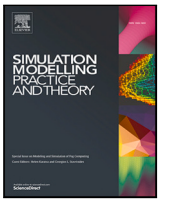
Simulation Modelling Practice and Theory 116 (2022) 102493

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat



Advancing the concept of cybersecurity as a public good

Mazaher Kianpour *, Stewart James Kowalski, Harald Øverby

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway

ARTICLE INFO

Keywords:
Cybersecurity economics
Social preferences
Public goods
Agent-based modeling
Collective actions
Heterogeneous preferences
Polycentric governance structure

ABSTRACT

This paper presents an agent-based model of cybersecurity as a participatory public good. Ineffective cybersecurity measures pose serious threats and risks to the development and stability of information societies in the world. Various doctrines and thesis explore how this domain should be treated by the public and private stakeholders. One of these doctrines is cybersecurity as a public good. In this paper, we highlight divergent views about the type of cybersecurity as an economic good. Then, the paper proposes an agent-based simulation model of a repeated public goods game among a set of defenders that are in an uncertain environment with incomplete and imperfect information. In the model, defenders have a probability to choose contribution or being a free-rider, depending on their own preferences and facing with revealed preferences of other defenders. This model implements a utility maximization that applies to each individual, modeling the existence of free-riders, punishments, and interdependency of decisions under a polycentric governance structure. The results of this simulation model show that, over time, defenders update their preferences in reaction to the behavior of other defenders and the experience of cyber-attacks. They indicate a high level of contribution to the provision of cybersecurity as a public good and the effectiveness of decentralized punishment on increasing the contributions. The consistency of the pattern of our results across different empirical studies lends us some reassurance that our model behavior is in quantitative agreement with empirical macro-structures. Furthermore, implementation of a polycentric structure challenges all the relevant agents to take action, and provides more robust environment.

1. Introduction

Evolving malicious cyber activities and increasing cyber risks to individuals, organizations and governments has made cybersecurity a significant challenge and core part of the societal, political and economic decisions [1,2]. The Global Risks Report 2021, published by the World Economic Forum, has categorized cybersecurity failures as the clear and present dangers [3]. This category reveals concern about lives and livelihoods — among them infectious diseases, employment crises, digital inequality and youth disillusionment. Moreover, the increasing value of these assets is becoming more attractive to those who wish to penetrate systems for financial gains, psychological, and reputations gains, or to cause instability. Ensuring cybersecurity through greater awareness and strong multi-stakeholders partnership are crucial for achieving Sustainable Development Goals in a hyper-connected world and societies that rely on digital infrastructure [4]. These features make cybersecurity a global issue that knows no boundaries. Hence, investment in cybersecurity and how this domain should be treated by the public and private sectors has been at issue over the course of the last decade. It also has been controversial if we can avert the tragedy of commons within the context of cybersecurity [5,6].

* Corresponding author.
E-mail addresses: mazaher.kianpour@ntnu.no (M. Kianpour), stewart.kowalski@ntnu.no (S.J. Kowalski), haraldov@ntnu.no (H. Øverby).

https://doi.org/10.1016/j.simpat.2022.102493
Received 27 July 2021; Received in revised form 22 October 2021; Accepted 6 January 2022
Available online 19 January 2022

Cybersecurity covers a vast domain that includes designing and development of robust systems against attacks, deployment of methods to detect anomalies and guarantee the system's resilience, and defining response and recovery mechanisms to attacks. Every aspect of cybersecurity is involved in achieving secure, safe, and dependable systems from initial security requirements specification and threat assessment to the provision of all required protective mechanisms, product selections and system security testing. In 2011, Mulligan and Schneider proposed to frame and manage cybersecurity as a public good [7]. While Mulligan doctrine demonstrates rational, defensible and legitimate arguments, it has not gone beyond an acknowledgment that the benefits of cybersecurity are to some degree non-rivalrous and non-excludable. They have not explored the aspects of both cybersecurity and public goods that contribute on efficiency and effectiveness of cybersecurity provision. On the basis of a general interpretation of the theory of public goods, developed by Samuelson, the notion of cybersecurity as a public good aims to reaffirm a collective responsibility to develop cybersecurity and manage cyber-insecurity. This perspective would create the much-needed overarching policy principle to define objectives and means, to bring cohesion to sectoral and specific, purpose-led policies and programs [8]. The leading role of the governments in cybersecurity policies, processes and practices is however increasingly being questioned, largely as a result of the changing dynamics in the global cybersecurity landscape. This is characterized by the increasing involvement of non-state actors in cybersecurity policy and provision, and interconnected trends that result in a dramatic shift in how cybersecurity is managed.

