strategy T.
R_{20}	The measure of $population_1$'s trust obtained by $population_2$ when considering the strategy S.

Let T and $\bar{T}$ respectively be the strategies that $population_1$ invests in cybersecurity awareness training and that $population_1$ does not invest in cybersecurity awareness training. Let S and $\bar{S}$ be the security best practices strategies that $population_2$ implements and does not implement, respectively, for IoT technology when manufacturing smart-home devices. Let A_1 be the strategy in which $population_3$ attacks $population_1$ directly and let A_2 be the strategy in which $population_3$ attacks $population_1$ after compromising $population_2$. As we show that the attacker incurs costs for direct/indirect attacks, we consider the strategy of no attack as well, i.e., A_0.

In terms of probabilities, we consider $P(A_1/T)$ and $P(A_1/\bar{T})$ to be the respective probabilities of $population_3$ compromising $population_1$ given strategies T and $\bar{T}$. Moreover, we consider $P(A_2/S)$ and $P(A_2/\bar{S})$ to be the respective probabilities of $population_3$ compromising $population_2$ given strategies S and $\bar{S}$. We assume that

$$P(A_1/\bar{T}) > P(A_1/T). \tag{1}$$

$$P(A_2/\bar{S}) > P(A_2/S). \tag{2}$$

$$P(A_2/\bar{S}) > P(A_1/T). \tag{3}$$

$$P(A_1/\bar{T}) > P(A_2/S). \tag{4}$$

$$P(A_2/\bar{S}) > P(A_1/\bar{T}). \tag{5}$$

$$P(A_1/T) > P(A_2/S). \tag{6}$$

We have (1) and (2) because we consider that $population_1$ and $population_2$ are more secure (i.e., less at risk of cyberattacks) when choosing the strategies T and S, respectively. We have (3) and (4) because we consider that an attacker is more likely to compromise a target that does not invest in cybersecurity. Moreover, we have (5) because $population_2$ has more assets (e.g., people, hardware, software, networks, cloud servers, and websites), resulting in more possible entry points for a cyberattack than $population_1$ in the case of strategies S and T, respectively. Finally, we have (6) because companies have more financial means to invest in cybersecurity than smart-home users, thereby acquiring adequate tangible, intangible, and human resources to ensure the implementation of security policies. Therefore, we assume that $population_1$ choosing the strategy T is less protected from cyberattacks than $population_2$ choosing strategy S.

With respect to costs, let C_{10}, C_{11}, C_{12}, C_{13}, and C_{14} be the costs related to $population_1$; C_{10} measures the cost of buying a smart home and IoT devices, C_{11} measures smart-home users' expenditures on goods and services such as education, food, furniture, transportation, communication, and medical care, C_{12} measures the costs related to the strategy T, C_{13} measures the costs of a security breach given the strategy $\bar{S}$, i.e., an unnoticed breach of $population_2$'s insecure computer systems that allows $population_3$ to create

backdoors to $population_1$'s IoT devices, and C_{14} measures the costs incurred by cyberattacks on $population_1$, which could involve interruption costs of smart-home services (e.g., home automation, electric power, healthcare, entertainment, the internet) and affect $population_1$'s comfort, convenience, and safety. Moreover, let C_{20} and C_{21} be the costs related to $population_2$; C_{20} measures the security implementation costs related to the strategy S, while C_{21} measures the costs incurred by cyberattacks on $population_2$, which could involve loss of intellectual property and confidential customer information, reputational damage, business operation disruption, and lost revenue. Finally, let C_{30}, C_{31}, C_{32}, and C_{33} be the costs related to $population_3$; C_{30} and C_{31} respectively measure the costs of conducting cyberattacks targeting $population_1$ when this population takes strategies T and $\bar{T}$, while C_{32} and C_{33} respectively measure the costs of conducting cyberattacks targeting $population_2$ when this population takes strategies S and $\bar{S}$.

In the following, we provide rational assumptions about the relationships between system parameters. We first assume that all the cost parameters are non-negative:

$$C_{ij} \geq 0. \tag{7}$$

where $(i, j) = (1,0), (1,1), (1,2), (1,3), (1,4), (2,0), (2,1), (3,0), (3,1), (3,2), (3,3)$.

$$C_{21} > C_{14}. \tag{8}$$

Equation (8) indicates that the costs of cyberattacks on $population_2$ are assumed to be higher than those on $population_1$ due to the relative value of stakeholders' assets versus smart-home assets.

For the relationship between cost parameters of $population_3$, we have the following assumptions:

$$C_{30} > C_{31}. \tag{9}$$

$$C_{32} > C_{33}. \tag{10}$$

We assume (9) and (10) because $population_3$ would require more resources to implement cyberattacks when $population_1$ (or $population_2$) takes strategy T (or S) instead of strategy $\bar{T}$ (or $\bar{S}$). In addition, we assume the following:

$$(C_{13} + C_{14})P(A_1/\bar{T}) > C_{14}P(A_1/\bar{T}) > C_{31}. \tag{11}$$

$$(C_{13} + C_{21})P(A_2/\bar{S}) > C_{33}. \tag{12}$$

$$C_{30} > (C_{13} + C_{14})P(A_1/T) > C_{14}P(A_1/T). \tag{13}$$

$$C_{32} > (C_{13} + C_{21})P(A_2/S). \tag{14}$$

Equations (11) and (12) indicate that the attacker, i.e., $population_3$, commits fewer resources for a large gain by compromising a target that does not invest in cybersecurity, e.g., when $population_1$ takes strategy $\bar{T}$ and $population_2$ takes strategy $\bar{S}$. In the case of (13) and (14), the targets, i.e., $population_1$ and $population_2$, invest in cybersecurity. They are more aware of cybersecurity threats and security best practices. In such a scenario, we presume that $population_3$ incurs higher costs than gains from a successful attack on $population_2$ and $population_3$.

Income and profits: I_{10} measures smart-home users' income, while P_{20} and P_{21} measure the amount of profit obtained by $population_2$ from selling smart-home devices given strategies S and $\bar{S}$, respectively.

For rewards, let R_{10} and R_{11} be the rewards of $population_1$; R_{10} quantifies the improved lifestyle that $population_1$ may enjoy by living in smart homes, while R_{11} is the reward of $population_1$ due to noticing security countermeasures based on the strategy T. This reward measures the increased sense of feeling safe and secure when using IoT devices

at home. Moreover, let R_{20} be the reward of $population_2$; R_{20} quantifies $population_1$'s trust obtained by $population_2$ when considering strategy S.

$$R_{11} > C_{12}. \tag{15}$$

We have (15) because $population_1$ would be willing to take strategy T only if the merit of investing in cybersecurity awareness training, i.e., R_{11}, is larger than its cost, i.e., C_{12}.

In addition, we assume that

$$P_{20} + R_{20} > C_{20} + P_{21}. \tag{16}$$

We have (16) because companies, including $population_2$ (i.e., manufacturing companies), are willing to invest in cybersecurity and take strategy S only if the profit P_{20} obtained from sales using strategy S and the good reputation R_{20} obtained based on the same strategy are larger than the cost of strategy S plus the profit P_{21} obtained from sales using strategy $\bar{S}$.

With the parameters of the game defined, we now describe the strategy sets of each population in a matrix, called the normal form.

3.3. Normal-Form Game

This subsection presents the strategies and payoffs resulting from our proposed game. Table 3 describes the strategic form of the game, known as the normal-form game. Each cell $(row, column)$ from (5, 3) to (7, 6) represents the payoffs of each population. The first line of these cells shows $population_1$'s payoffs, the second line shows $population_2$'s payoffs, and the third line shows $population_3$'s payoffs. As an illustration, we explain the payoffs described in the cell (Row 6, Column 3). The strategies of $population_1$, $population_2$, and $population_3$ consist of playing strategies T, S, and A_1, respectively. When each population engages in this contest, the payoffs of $population_1$, $population_2$, and $population_3$ are $I_{10} + R_{10} - C_{10} - C_{11} - C_{12} + R_{11} - C_{14}P(A_1/T)$, $P_{20} - C_{20} + R_{20}$, and $C_{14}P(A_1/T) - C_{30}$, respectively.

Table 3. Payoffs for the proposed game.