This work is an extension our earlier work in [9] where we focused on heterogeneous preferences and contribution pattern of agents in providing cybersecurity as a public good. In this study, we are not trying to provide normative justification for governments to invest more heavily in cybersecurity as a public good. Conversely, we aim to investigate whether this idea matches the existing theories and how this doctrine affects the resilience of such dynamic and uncertain environments like digital ecosystems. The purpose of our study is two-fold: (i) to construct an agent-based model that captures the main elements of public goods theory (i.e. free-riders problem, effectiveness of punishment, and collective action) and investigate whether it complies with the unique characteristics of cybersecurity (i.e. dynamic and uncertain environment with incomplete and imperfect information, and difficulty in assessing the cybersecurity value and cyber risks), and (ii) to characterize and study the cybersecurity posture under different settings where agents contribute to provide security measures that their benefits are not excludable and rivalrous. We look at how agent-based modeling (ABM) can contribute to exploring macro outcomes of collective contributions of agents to provide cybersecurity as a public good while considering the heterogeneous social preferences of agents. Introduction of social preferences into this model provides us with a better understanding how agents behavior deviates them from the standard model of utility maximization.

We summarize our main contributions of this work as follows:

- Problem formulation: To our best knowledge, this is the first work that quantitatively addresses cybersecurity provision problem from the perspective of public goods theory. In particular, we model and simulate the heterogeneous preferences and patterns of contribution in cybersecurity as a public good.
- Provision mechanism design: We implement a polycentric governance structure to describe a process of decision making where multiple independent actors interact to produce an outcome that is commonly valued. Our scheme can incentivize the agents to participate in the mechanism, and can achieve several desirable security properties such as enhanced cybersecurity posture in the environment and budget balanced.
- The characterization and exploration the impact of different parameters on the agents' evolving strategies and cybersecurity posture when cybersecurity is treated as a public good.

This paper proceeds first by reviewing the types of economic goods and outlines the aspects of cybersecurity that are suggested to be treated as a public good in Section 2. Section 3 discusses how the notion of cybersecurity as a public good has developed over time. We present our basic model and simulation in Section 4. Section 5 demonstrates the results of the simulation and discusses the issues of sensitivity analysis and validation. In Section 6, we discuss the findings and compile several practical implications for promoting cybersecurity as a public good. The paper is concluded in Section 7 with suggestions for future work.

2. Background

To avoid vagueness regarding what cybersecurity entails, we use the definition suggested by [10]: the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users. However, it seems difficult to discuss whether cybersecurity is public or not without first knowing whether it is a good at all. According to economic principles, a good is an object or service that satisfies human wants and provides utility [11]. That is to say, agents value a good and are willing to pay for it. An individual, organization, or a government values cybersecurity and pays for it because they expect their utility increase by utilizing it. They do not pay for cybersecurity per se. They might be willing to pay more for products or services that are provided with top ranked companies and vendors. Rosenzweig argues that cybersecurity is not a singular good. Rather it is a bundle of various goods, some of which operate independently and others of which act only in combination [12].

In 1954, Samuelsen defines public goods as non-rival and non-excludable goods when consumed [13]. The former implies that once the good is produced, it can be consumed by other consumers at no additional cost. The latter, however, is sometimes added and specifies that consumers cannot be excluded from consumption of the good once produced. The classic understanding of a public good based on Samuelson's taxonomy has been much debated and modified over time. Galbraith suggests that public goods are things that do not lend themselves to market production, purchase, and sale. They must be provided for everyone if they are

Table 1
Typology of Economic Goods.

	Rivalrous	Non-rivalrous
Excludable	Private goods *(Cars, apples)*	Club goods *(museum, cable television network)*
Non-excludable	Common Goods *(oil well, national forest)*	Public goods *(national defense, country's financial stability)*

to be provided for anyone, and they must be paid for collectively or they cannot be had at all [14]. However, since Samuelson's definition of types of economic goods has been the base of all discussions on cybersecurity as a public good, this study also relies on this definition. Using rivalrous and excludable characteristics, economic goods can be categorized into four main types. Table 1 shows the typology of economic goods and two examples of each type.

According to the typology represented in Table 1, many security systems such as anti-virus software, intrusion prevention systems, and network firewalls are private goods. However, there are other aspects of cybersecurity, such as threat intelligence and vulnerability information sharing, collective response to cyber-attacks, integrity of elections, and critical infrastructure protection, that have the characteristics of public goods [15]. Goods with the characteristics of public goods are often produced with some form of public assistance (e.g. taxation or other mandates). Accurate production and provision of these goods compared to the level that would be best for society is the main challenge of policy makers. Consumption of a public good by an end-user does not necessarily have to be free of charge, however, it is essential that its costs do not become a discriminating factor, and consequently, determining access and use of it. Some public goods are best created by direct government provisioning, while other may be best created by the all beneficiaries as a participatory public good. Participatory public goods are created best by changing individuals and organizations' incentives through different policies and regulations. For example, there are many reasons (e.g., risk of loss of reputation and trust, liability, negative effects on financial markets, and signals of weakness to adversaries [16]) that why an organization may be reluctant to share information threats and vulnerabilities in its systems. Treating such information as a public good tends to overcome these issues.

It is necessary to consider economic goods not only in their original forms, but also as social constructs and as a result of deliberative policy choices [17]. According to Hagedorn [18] and Kaul [19], with the evolution of social institutions, many goods have developed into mixed types, showing both exclusive and non-exclusive characteristics, since they might change as a result of new technologies, or different policies and regulations that are implemented. Kaul and Mendoza proposed a conceptual framework to evaluate the publicness of the goods according to this perspective [19]. Their framework examines goods according to three criteria.

- Publicness of decision-making is used to assess the participatory nature of the processes (e.g. how to distribute the benefits among the consumers) and decisions (e.g. the level and quality of production) related to the provision of the good.
- Publicness of distribution of benefits is used to assess the equity of benefits from the public goods.
- Publicness of consumption represents the non-exclusiveness across consumers.

While this framework shows an ideal situation and usually goods do not fully meet all the three criteria, it helps policymakers and the public to understand the issues to be addressed through policy tools, institutional changes and new governance settings. Other frameworks have been used to conceptualize and understand the public goods. However, features such as multi-dimensionality, multi-agent and context-dependent processes, uncertainty, and evolution, makes treating cybersecurity as a public good a special topic in public goods economics. Therefore, this study adds to the literature by further extending focus from descriptive discussions to quantitative analysis using an agent-based model.

3. State of the art

The necessity for public–private collaboration, multifaceted strategies, and recognition of the significant role that industry plays in securing the information networks have been the fundamental notions of approaches to cybersecurity in the past decade [20,21]. However, with the raise of dependencies on critical infrastructures and increasing concerns about the consequences of possible cyber–physical incidents, many governments and super-national organizations like European Union (EU) are concerned with the possible failure of the private sector in delivering acceptable level of security in the society without governmental intervention [22,23]. This shift of the concept has lead to the proposals which suggest that cybersecurity needs to be treated as a public good.