		$Population_2$	
		S	
		$Population_1$	
		T	$\bar{T}$
$Population_3$	A_0	$I_{10} + R_{10} - C_{10} - C_{11} - C_{12} + R_{11}$ $P_{20} - C_{20} + R_{20}$ 0	$I_{10} + R_{10} - C_{10} - C_{11}$ $P_{20} - C_{20} + R_{20}$ 0
	A_1	$I_{10} + R_{10} - C_{10} - C_{11} - C_{12} + R_{11} - C_{14}P(A_1/T)$ $P_{20} - C_{20} + R_{20}$ $C_{14}P(A_1/T) - C_{30}$	$I_{10} + R_{10} - C_{10} - C_{11} - C_{14}P(A_1/\bar{T})$ $P_{20} - C_{20} + R_{20}$ $C_{14}P(A_1/\bar{T}) - C_{31}$
	A_2	$I_{10} + R_{10} - C_{10} - C_{11} - C_{12} + R_{11} - C_{13}P(A_2/S)$ $P_{20} - C_{20} + R_{20} - C_{21}P(A_2/S)$ $(C_{13} + C_{21})P(A_2/S) - C_{32}$	$I_{10} + R_{10} - C_{10} - C_{11} - C_{13}P(A_2/S)$ $P_{20} - C_{20} + R_{20} - C_{21}P(A_2/S)$ $(C_{13} + C_{21})P(A_2/S) - C_{32}$

Table 3. *Cont.*

		$Population_2$	
		$\bar{S}$	
		$Population_1$	
		T	$\bar{T}$
$Population_3$	A_0	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}$ P_{21} 0	$I_{10}+R_{10}-C_{10}-C_{11}$ P_{21} 0
	A_1	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-(C_{13}+C_{14})P(A_1/T)$ P_{21} $(C_{13}+C_{14})P(A_1/T)-C_{30}$	$I_{10}+R_{10}-C_{10}-C_{11}-(C_{13}+C_{14})P(A_1/\bar{T})$ P_{21} $(C_{13}+C_{14})P(A_1/\bar{T})-C_{31}$
	A_2	$I_{10}+R_{10}-C_{10}-C_{11}-C_{12}+R_{11}-C_{13}P(A_2/\bar{S})$ $P_{21}-C_{21}P(A_2/\bar{S})$ $(C_{13}+C_{21})P(A_2/\bar{S})-C_{33}$	$I_{10}+R_{10}-C_{10}-C_{11}-C_{13}P(A_2/\bar{S})$ $P_{21}-C_{21}P(A_2/\bar{S})$ $(C_{13}+C_{21})P(A_2/\bar{S})-C_{33}$

4. Game Analysis

This section aims to analyze the evolutionary stability of the proposed game, which relates to three populations: $population_1$, $population_2$, and $population_3$. We first derive the replicator equation related to each population. Then, we analyze the conditions that satisfy the evolutionary stability of the game.

4.1. Replicator Dynamics

Replicator dynamics is a fundamental concept in evolutionary game dynamics [37]. It is a deterministic model that describes selection dynamics (frequency-dependent selection) through the use of equations.

Let $x(t)$, $y(t)$, $z_1(t)$, and $z_2(t)$ be the frequencies of the strategies T, S, A_1, and A_2, respectively, at time t ($t \geq 0$), where $0 \leq x(t), y(t), z_1(t), z_2(t) \leq 1$. Whenever possible, we omit the time t for brevity. Note that the frequencies of strategies $\bar{T}$, $\bar{S}$, and A_0 are provided by $1-x$, $1-y$, and $1-z_1-z_2$, respectively.

4.1.1. Replicator Equation of $Population_1$

Let F_T and $F_{\bar{T}}$ be the fitness of T and $\bar{T}$, respectively, with $\overline{F_1}$ being the average expected fitness for $population_1$. The replicator equation of $population_1$ is then

$$\frac{dx}{dt} = x(F_T - \overline{F_1}) \tag{17}$$

Thus, we obtain

$$\begin{aligned}\frac{dx}{dt} =& x(x-1)[C_{12}-R_{11}+z_1C_{13}P(A_1/T)+z_1C_{14}P(A_1/T)-z_1C_{13}P(A_1/\bar{T})\\ &-z_1C_{14}P(A_1/\bar{T})-yz_1C_{13}P(A_1/T)+yz_1C_{13}P(A_1/\bar{T})].\end{aligned} \tag{18}$$

4.1.2. Replicator Equation of $Population_2$

Let F_S and $F_{\bar{S}}$ be the fitness of S and $\bar{S}$, respectively, with $\overline{F_2}$ being the average expected fitness for $population_2$. The replicator equation of $population_2$ is then

$$\frac{dy}{dt} = y(F_S - \overline{F_2}) \tag{19}$$

Thus, we obtain

$$\frac{dy}{dt} = y(y-1)[C_{20}-P_{20}+P_{21}-R_{20}+z_2C_{21}P(A_2/S)-z_2C_{21}P(A_2/\bar{S})]. \tag{20}$$

4.1.3. Replicator Equations of $Population_3$

Let F_{A_0}, F_{A_1}, and F_{A_2} be the fitness of A_0, A_1 and A_2, respectively, with $\overline{F_3}$ being the average expected fitness for $population_3$. The replicator equation of $population_3$ regarding strategy A_1 is then

$$\frac{dz_1}{dt} = z_1(F_{A_1} - \overline{F_3}) \tag{21}$$

Thus, we obtain

$$\begin{aligned}\tfrac{dz_1}{dt} = \; & -z_1[z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)) \\ & (y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1))] - [x(C_{30} - \\ & P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)](y-1) + z_2 \\ & [(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)) \\ & (y-1) - y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13} + C_{21})) \\ & (x-1))] + y[x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1)]].\end{aligned} \tag{22}$$

The replicator equation of $population_3$ regarding strategy A_2 is

$$\frac{dz_2}{dt} = z_2(F_{A_2} - \overline{F_3}). \tag{23}$$

Thus, we obtain

$$\begin{aligned}\tfrac{dz_2}{dt} = \; & -z_2[z_1[(x(C_{30} - P(A_1/T)(C_{13} + C_{14})) - (C_{31} - P(A_1/\bar{T})(C_{13} + C_{14}))(x-1)) \\ & (y-1) - y(x(C_{30} - C_{14}P(A_1/T)) - (C_{31} - C_{14}P(A_1/\bar{T}))(x-1))] - [x(C_{33} - \\ & P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1)](y-1) + z_2 \\ & [(x(C_{33} - P(A_2/\bar{S})(C_{13} + C_{21})) - (C_{33} - P(A_2/\bar{S})(C_{13} + C_{21}))(x-1))(y-1) \\ & -y(x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13} + C_{21}))(x-1))] \\ & +y[x(C_{32} - P(A_2/S)(C_{13} + C_{21})) - (C_{32} - P(A_2/S)(C_{13} + C_{21}))(x-1)]].\end{aligned} \tag{24}$$

Let f be a multivariate function. We can observe from (18), (20), (22), and (24) that the system of equations below defines the game.

$$\begin{cases} f(x) & = \frac{dx}{dt} \\ f(y) & = \frac{dy}{dt} \\ f(z_1) & = \frac{dz_1}{dt} \\ f(z_2) & = \frac{dz_2}{dt} \end{cases} \tag{25}$$

4.2. Conditions for ESS

Any solution of the system defined in (25) is a Nash equilibrium of the proposed evolutionary game. Moreover, any stable equilibrium of the replicator equations is an ESS. A Jacobian matrix can be used to analyze the stability of the equilibrium solutions [38].

4.2.1. Nash Equilibrium

In each Nash equilibrium, any agent (player) cannot improve its own payoff if other players do not change their strategies. This situation can be interpreted as a steady state of the system as a result of individuals' rational decision-making for payoff maximization. A pure strategy Nash equilibrium refers to a game in which every player's mixed strategy in a mixed strategy Nash equilibrium assigns probability 1 to a single action [39]. A mixed strategy Nash equilibrium refers to a game in which every player plays a mixed strategy (i.e., a probability distribution over the pure strategies) and cannot improve his or her payoff

under the mixed-strategy profile. In an attack–defense game, we use the Nash equilibrium to identify the best set of actions that maximize the defenders' payoff against cyberattacks.