Taddeo argues that considering cybersecurity as a public good will be a step in the right direction to support policy and governance approaches that will foster robust, open, pluralistic, and stable information societies [24]. She elaborates managing cybersecurity as a public good brings the advantages of systemic approaches to security, shared responsibilities among different stakeholders; and facilitation of collaboration. Asllani et al. also explores the role of establishing an appropriate legal, social, and ethical framework to enhance cybersecurity [25]. The authors compare the cybersecurity with safety and conclude that financing of cybersecurity by taxes justifies the significant role of governments in enhancing cybersecurity. Comparison of cybersecurity with other public goods is not limited to public safety and other researchers also compared it with public health. Sedenberg and Mulligan evaluated different cybersecurity information sharing proposals leaning on the analogous public good-oriented field of public health, and proposed some recommendations to orient cybersecurity policies towards adopting the doctrine of public cybersecurity [26].

The studies by McCarthy [27], Assaf [28], and Shore et al. [29] also discuss that cybersecurity appears to have the character of a public good. These studies question rational choice approaches and classic solutions that suggest public goods should be provided by the governments to avoid market failures. However, the incapability of the governments in providing the public good of cybersecurity on their own is also supported by [30]. Hence, they propose solutions based on public–private partnerships to overcome the problems of treating cybersecurity as a public good. The effectiveness of these solutions has been the focus of analyses such as [31–33]. The concern of these analyses is determining institutional forms, policy processes, and levels of government intervention through which partnerships can most effectively provide cybersecurity. Drawing from this interdisciplinary literature, Shackelford used the concept of polycentric governance to describe how cybersecurity as a public good should be regulated [34].

Reviewing the literature shows that there are different arguments favoring treating cybersecurity as a public good. There are also several studies that have incorporated this perspective in their game-theoretical analyses that capture essential characteristics of decision-making to protect assets withing an environment. Bauer and Eeten argue that cybersecurity has strong public good characteristics, although it is mostly provided by private stakeholders at a cost [35]. Varian's exposition supports this argument. Varian observed that the success of reliability (as a critical component of security) decision-making depends on joint protection by all the agents in a network [36]. Moreover, he posits that the computation of the protection level will often take the form of a public good contribution function with non-excludable and non-rival benefits or consequences. As a result, individuals may be able to free-ride on others' efforts or suffer from inadequate protection efforts by those members that have a decisive impact on the overall protection level in the environment.

Grossklags et al. continue Varian's work by adding another action available to the individuals. They can decide to self-insure themselves from harm. Consequently, the security games developed by Grossklags et al. consider share qualities of private (on the insurance side) and public (on the protection side) goods [37]. Johnson et al. extend these security games by modeling network security investments that account for the choice between the hybrid goods of collective protection and individual mitigation and externally provided market insurance. Their study shows that several equilibria with full market insurance exist and, consequently, market insurance has a place in security games [38].

Unlike [37,38], this work assumes only public components have a constant marginal impact across the range of investment opportunities. Therefore, in this study, individual agents decide strategically on how their security investment reduces the probability mass in the loss distribution function of all agents. Furthermore, their works look at homogeneous population of fully rational agents with perfect information. Therefore, our work adds to the research literature by (1) considering heterogeneous population of agents, where every agent has different utility function, (2) exploring the impact of decentralized punishment under a polycentric governance structure, and (3) featuring bounded rationality under uncertainty concepts.

However, the public goods theory plays a relatively minor role in both cybersecurity policy and practices. Although appraisal of these arguments are beyond the scope of this research, we attempt to quantitatively analyze whether the context of cybersecurity complies with this theory, and employing this theory maintains the robustness and resilience of such dynamic and stochastic environment in presence of various externalities. In the next section, we develop a model that addresses the interdependence among the agents and captures the impact of social preferences and punishment on their average contribution to enhance their cybersecurity posture. Cybersecurity posture is used to describe the cybersecurity capabilities of a country, organization or business and collective efforts to protect their assets. It refers to the overall defense mechanisms in place to tackle malicious cyber activities. This metric relates to any kind of security measure, including policies, staff training, and intrusion prevention systems. In this model, we assess the cybersecurity posture of the organizations by the number of failed attacks against them and their resources after each period.

4. Model

This section presents our agent-based model (ABM). ABM is a class of computational models that can simulate a complex macro-level system (e.g., digital ecosystem) based on formally assumed simple behavioral rules of individual agents (e.g., people, organizations, or governments), learning algorithms, and evolutionary settings. By simulating micro-level agents' behavioral processes (e.g., organizations' willingness to contribute) and interactions with each other (e.g., punishing free-riders), it allows the detection of macro-level pattern variations (e.g., cybersecurity posture) caused by individual agents' behavioral changes, which is hardly observable using traditional analytical models. ABM shows advantages in revealing the hidden causal mechanisms driving the macro-level developments in complex systems like digital ecosystems [39].

Digital ecosystems are highly complex socio-technical systems, in which autonomous and heterogeneous decision-making entities, hereafter called agents, operate, interact, and evolve. When some of the problems in such systems resolved with traditional analytical models, the multifaceted realities are largely simplified to build theories with generalizability at the expense of accuracy [39]. The unrealistic assumptions (e.g., homogeneity, linearity, and equilibrium) often fail to gauge the complex behavioral patterns [40]. ABM instead allows agents to be heterogeneous in behavioral patterns, make boundedly rational decisions based on imperfect information (collected or interpreted), perform evaluations based on interactions with each other and the environment, and adapt based on their experiences and environmental changes [41]. ABM is thereby a well-suited tool for identifying causal mechanisms of change in the security or in-security of the digital ecosystems where agents do not act out fully rational. ABM can be employed to produce an accurate prediction of future system patterns [42]. It functions as an explanatory tool when empirical data is unavailable. It enables the researchers to conduct experiments with possible scenarios simulated and compare their outcomes to identify reasonable explanations and propose theoretical advances, without having to be anchored to existing empirical evidence [43]. The rest of this section, describes our underlying model. Table 2 shows the list of notations used to describe this model.

Table 2
The list of notations used in the model.

Notations	Meaning
g_i	Monetary gain of the defender i
c_i	Contribution of defender i to provide cybersecurity
γ_j	The cost incurred by the punisher j
λ_i	Penalty of punishing i
R	Resource of agents
c_i	Contribution of i
p_{ij}	Probability of punishing j by i
p_{ji}	Probability of punishing i by j
Defenders	All the agents that belong to the defense group
defender	An agent that is a Defender
Attackers	All the agents that belong to the offense group
attacker	An agent that is an Attacker
W/O punishment	Without punishment
W/ punishment	With punishment

4.1. The basic model

The classical setting of a Public Goods Game (PGG) models an economic or social group of n agents, termed Defenders, whose strategies include either Contribute or Defect. If an agent contributes, she invests a quantity c into the public pool whereas defectors do not contribute anything. In our study, we add another group of m agents, termed Attackers, whose strategy is to attack one or more of the Defenders to gain financial benefits. The attackers target one of the Defenders and conduct an attack. The Defenders prevent or minimize the risk of these cyber-attacks by employing security measures (SM). Security measures may include: physical access controls, staff training, encryption technologies, and architectural approaches, among others.

In our model, each of the defenders has an initial resource of $R > 0$, expressed in monetary units. The organizations simultaneously decide on their respective contributions $c_i \geq 0$ to invest on SM as participatory public goods. The total contributions towards the cybersecurity provision using these measures is $C = \sum_{i=1}^{n} c_i$. The monetary gain of the defender $i \in n$ is given by

$$g_i = \begin{cases} R - c_i + ROSI & W/O\ punishment \\ R - c_i + ROSI - \gamma_j p_{ij} - \lambda_i p_{ji} & W/\ punishment \end{cases} \tag{1}$$