We solve (25) to identify the Nash equilibrium solutions of the proposed game. With $f(x) = f(y) = f(z_1) = f(z_2) = 0$, we obtain 22 solutions. Thus, the proposed evolutionary game admits 22 Nash equilibrium solutions: 12 pure solutions and 10 mixed solutions. According to Abass et al. [16], when the game is asymmetric only the pure solutions are necessary to build the Jacobian matrix. The pure Nash equilibrium solutions of the proposed game are $E_1 = (0,0,0,0); E_2 = (1,0,0,0); E_3 = (0,1,0,0); E_4 = (0,0,1,0); E_5 = (0,0,0,1); E_6 = (1,1,0,0); E_7 = (1,0,1,0); E_8 = (0,1,1,0); E_9 = (1,0,0,1); E_{10} = (0,1,0,1); E_{11} = (1,1,1,0); E_{12} = (1,1,0,1)$.

4.2.2. Jacobian Matrix

We can use the Jacobian matrix to analyze the signs of eigenvalues and evaluate the stability of the Nash equilibrium solutions that we found above. Let J be the Jacobian matrix of the multivariate function f.

$$\mathbf{J} = \begin{bmatrix} \frac{\partial f(x)}{\partial x} & \frac{\partial f(x)}{\partial y} & \frac{\partial f(x)}{\partial z_1} & \frac{\partial f(x)}{\partial z_2} \\ \frac{\partial f(y)}{\partial x} & \frac{\partial f(y)}{\partial y} & \frac{\partial f(y)}{\partial z_1} & \frac{\partial f(y)}{\partial z_2} \\ \frac{\partial f(z_1)}{\partial x} & \frac{\partial f(z_1)}{\partial y} & \frac{\partial f(z_1)}{\partial z_1} & \frac{\partial f(z_1)}{\partial z_2} \\ \frac{\partial f(z_2)}{\partial x} & \frac{\partial f(z_2)}{\partial y} & \frac{\partial f(z_2)}{\partial z_1} & \frac{\partial f(z_2)}{\partial z_2} \end{bmatrix} \tag{26}$$

4.2.3. Equilibrium Stability Analysis

This section studies the stability of the equilibrium solutions. Among the existing Nash equilibrium solutions, $E_1 = (0,0,0,0)$, $E_2 = (1,0,0,0)$, $E_3 = (0,1,0,0)$, and $E_6 = (1,1,0,0)$ are desirable solutions. As a matter of fact, the proposed game is based on attack–defense strategies in which the defenders' strategies consist of investing in cybersecurity, i.e., playing 1 (S or T), in order to protect themselves effectively against cyberattacks. It is obvious that the ultimate and invariable condition that guarantees that the defenders will always be safe regardless of their choice of strategy is the absence of attacks, i.e., when the attacker plays $(0,0)$.

We analyze the sign of the eigenvalues of the Jacobian matrices, i.e., $J(E_1), \ldots, J(E_{12})$, obtained using the respective corresponding solutions, i.e., $E_1, \ldots, E_{12}$. An equilibrium solution E_p (with $p = 1, \ldots, 12$) is asymptotically stable if the eigenvalues obtained from $J(E_p)$ have all-negative real parts. Table 4 presents the results of the equilibrium stability analysis. The eigenvalues associated with each equilibrium solution, i.e., $J(E_p)$, are real; on the other hand, the sign of each eigenvalue depends on the Nash equilibrium.

Thus, we have the following theorem.

Theorem 1. *The proposed evolutionary game admits a unique ESS. Only $E_6 = (1,1,0,0)$ satisfies the conditions for asymptotic stability ($\lambda_q < 0$, where $q = 1, \ldots, 4$).*

Proof. We show that the eigenvalues of E_6 are all negative. Then, we demonstrate that the other Nash equilibrium solutions have at least one positive eigenvalue.

- *E_6 is asymptotically stable.*

The eigenvalues of E_6 are $\lambda_1 = C_{12} - R_{11}$, $\lambda_2 = C_{20} - P_{20} + P_{21} - R_{20}$, $\lambda_3 = C_{14}P(A_1/T) - C_{30}$, and $\lambda_4 = (C_{13} + C_{21})P(A_2/S) - C_{32}$.

First, we have $\lambda_1 < 0$, because $R_{11} > C_{12}$ (15). Then, we have $\lambda_2 < 0$, because $P_{20} + R_{20} > C_{20} + P_{21}$ (16). Next, we have $\lambda_3 < 0$, because $C_{30} > C_{14}P(A_1/T)$ (13). Finally, we have $\lambda_4 < 0$, because $C_{32} > (C_{13} + C_{21})P(A_2/S)$ (14). The eigenvalues λ_1, λ_2, λ_3, and λ_4 are negative. Therefore, E_6 is asymptotically stable.

- *The other Nash equilibrium solutions are not asymptotically stable.*

Table 4. Summary of equilibrium stability analysis.

Pure Nash Equilibrium Solutions	Eigenvalues				Sign of Eigenvalues	Conditions for Asymptotic Stability	ESS
	λ_1	λ_2	λ_3	λ_4			
$E_1 = (0,0,0,0)$	$R_{11} - C_{12}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/\bar{T}) - C_{31}$	$(C_{13} + C_{21})P(A_2/\bar{S}) - C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ $\lambda_3 > 0$ $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_2 = (1,0,0,0)$	$C_{12} - R_{11}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/T) - C_{30}$	$(C_{13} + C_{21})P(A_2/\bar{S}) - C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ $\lambda_3 < 0$ $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_3 = (0,1,0,0)$	$R_{11} - C_{12}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/\bar{T}) - C_{31}$	$(C_{13} + C_{21})P(A_2/S) - C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ $\lambda_3 > 0$ $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_4 = (0,0,1,0)$	$(C_{13} + C_{14})[P(A_1/\bar{T}) - P(A_1/T)] + R_{11} - C_{12}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(-C_{13} - C_{14})P(A_1/\bar{T}) + C_{31}$	$(-C_{13} - C_{14})P(A_1/\bar{T}) + (C_{13} + C_{21})P(A_2/\bar{S}) + C_{31} - C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ $\lambda_3 < 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_5 = (0,0,0,1)$	$R_{11} - C_{12}$	$C_{21}[P(A_2/\bar{S}) - P(A_2/S)] + P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/\bar{T}) + (-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33} - C_{31}$	$(-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33}$	$\lambda_1 > 0$ $\lambda_2 > 0$ Uncertain $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_6 = (1,1,0,0)$	$C_{12} - R_{11}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/T) - C_{30}$	$(C_{13} + C_{21})P(A_2/S) - C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✓
$E_7 = (1,0,1,0)$	$(C_{13} + C_{14})[P(A_1/T) - P(A_1/\bar{T})] + C_{12} - R_{11}$	$P_{20} - C_{20} - P_{21} + R_{20}$	$(-C_{13} - C_{14})P(A_1/T) + C_{30}$	$(-C_{13} - C_{14})P(A_1/T) + (C_{13} + C_{21})P(A_2/\bar{S}) + C_{30} - C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ $\lambda_3 > 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗

Table 4. *Cont.*

Pure Nash Equilibrium Solutions	Eigenvalues				Sign of Eigenvalues	Conditions for Asymptotic Stability	ESS
	λ_1	λ_2	λ_3	λ_4			
$E_8 = (0,1,1,0)$	$C_{14}[P(A_1/\bar{T}) - P(A_1/T)] + R_{11} - C_{12}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$-C_{14}P(A_1/\bar{T}) + C_{31}$	$-C_{14}P(A_1/\bar{T}) + (C_{13} + C_{21})P(A_2/S) + C_{31} - C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_9 = (1,0,0,1)$	$C_{12} - R_{11}$	$C_{21}[P(A_2/\bar{S}) - P(A_2/S)] + P_{20} - C_{20} - P_{21} + R_{20}$	$(C_{13} + C_{14})P(A_1/T) + (-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33} - C_{30}$	$(-C_{13} - C_{21})P(A_2/\bar{S}) + C_{33}$	$\lambda_1 < 0$ $\lambda_2 > 0$ Uncertain $\lambda_4 < 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{10} = (0,1,0,1)$	$R_{11} - C_{12}$	$C_{21}[P(A_2/S) - P(A_2/\bar{S})] + C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/\bar{T}) + (-C_{13} - C_{21})P(A_2/S) + C_{32} - C_{31}$	$(-C_{13} - C_{21})P(A_2/S) + C_{32}$	$\lambda_1 > 0$ $\lambda_2 < 0$ Uncertain $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{11} = (1,1,1,0)$	$C_{14}[P(A_1/T) - P(A_1/\bar{T})] + C_{12} - R_{11}$	$C_{20} - P_{20} + P_{21} - R_{20}$	$-C_{14}P(A_1/T) + C_{30}$	$-C_{14}P(A_1/T) + (C_{13} + C_{21})P(A_2/S) + C_{30} - C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 > 0$ Uncertain	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗
$E_{12} = (1,1,0,1)$	$C_{12} - R_{11}$	$C_{21}[P(A_2/S) - P(A_2/\bar{S})] + C_{20} - P_{20} + P_{21} - R_{20}$	$C_{14}P(A_1/T) + (-C_{13} - C_{21})P(A_2/S) + C_{32} - C_{30}$	$(-C_{13} - C_{21})P(A_2/S) + C_{32}$	$\lambda_1 < 0$ $\lambda_2 < 0$ Uncertain $\lambda_4 > 0$	$\lambda_1 < 0$ $\lambda_2 < 0$ $\lambda_3 < 0$ $\lambda_4 < 0$	✗

The eigenvalue λ_1 of Nash equilibrium solutions E_1, E_3, E_4, E_5, E_8, and E_{10} is positive because of (15). The eigenvalue λ_2 of E_2 and E_7 is positive because of (16). Similarly, the eigenvalue λ_2 of E_9 is positive because of (2), (7), and (16). From (13), we can see that the eigenvalue λ_3 of E_{11} is positive. Moreover, the eigenvalue λ_4 of E_{12} is positive because of (14). As a result, the Nash equilibrium solutions E_p (with $p = 1, \ldots, 12, p \neq 6$) have at least one positive eigenvalue. For this reason, they are not asymptotically stable. □

5. Numerical Results

This section presents the results of simulations based on the analyses conducted in Section 4. First, we show graphically that E_6 is an ESS. Next, we investigate the impacts of cybersecurity investment costs and benefits on E_6. We choose the parameter settings described in Table 5 to illustrate the numerical results.

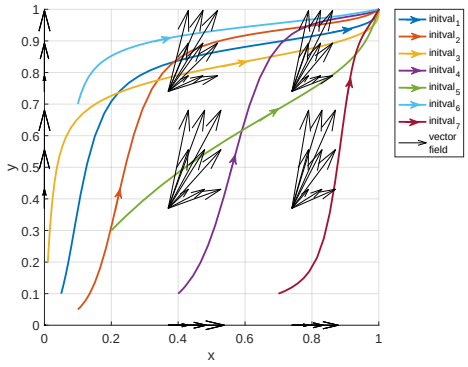
Table 5. List of parameter values used in the numerical results.

Parameters	Values
$P(A_1/T)$	0.3
$P(A_1/\bar{T})$	0.6
$P(A_2/S)$	0.1
$P(A_2/\bar{S})$	0.8
C_{12}	0.1
C_{13}	0.2
C_{14}	0.6
C_{20}	0.2
C_{21}	0.8
C_{30}	0.4
C_{31}	0.15
C_{32}	0.7
C_{33}	0.25
P_{20}	0.25
P_{21}	0.1
R_{11}	0.2
R_{20}	0.15
Seven kinds of initial values $(x(0), y(0), z_1(0), z_2(0))$: $initval_1, \ldots, initval_7$	(0.05, 0.1, 0.4, 0.5); (0.1, 0.05, 0.2, 0.3); (0.01, 0.2, 0.6, 0.3); (0.4, 0.1, 0.3, 0.6); (0.2, 0.3, 0.4, 0.1); (0.1, 0.7, 0.1, 0.2); (0.7, 0.1, 0.3, 0.1).

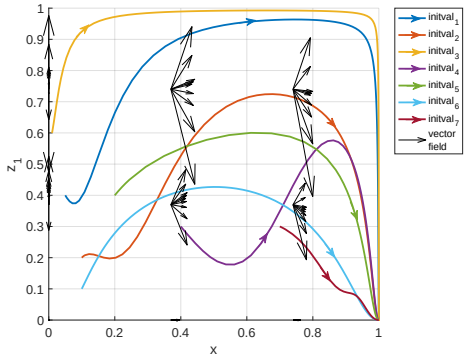
5.1. Numerical Validation of the Stability of E_6

We start by demonstrating that the proposed system is asymptotically stable by using the n-dimensional phase portraits by state combinations [40]. According to this method, Figure 3 illustrates the phase portrait views for the $m = 6$ combinations of states where $m = \frac{n!}{2(n-2)!}$ with $n = 4$. In addition to the vector fields, we plot the system trajectories using different colored lines (blue, brown, orange, purple, green, cyan, and maroon) based on the seven initial values described in Table 5. Figure 3a–f shows that the vector fields converge to $(x, y) = (1, 1)$, $(x, z_1) = (1, 0)$, $(x, z_2) = (1, 0)$, $(y, z_1) = (1, 0)$, $(y, z_2) = (1, 0)$, and $(z_1, z_2) = (0, 0)$, respectively. The analysis of the view of each state combination reveals that the vector fields converge to the Nash equilibrium $E_6 = (1, 1, 0, 0)$. Figure 4a,b shows the evolution of population fractions x, y, z_1, and z_2 over time under the initial values $initval_1$ and $initval_7$, respectively. We can confirm from Figure 4a,b that the system converges to the Nash equilibrium E_6. The convergence of the directional fields and the asymptotic stability of the evolution of x, y, z_1, and z_2 over time validate the correctness of our theoretical analysis regarding the stability of E_6.

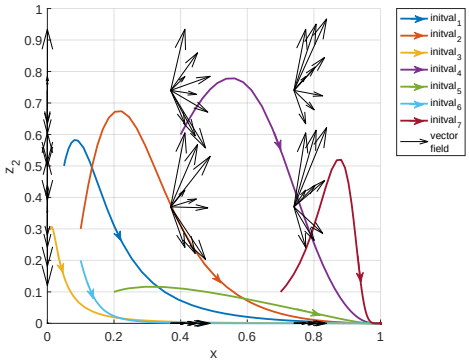
In the following, we examine the effects of various parameters on the ESS, i.e., E_6.



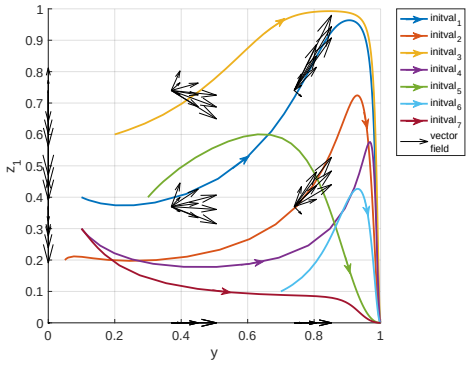
(a) Phase portrait view (x y) of the dynamic game.



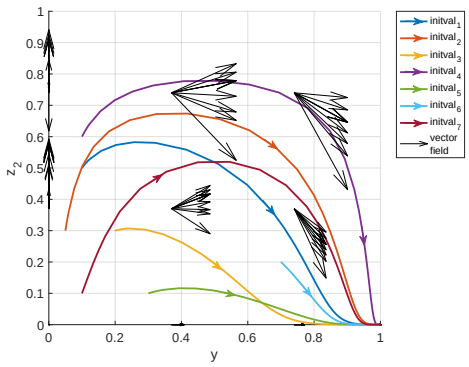
(b) Phase portrait view (x z_1) of the dynamic game.