where ROSI is the return on security investment by all contributor agents arising from implementation of security measures. In the public goods theory literature, this private benefit is called the marginal per capita return (MPCR). In a standard PGG, the contributions of agents are multiplied by an enhancement factor. This amount is then equally distributed among all the agents of the PGG regardless of their contributions. In our model, however, we calculate this variable as follows:

$$ROSI = \frac{ALE - (ALE \times (1 - RM)) - AC_{SM}}{AC_{SM}} \tag{2}$$

where ALE, RM and AC_{SM} are the annual loss expectancy, mitigated risk by implementation of the security measure, and the annual cost of deployment and maintenance of the security measure, respectively. On the other side, the return on the conducted attack for the attackers will be calculated by:

$$ROA = \frac{EMG - (EMG \times RM) - Cost_{att}}{Cost_{att}} \tag{3}$$

where EMG and $Cost_{att}$ are the expected monetary gain and cost of the conducted attack, respectively. ROSI and ROA are computed by using quantitative indexes and defense/attack trees presented in [44]. When the computation of ROSI and ROA is complete, the agents have two options; selecting security measures that maximize ROSI or minimize ROA. The first thing that the agents can do is to eliminate, if any, sets with negative value of ROSI as they do not represent profitable investments. Then, some of the agents can invest in security measures that maximize ROSI, while some of them can invest in measures that minimize ROA. The agents evaluate effectiveness and profitability of measures as well as their deterrent effect on attackers. According to the result of this evaluation, they can change their strategy.

Eq. (1) shows two expressions to calculate the gain of Defenders: with punishment (w/ punishment) and without punishment (w/o punishment). In case of punishment, the contributors are allowed to punish the non-contributors (i.e. free-riders). The punishers incur certain costs (γ) to perform the punishment, and subsequently, they impose a penalty (λ) on the agents who are punished. Since punishment incurs expenses on both sides, it is likely that contributors ignore punishment considering the cost of punishment and their social preferences. The attackers play an important role in inducing more contributors as experience of attack increases the willingness to cooperation among the defenders [45].

As [45] argued, social preferences models with risk aversion may break down into two main elements of self-regarding and other-regarding preferences. With this in mind, we express our utility function as below:

$$\pi_i(g_i, g_j) = g_i - \alpha_i\ max[g_j - g_i, 0] - \beta_i\ max[g_i - g_j, 0] \tag{4}$$

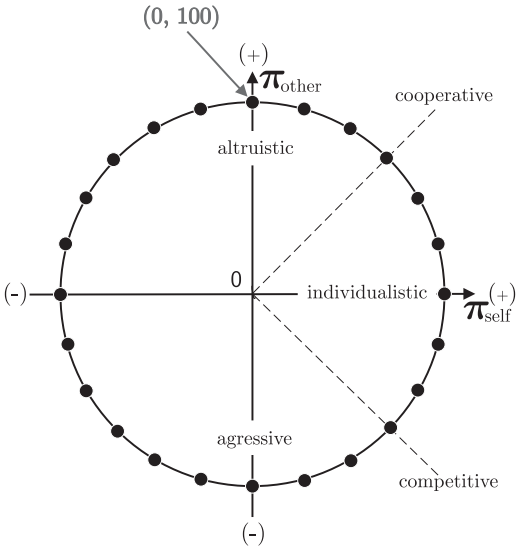


Fig. 1. Social orientation value ring is used to illustrate how individuals weigh their own payoffs vs. the payoffs of one or more others.

where α_i and β_i represent the constant elasticity of substitution in this function to exhibit the elasticity of the ratio of other-regarding preferences and individualism, respectively. Fig. 1 depicts these two elements. In our model $-100 \leq \alpha_i \leq 100$ and $0 \leq \beta_i \leq 100$. We have considered two possible types of other-regarding preferences which exhibit altruism and envy (aggressive). Defenders are initially endowed with certain values for α and β, but these values can change through the time. While the Defenders act to maximize their utility, it is the prevalence of their preferences (i.e. internal norms) that determines the social norm in the long-term. The literature shows that different social norms generate multiple equilibria within the environment [46,47]. It also shows that the norms evolve over time, according to the actual contribution of the individuals [48,49].