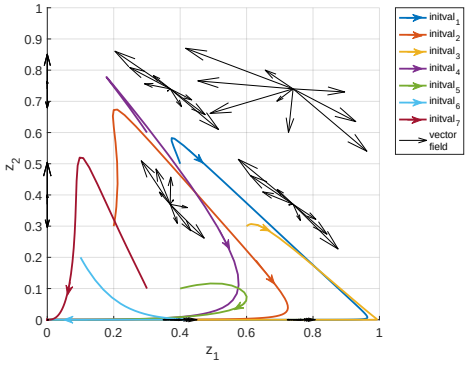
(c) Phase portrait view (x z_2) of the dynamic game.



(d) Phase portrait view (y z_1) of the dynamic game.



(e) Phase portrait view (y z_2) of the dynamic game.



(f) Phase portrait view (z_1 z_2) of the dynamic game.

Figure 3. Four-dimensional phase portraits by state combinations.

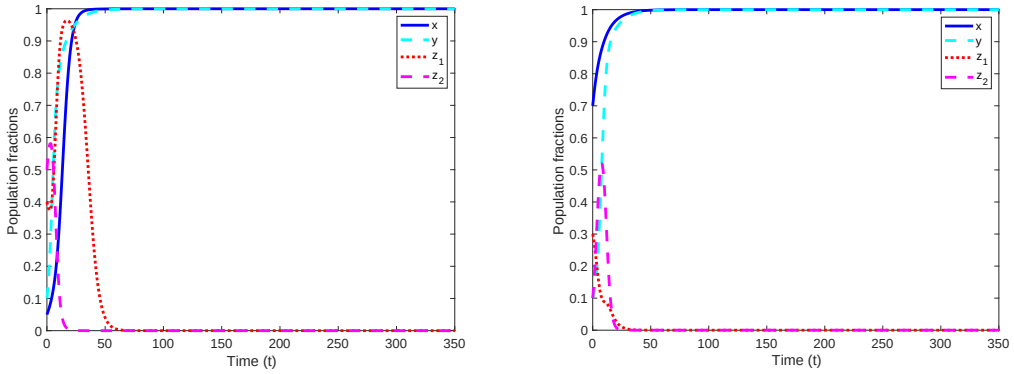


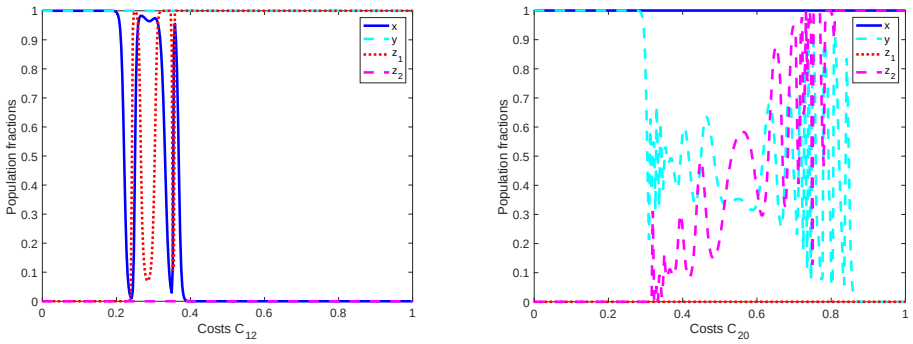
Figure 4. Population evolution of x, y, z_1, and z_2 over time. (**a**) Evolution of population fractions over time with initial values $x(0) = 0.05$, $y(0) = 0.1$, $z_1(0) = 0.4$, and $z_2(0) = 0.5$. (**b**) Evolution of population fractions over time with initial values $x(0) = 0.7$, $y(0) = 0.1$, $z_1(0) = 0.3$, and $z_2(0) = 0.1$.

5.2. Analyzing the Effects of Cybersecurity and Cyberattack Costs on E_6

We have shown that E_6 can be a desirable ESS under the rational conditions provided in Section 3.2. In actual systems, however, certain parameter settings may violate the rational conditions due to various reasons, e.g., mis-estimation of costs, profits, and/or rewards. In this section, we first classify the cost, profit, and reward parameters into four categories: cybersecurity costs, rewards for commitment to cybersecurity, cyberattack costs, and costs of setting up cyberattack operations. Then, we numerically evaluate how these affect the system stability and change its equilibrium. We use the initial values $initval_1$ of variables, as in Figure 4a, and apply the parameter settings in Table 5 as default values. In the following, we show the impact of a certain parameter, e.g., C_{12}, on the system behavior by changing its value while maintaining the same values for the other parameters. Considering the convergence property in Figure 4, we show $(x(t), y(t), z_1(t), z_2(t))$ for $t = 300$ in the following simulations. We use a solid blue line, a dashed cyan line, a dotted red line, and a dashed magenta line to describe the evolution of population fractions $x(t)$, $y(t)$, $z_1(t)$, and $z_2(t)$, respectively.

5.2.1. The Impact of Cybersecurity Costs

We first focus on the cybersecurity costs (C_{12} and C_{20}) and numerically evaluate their impacts by changing one of them. Recall that $C_{12} < 0.2$ is required by (15) for making E_6 ESS. Similarly, $C_{20} < 0.3$ is required by (16). Figure 5a presents the evolution of population fractions over C_{12}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ and $E_8 = (0, 1, 1, 0)$ when $C_{12} < 0.2$ and $C_{12} > 0.38$, respectively. On the other hand, the population fractions x and z_1 fluctuate when $0.2 < C_{12} < 0.38$. Figure 5b presents the evolution of population fractions over C_{20}. The system converges to $E_6 = (1, 1, 0, 0)$ and $E_9 = (1, 0, 0, 1)$ when $C_{20} < 0.3$ and $C_{20} > 0.86$, respectively. On the other hand, the population fractions y and z_2 fluctuate when $0.3 < C_{20} < 0.86$. The evaluation of cybersecurity cost parameters shows that $C_{12} < 0.2$ and $C_{20} < 0.3$ satisfy the ESS conditions for E_6.

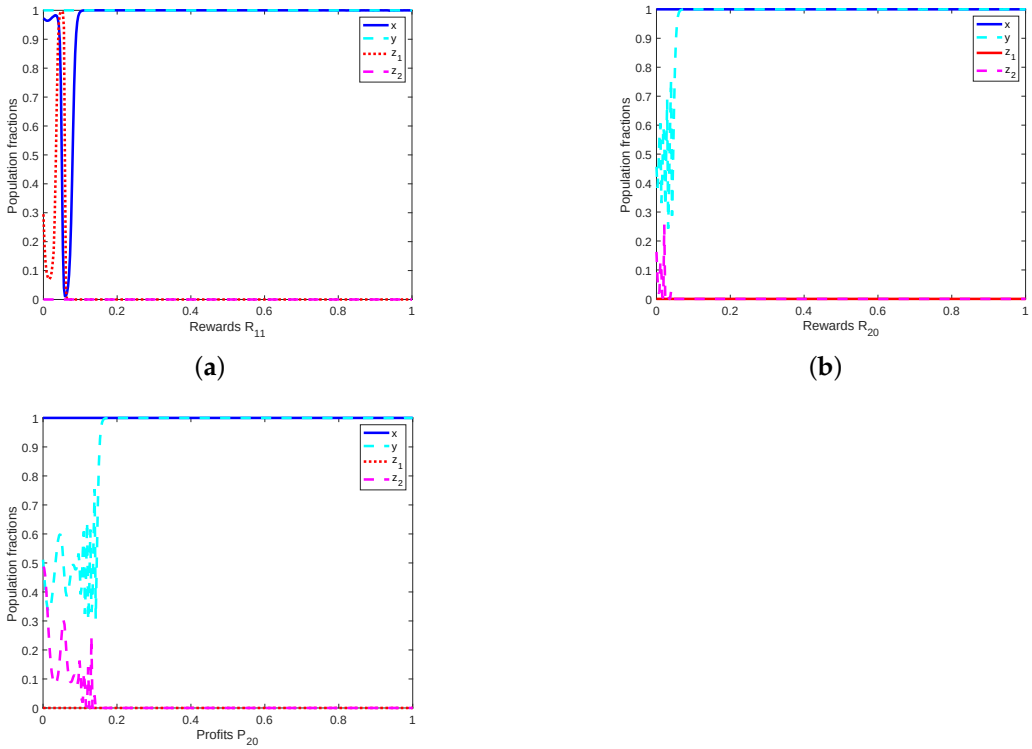


(**a**) (**b**)

Figure 5. The impact of cybersecurity costs on the ESS E_6. (**a**) Evolution of population fractions x, y, z_1, and z_2 over C_{12}. (**b**) Evolution of population fractions x, y, z_1, and z_2 over C_{20}.

5.2.2. The Impact of Rewards for Commitment to Cybersecurity

We now numerically evaluate the impacts of rewards (R_{11} and R_{20}) and profits (P_{20}) for commitment to cybersecurity. Recall that $R_{11} > 0.1$ is required by (15) for making E_6 ESS. Similarly, $R_{20} > 0.05$ and $P_{20} > 0.15$ are required by (16). Figure 6a presents the evolution of population fractions over R_{11}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ when $R_{11} > 0.1$. On the other hand, the population fractions x and z_1 fluctuate when $R_{11} < 0.1$. Figure 6b,c shows that the population fractions x, y, z_1, and z_2 over R_{20} and P_{20} remain constant and equivalent to E_6 when $R_{20} > 0.05$ and $P_{20} > 0.15$, respectively. When $R_{20} < 0.05$ and $P_{20} < 0.15$, y and z_2 fluctuate. The evaluation of the profit and reward parameters shows that $R_{11} > 0.1$, $R_{20} > 0.05$, and $P_{20} > 0.15$ satisfy the ESS conditions for E_6.



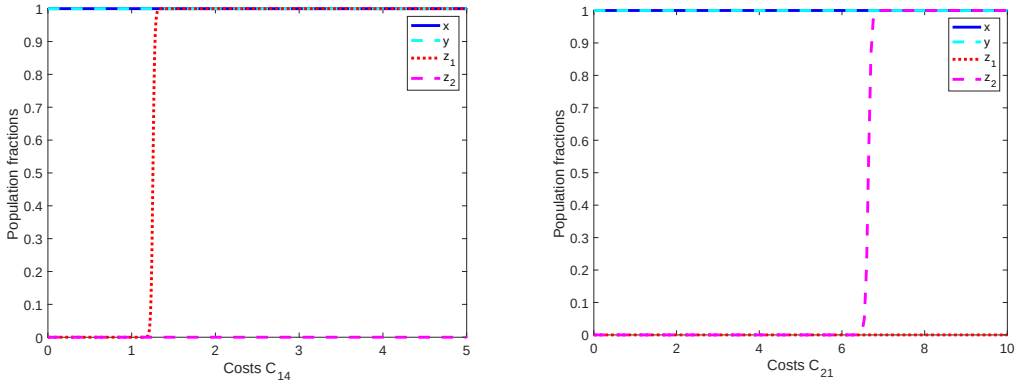
(**a**) (**b**)

(**c**)

Figure 6. The impact of rewards for cybersecurity commitment on the ESS E_6. (**a**) Evolution of population fractions x, y, z_1, and z_2 over R_{11}. (**b**) Evolution of population fractions x, y, z_1, and z_2 over R_{20}. (**c**) Evolution of population fractions x, y, z_1, and z_2 over P_{20}.

5.2.3. The Impact of Cyberattack Costs

Next, we investigate the cyberattack costs and numerically evaluate their impacts by changing one of them. Recall that $C_{14} < 0.8$ and $C_{21} > 0.6$ are required by (8) for making E_6 ESS. Figure 7a presents the evolution of population fractions over C_{14}. We can see that the system converges to $E_6 = (1, 1, 0, 0)$ when $C_{14} \leq 1.333$. Otherwise, it converges to $E_{11} = (1, 1, 1, 0)$. Figure 7b presents the evolution of population fractions over C_{21}. The system converges to E_6 when $C_{21} < 6.8$. Otherwise, it converges to $E_{12} = (1, 1, 0, 1)$. The evaluation of cyberattack costs shows that $C_{14} \leq 1.333$ and $C_{21} < 6.8$ satisfy the ESS conditions for E_6.

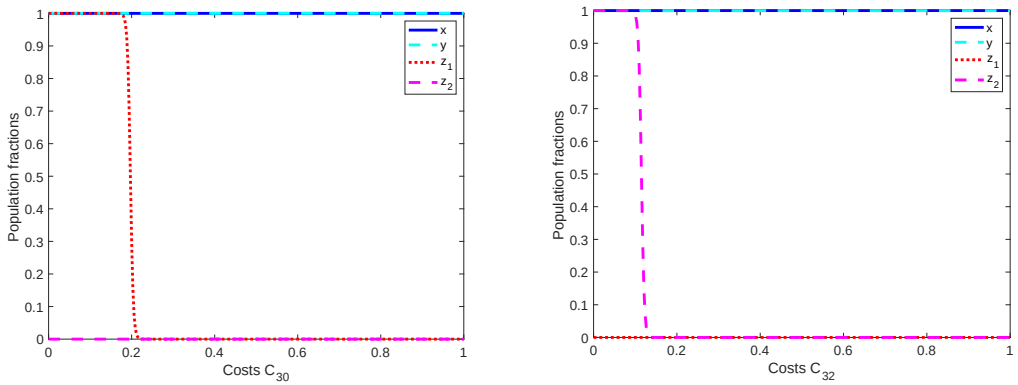


(**a**) (**b**)

Figure 7. Impact of cyberattack costs on the ESS E_6. (**a**) Evolution of population fractions x, y, z_1, and z_2 over C_{14}. (**b**) Evolution of population fractions x, y, z_1, and z_2 over C_{21}.

5.2.4. Costs of Setting Up Cyberattack Operations

Finally, we investigate the operation costs of cyberattacks and numerically evaluate their impacts by changing one of them. Recall that $C_{30} > 0.15$ is required by (9) for making E_6 ESS. Similarly, $C_{32} > 0.25$ is required by (10). Figure 8a shows that the system converges to $E_6 = (1, 1, 0, 0)$ and $E_{11} = (1, 1, 1, 0)$ when $C_{30} > 0.18$ and $C_{30} < 0.18$, respectively. Figure 8b shows that the system converges to E_6 and $E_{12} = (1, 1, 0, 1)$ when $C_{32} > 0.1$ and $C_{32} < 0.1$, respectively. The evaluation of cost parameters of implementing cyberattacks shows that $C_{30} > 0.18$ and $C_{32} > 0.1$ satisfy the ESS conditions for E_6.



(**a**) (**b**)

Figure 8. The impact of operation costs of cyberattacks on the ESS E_6. (**a**) Evolution of population fractions x, y, z_1, and z_2 over C_{30}. (**b**) Evolution of population fractions x, y, z_1, and z_2 over C_{32}.

6. Discussions

This section discusses the findings of this study, highlights its limitations, and presents avenues for future work.

6.1. Interpretation of the Results

For the purpose of verifying whether it is worthwhile for smart-home users to invest in cybersecurity over time, we defined and analyzed a smart-home ecosystem-based game model using evolutionary game theory. Our numerical results show that the best strategy set for smart-home users is $E_6 = (1, 1, 0, 0) = (T, S, A_0)$. This implies that smart-home users and smart-home stakeholders must invest in cybersecurity and follow security best practices. If they commit to cybersecurity as recommended, we find that adversaries abstain from attacking because the costs of setting up cyberattack operations are higher than the expected gain. Thus, it is beneficial for smart-home users to incur the cost of engaging in cybersecurity awareness training.

On the basis of these findings, we now discuss the essential parameters used in this study.

6.1.1. Cybersecurity Costs

The results indicate that low cybersecurity costs ($C_{12} < 0.2$ and $C_{20} < 0.3$) maintain the desired equilibrium solution E_6, while increasing costs of cybersecurity awareness training and implementing security best practices for IoT technology lead smart-home users and manufacturers to stop investing in cybersecurity strategies. This outcome is consistent with the finding that reducing investment costs promotes information security investment [30]. Moreover, smart-home users are willing to commit to cybersecurity awareness training if the training costs are zero [17]. Indeed, not all smart-home users have the means to pay for additional training outside of spending on everyday goods and services. Therefore, governments might encourage smart-home users to take an interest in cybersecurity by giving it greater prominence in national cybersecurity plans and subsidizing training costs.