The static equilibrium of this game, when all the quantities have unchanging values and organizations are self-regarded, is zero contributions ($\forall i \in n : c_i = 0$). In this case, the Defenders fail to provide cybersecurity. Furthermore, [50] shows that the social optimum will be achieved under $\forall i \in n : c_i = R$. However, in the presence of externalities and other preferences included as a part of our study and the context of cybersecurity, these fundamental theorems do not hold. In an evolutionary context, agents are not considered fully rational [51]. Therefore, they do not necessarily act a Nash equilibrium found from rational analysis. Agents are allowed to change their strategy after each round of the game. In our model, the evolution of strategies follow certain evolutionary rules, in which agents evaluate their payoffs comparing their fitness with those of the rest of the population. In this model, we assume that the Defenders report their amount of contributions after each round. Therefore, the Defenders can infer the percentage of contributors and free-riders. The level of free-riding influences the Defenders' probability of contribution in the next round. Therefore, Defender i compares her payoff of the last two rounds (the recency-biased is 1). The probability that i contributes in round $t+1$ obeys a saturated Fermi function of the payoff difference, and is calculated as follows

$$Prob(contribution) = \frac{1}{1 + e^{\frac{\pi_i^t - \pi_i^{t-1}}{k}}} \tag{5}$$

where k is the percentage of free-riders in the population. This means that although the probability of contribution is a function of changes in the agents' utility, it is also based on the level of contributions observed in the environment in the current round. When $k = 0$ (i.e., there is no free-rider), the agents keep their strategy, with probability 1, in round $t+1$ since it has a better payoff. If $k \to \infty$ (i.e., all the Defenders are free-riders), the Defenders update their strategies with probability of $1/2$, regardless of the payoff difference. The agents do not know the contribution probability of other agents but can infer the amount of contribution in each round. k has been considered fixed in the literature of evolutionary public good games for simplicity. However, we relate this variable to the dynamic percentage of free-riders to characterize the stochastic uncertainties in the game dynamics an incorporate interdependencies and reciprocity in our model.

The free-riding problem, in which a self-interested defender seeks to free ride on other's contribution, is likely to exist in any collective action. In this model, we implement a decentralized punishment strategy by contributors to explore the effectiveness of this strategy in maintaining, or perhaps increasing, the average level of contribution by the Defenders. Experimental studies show the importance of decentralized punishment (i.e. punishments are carried out without the intervention of a central authority by the individuals) in promoting the cooperation among the agents [52–54]. Therefore, the contributors can target those who defect. Eq. (6) gives the probability of punishing j by i if the contribution of i is more than a defined threshold. The punishment would be carried out by i if $p_{ij} = 1$.

$$p_{ij} = min\{\frac{|arctan(\beta, \alpha)|\ \lambda_j - \gamma_i}{2\gamma_i}, 1\} \tag{6}$$

Agent i chooses one of the free-riders proportionally to their payoff. In our model, this obeys from the Moran rule where probability of choosing agent j is given by

$$Prob(punishing\ j) = \frac{\pi_j}{\sum_{l=1}^{N} \pi_l} \tag{7}$$

This rule uses the global knowledge about the payoffs of the Defenders. It should be noted that both Fermi and Moran rules are purely stochastic when describing the probabilistic dynamics in a finite population of constant size N.