6.1.2. Rewards

Our results indicate that offering rewards and benefits ($R_{11} > 0.1$, $R_{20} > 0.05$, and $P_{20} > 0.15$) based on a commitment to cybersecurity helps to maintain the desired equilibrium solution, E_6, in which smart-home users are involved in cybersecurity. These findings align with previous research [17] showing that, through a static game model, providing smart-home users with tangible rewards can engage them in cybersecurity education programs. Indeed, both financial and non-financial rewards can have positive effects on users' cybersecurity behavior [41]. From this perspective, additional research on non-financial rewards that might motivate smart-home users to engage in cybersecurity would be appropriate.

6.1.3. Cyberattack Costs

The results of this study indicate that if the respective costs incurred by cyberattacks on smart-home users and manufacturers are low ($C_{14} \leq 1.333$ and $C_{21} < 6.8$), adversaries become less interested in carrying out cyberattacks. Therefore, the desired equilibrium E_6 remains intact. This outcome is obtained because the proposed model considers that attackers incur costs to carry out cyberattacks. Even though this is true in reality, it is clear that with the sources of information available in the digital era attackers can carry out cyberattacks at almost no cost. Thus, even with low costs incurred by cyberattacks on smart-home users and manufacturers, attackers may not refrain from attacking. This pattern would break the desired equilibrium and expose smart-home users and manufacturers to potential cyberattacks. It is therefore essential to strengthen the cybersecurity of smart homes by taking into consideration international standards such as ISO/IEC 27403 [42], which is currently under development. The objective is to not tolerate any costs due to cyberattacks, thereby deterring attackers.

6.1.4. Operation Costs of Cyberattacks

Our results indicate that if the costs of setting up cyberattack operations, i.e., $C_{30} > 0.18$ and $C_{32} > 0.1$, become very expensive, adversaries abandon attack strategies, which in

turn helps to preserve the desired equilibrium solution E_6. On the other hand, the results show that smart-home users and manufacturers are continuously exposed to cyberattacks when the costs of implementing cyberattacks are low or negligible. In an increasingly digitalized world, attackers can afford to develop targeted attack scenarios that could have a significant global impact at little or no cost. Based on this observation, it is apparent that if attackers can develop attacks at a lower cost, it is necessary to in turn allow smart-home users to become educated and trained in cybersecurity at a lower cost. Thus, it is important to ensure cybersecurity for all, by all, and of all in the near future in order to lessen the likelihood of successful cyberattacks.

6.2. Limitations and Future Work

The existing literature on cost–benefit analysis of cybersecurity investment for individuals such as smart-home users is limited. This may be because home users in the past were not as exposed to cyberattacks as they are today in an increasingly digitalized world. It should be stressed that cyberattacks on smart-home users can affect their physical and moral security. As such, we encourage more research on the cybersecurity of smart-home users to protect users from these risks.

Regarding the proposed model, it is essential to note that the smart-home environment includes several independent stakeholders, such as IoT device manufacturers, network providers, and cloud service providers. For the sake of simplicity, we have grouped them into a single entity, i.e., $population_2$, to provide a holistic study, as in essence all of these entities must choose between investing or not investing in cybersecurity. We recommend additional research to model the interaction between smart-home users and different stakeholder groups. Moreover, in our model the attacker can target smart-home users either directly or indirectly via stakeholders, and cannot target smart-home users and stakeholders at the same time. Future research might address the latter scenario.

It is challenging to accurately model the real world with its numerous variables using only a few parameters. While our model is built on realistic assumptions, it is uncertain whether it perfectly captures the reality of smart-home users. To enhance the practicality of our results, future studies must design more sophisticated game models that illustrate greater depth and volume of agents' choices in order to improve the applicability of the findings. Using the Monte Carlo method to simulate such a model is an approach that we recommend. Note that we omitted Monte Carlo simulations in our results, as they were deemed redundant based on previous research [43]. This study demonstrates, both theoretically and through experimental simulations, that multi-agent simulations with Monte Carlo dynamics and evolutionary games with replicator equations produce equivalent results. This could be one of the reasons that other works [15,16] using evolutionary game theory did not compare directly their evolutionary game-based results with other methods such as Monte Carlo simulations.

Verifying the correctness of the parameter values used in our simulation is another challenge. Collecting empirical data to compare theoretical and empirical results is highly recommended. An additional limitation is related to the cost parameters used in our system. Our model focuses only on monetary costs as the study problem; future studies could consider time-related costs in the model. Indeed, while the monetary costs of conducting cyberattacks may be close to zero, the time taken to identify vulnerabilities and develop cyberattacks may be very long, and could be a determining factor that might lead the attacker to refrain from attacking.

It is worth noting that our game-theoretic approach works in reality if smart-home users observe the punishments and rewards through their experience. This evidence-based approach is one way to stress the importance of cybersecurity awareness in smart homes. However, achieving the goal of evidence-based security is just as challenging as providing evidence-based healthcare [44]. Interested researchers can investigate evidence-based effects of punishments and rewards on smart-home users' security practices and behaviors.

Furthermore, our study does not focus on the content of cybersecurity training, and assumes the effectiveness of such training in preventing cyberattacks. Considering the existence of unknown vulnerabilities, for example, it is evident that cybersecurity training cannot cover all possible vulnerabilities and attack scenarios. This is one of the reasons why our study looked at investing in cybersecurity over the long term through an evolutionary game-theoretic approach. In the real world, smart-home users have to frequently update their cybersecurity knowledge and skills in order to continuously protect themselves against cyberattacks.

Finally, it is necessary to promote strengthened IoT cybersecurity regulations, such as the European Union (EU) Cyber Resilience Act [45], to mandate security-by-design and essential cybersecurity requirements for manufacturers, importers, and distributors of IoT devices and services and ensure compliance through certification, reporting, and conformity assessments. This can reduce the need for in-depth cybersecurity awareness training on the part of smart-home users and consequently lower the cost of cybersecurity education.

7. Conclusions

In this work, we study the costs and benefits of cybersecurity investment strategies for smart-home users through an evolutionary game-theoretic approach. We aim to demonstrate the long-term advantages of investing in cybersecurity for smart-home users, as the cost of cybersecurity training can be a barrier for many individuals. To achieve this, we model the interactions between smart-home users, smart-home stakeholders, and attackers using different strategies and associated payoffs. The numerical results show that the optimal strategy for smart-home users involves both users and stakeholders investing in cybersecurity, thereby reducing the likelihood of successful attacks and discouraging attackers from continuing their attack efforts unless they are willing to incur losses. On the other hand, in order to prioritize cybersecurity, smart-home users must have low training costs and receive rewards for their commitment. Thus, subsidizing cybersecurity training costs and exploring non-financial rewards to motivate smart-home users are potential strategies to consider. In addition, our study highlights the importance of user behavior in securing smart homes. In our future work, we plan to investigate this further using behavioral game theory and Monte Carlo simulations. This upcoming research will provide a comprehensive understanding of how to ensure the privacy and security of individuals living in smart homes.

Author Contributions: Conceptualization, N.Y.-R.D., M.S. and Y.T.; formal analysis, N.Y.-R.D. and M.S.; supervision, Y.T. and Y.K.; writing—original draft, N.Y.-R.D.; writing—review and editing, N.Y.-R.D., M.S., Y.T. and Y.K.; funding acquisition, Y.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Industrial Cyber Security Center of Excellence (ICS-CoE) Core Human Resources Development Program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Statista. Smart Home Report 2022. 2022. Available online: https://www.statista.com/study/42112/smart-home-report/ (accessed on 10 January 2023).
2. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. *J. Inf. Secur. Appl.* **2018**, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002.
3. Furnell, S.; Bryant, P.; Phippen, A. Assessing the security perceptions of personal Internet users. *Comput. Secur.* **2007**, *26*, 410–417. https://doi.org/10.1016/j.cose.2007.03.001.

4. Furnell, S.; Tsaganidi, V.; Phippen, A. Security beliefs and barriers for novice Internet users. *Comput. Secur.* **2008**, *27*, 235–240. https://doi.org/10.1016/j.cose.2008.01.001.
5. Tomczyk, Ł.; Potyrała, K. Parents' knowledge and skills about the risks of the digital world. *S. Afr. J. Educ.* **2021**, *41*, 1–19. https://doi.org/10.15700/saje.v41n1a1833.
6. D'Arcy, J.; Hovav, A.; Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inf. Syst. Res.* **2009**, *20*, 79–98.
7. Aldawood, H.; Skinner, G. Challenges of implementing training and awareness programs targeting cyber security social engineering. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia, 8–9 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 111–117.
8. Morrison, B.; Coventry, L.; Briggs, P. How do Older Adults feel about engaging with Cyber-Security? *Hum. Behav. Emerg. Technol.* **2021**, *3*, 1033–1049. https://doi.org/10.1002/hbe2.291.
9. Zhang, Z.J.; He, W.; Li, W.; Abdous, M. Cybersecurity awareness training programs: a cost-benefit analysis framework. *Ind. Manag. Data Syst.* **2021**, *121*, 613–636.
10. Douha, N.Y.R.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager. In Proceedings of the Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021), Athens, Greece, 14–18 November 2021; pp. 31–40.
11. Krichen, M.; Alroobaea, R. A New Model-Based Framework for Testing Security of IoT Systems in Smart Cities Using Attack Trees and Price Timed Automata. In Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2019), Setubal, Portugal, 4–5 May 2019; pp. 570–577. https://doi.org/10.5220/0007830605700577.
12. Tabrizi, F.M.; Pattabiraman, K. Formal Security Analysis of Smart Embedded Systems. In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC '16), New York, NY, USA, 5–7 April 2016; pp. 1–15. https://doi.org/10.1145/2991079.2991085.
13. Kumar, P.; Braeken, A.; Gurtov, A.; Iinatti, J.; Ha, P.H. Anonymous Secure Framework in Connected Smart Home Environments. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 968–979. https://doi.org/10.1109/TIFS.2016.2647225.
14. Sandholm, W. Evolutionary Game Theory in Encyclopedia of Complexity and System Science, 2009.
15. Tosh, D.; Sengupta, S.; Kamhoua, C.; Kwiat, K.; Martin, A. An evolutionary game-theoretic framework for cyber-threat information sharing. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7341–7346. https://doi.org/10.1109/ICC.2015.7249499.
16. Alabdel Abass, A.A.; Xiao, L.; Mandayam, N.B.; Gajic, Z. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access* **2017**, *5*, 8482–8491. https://doi.org/10.1109/ACCESS.2017.2691326.
17. Douha, N.Y.R.; Sane, B.O.; Sasabe, M.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. Cost-benefit Analysis Toward Designing Efficient Education Programs for Household Security . In Proceedings of the Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021), Athens, Greece, 14–18 November 2021; pp. 59–68.
18. Kritzinger, E.; von Solms, S. Cyber security for home users: A new way of protection through awareness enforcement. *Comput. Secur.* **2010**, *29*, 840–847. https://doi.org/10.1016/j.cose.2010.08.001.
19. Howe, A.E.; Ray, I.; Roberts, M.; Urbanska, M.; Byrne, Z. The Psychology of Security for the Home Computer User. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 209–223. https://doi.org/10.1109/SP.2012.23.
20. Alotaibi, F.; Clarke, N.; Furnell, S. An analysis of home user security awareness & education. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 116–122. https://doi.org/10.23919/ICITST.2017.8356359.
21. Ricci, J.; Breitinger, F.; Baggili, I. Survey results on adults and cybersecurity education. *Educ. Inf. Technol.* **2019**, *24*, 231–249.
22. Pattnaik, N.; Li, S.; Nurse, J.R. A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *ACM Comput. Surv.* **2022**. *just accepted*. https://doi.org/10.1145/3558095.
23. Cavusoglu, H.; Raghunathan, S.; Yue, W.T. Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *J. Manag. Inf. Syst.* **2008**, *25*, 281–304. https://doi.org/10.2753/MIS0742-1222250211.
24. Douha, N.Y.R.; Bhuyan, M.; Kashihara, S.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. A survey on blockchain, SDN and NFV for the smart-home security. *Internet Things* **2022**, *20*, 100588. https://doi.org/10.1016/j.iot.2022.100588.
25. Nagurney, A.; Nagurney, L.S. A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS Econ. Res. Electron. Netw.* **2015**, *16*, 127–148. https://doi.org/10.1007/s11066-015-9094-7.
26. Nagurney, A.; Nagurney, L.S.; Shukla, S. A supply chain game theory framework for cybersecurity investments under network vulnerability. In *Computation, Cryptography, and Network Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 381–398.
27. Nagurney, A.; Daniele, P.; Shukla, S. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Ann. Oper. Res.* **2017**, *248*, 405–427.
28. Tosh, D.K.; Vakilinia, I.; Shetty, S.; Sengupta, S.; Kamhoua, C.A.; Njilla, L.; Kwiat, K. Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance. In *Proceedings of the Decision and Game Theory for Security*; Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S., Eds.; Springer: Cham, Switzerland, 2017; pp. 519–532.

29. Hyder, B.; Govindarasu, M. Optimization of Cybersecurity Investment Strategies in the Smart Grid Using Game-Theory. In Proceedings of the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2020; pp. 1–5. https://doi.org/10.1109/ISGT45199.2020.9087634.
30. Sun, W.; Kong, X.; He, D.; You, X. Information Security Problem Research Based on Game Theory. In Proceedings of the 2008 International Symposium on Electronic Commerce and Security, Guangzhou, China, 3–5 August 2008; pp. 554–557. https://doi.org/10.1109/ISECS.2008.147.
31. Smith, J.M. Game theory and the evolution of fighting. In *On Evolution*; Edinburgh University Press: Edinburgh, UK, 1972; pp. 8–28.
32. Smith, J.; Price, G.R. The logic of animal conflict. *Nature* **1973**, *246*, 15–18.
33. Nash, J. Non-cooperative games. *Ann. Math.* **1951**, *54*, 286–295.
34. Morgenstern, O.; Von Neumann, J. *Theory of Games and Economic Behavior*; Princeton University Press: Princeton, NJ, USA, 1953.
35. Cressman, R.; Tao, Y. The replicator equation and other game dynamics. *Proc. Natl. Acad. Sci. USA* **2014**, *111*, 10810–10817. https://doi.org/10.1073/pnas.1400823111.
36. IBM. X-Force Threat Intelligence Index 2022. 2022. Available online: https://www.ibm.com/security/data-breach/threat-intelligence/ (accessed on 17 January 2023).
37. Sandholm, W.H., Evolutionary Game Theory. In *Encyclopedia of Complexity and Systems Science*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 1–38. https://doi.org/10.1007/978-3-642-27737-5_188-3.
38. Friedman, D. Evolutionary Games in Economics. *Econometrica* **1991**, *59*, 637–666.
39. Osborne, M.J. *An Introduction to Game Theory*; Oxford University Press: New York, NY, USA, 2004; Volume 3.
40. Rodríguez-Licea, M.A.; Perez-Pinal, F.J.; Nuñez-Pérez, J.C.; Sandoval-Ibarra, Y. On the n-Dimensional Phase Portraits. *Appl. Sci.* **2019**, *9*, 872. https://doi.org/10.3390/app9050872.
41. Acquisti, A.; Adjerid, I.; Balebako, R.; Brandimarte, L.; Cranor, L.F.; Komanduri, S.; Leon, P.G.; Sadeh, N.; Schaub, F.; Sleeper, M.; et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* **2017**, *50*, 1–41. https://doi.org/10.1145/3054926.
42. *ISO/IEC CD 27403.2*; Cybersecurity—IoT security and privacy— Guidelines for IoT-domotics. ISO: London, UK, 2022. Available online: https://www.iso.org/standard/78702.html (accessed on 17 January 2023).
43. Sasaki, Y. *The Equivalence of Evolutionary Games and Distributed Monte Carlo Learning*; Economic Research Institute Study Papers; Utah State University: Logan, UH, USA, 2004.
44. DeKoven, L.F.; Randall, A.; Mirian, A.; Akiwate, G.; Blume, A.; Saul, L.K.; Schulman, A.; Voelker, G.M.; Savage, S. Measuring Security Practices. *Commun. ACM* **2022**, *65*, 93–102. https://doi.org/10.1145/3547133.
45. European Commission. State of the Union: EU Cyber Resilience Act—Questions & Answers. 2022. Available online: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375 (accessed on 24 January 2023).