Assuming that the preferences of all the agents are separable, Dufwenberg proposes a general equilibrium for the conditions that other-regarding preferences exist in the market, particularly if it is competitive [55]. Another promising solution to efficiently provide the public good is the implementation of Lindahl equilibrium, which achieves optimum social welfare for the public good economy at a Nash equilibrium. The existing Nash implementation literature involves several mechanisms with desirable economic properties such as integration of static and dynamic settings and budget balance [56–58]. However, there are two unaddressed issues in the literature of equilibrium implementation for public good provision. First, the existing approaches cannot perfectly incentivize agents to contribute in the process of public goods provision. Therefore, the free-riding problem cannot completely be avoided [59]. Second, for the constrained public good provision problem (i.e., the principle that agents face with some constraints such as constitutional or legislative, for a public good provision mechanism to be implemented), there does not exist an agent adaptation policy that is guaranteed to converge to the equilibrium. This motivates us to propose a polycentric governance structure with a proper economic mechanism to resolve these two issues. The basic idea of polycentric governance is that any group facing some collective problem should be able to address that problem in whatever way they best see fit [60]. We implement our model under this structure because (1) the polycentric structure recognizes that diverse organizations and governments operating in a multi-level environment can create policies to increase cooperation and compliance levels by enhancements of flexibility and adaptability over time, and (2) it contributes to the solution of free-rider problem since a central governance unit is often incapable of managing collective action problems such as efficient response to cyber attacks.

4.2. Agent-based simulation

The agent-based simulation presented in this paper implements the impact of an agent's social preferences on the decision to cooperate or not cooperate in the provision of cybersecurity as a participatory public good (i.e., requires the beneficiaries to contribute in provision of the good). Thus, we implement our model as a polycentric governance structure to describe a process of decision making where multiple independent actors interact to produce an outcome that is commonly valued [61]. The outcome is protection of their resources and mitigation of the consequence of attacks by implementing the security measures with specific cost and applications. In case of an attack, if the measure is implemented adequately, the attack fails and at the end of the period, the calculated ROSI is shared equally among all the defenders. Otherwise, the impact of the conducted attack will reduce the attack target's resource and add to the attacker's resource.

Four cyber attacks with different levels of impact may occur in each round. The impacts and costs of these attacks are extracted from the Ninth Annual Cost of Cybercrime Study by Accenture and Ponemon Institute [62]. This study reports findings of field research conducted over several months across 11 countries in 16 industries. The findings give us good insights into the economic impact of cyber-attacks and benchmarking cybersecurity investments. The information that we extracted from this study includes the total cost by attack type and the core process-related activities that drive a range of expenditures to implement cybersecurity measures.

The Attackers have no information regarding the implemented measures and Defenders. However, Defenders have the information regarding the contributions of other defenders. Accordingly, to store this information and introduce the reciprocity behavior into the model, all the defenders have their own memory which stores the attacks that have occurred to them, the defenders that they have punished and the defenders that were punished by. To address the problem of recency bias [63], the model assumes that the players outweigh the experience of the most recent round compared to the previously played rounds. This study does not explore the impact of variable recency bias and memory length of the agents.

The model is written in NetLogo 6.1.1 and each tick of the simulation represents one day. The simulation period is 365 steps (equivalent to one year). The probability of cooperation for each defender in each period is based on personal motivation, level of resource, and experience. The defenders do not know the contribution probability of the other defenders and the attack likelihood, however, they are able to observe if any contribution is made or if any attack has occurred. Thus, the game is implemented with incomplete and imperfect information among the agents.

The following occurs in each tick of the simulated process:

1. Decisions and Actions: Each defender decides whether to contribute or defect, according to their probability of contribution (Eq. (5)). The Defenders who decide to punish another agent carry out the punishment. Each attacker selects a target according to their resources and costs of the attack, and conducts the attack against the selected target. The impact of these attacks can be mitigated by the security measures that the Defenders can implement through their collective action.
2. Payout Distribution: Each agent get the payout from their decision. The Defenders get the payout from their collective action and the attack (those who have been targeted). The Attackers get the payout of the attack, whether it has been a success or failure.
3. Updating Strategies: Depending on the cooperation levels within the Defenders and the received payouts, each defender updates their probability of contribution and punishment according to Eqs. (5)–(7).

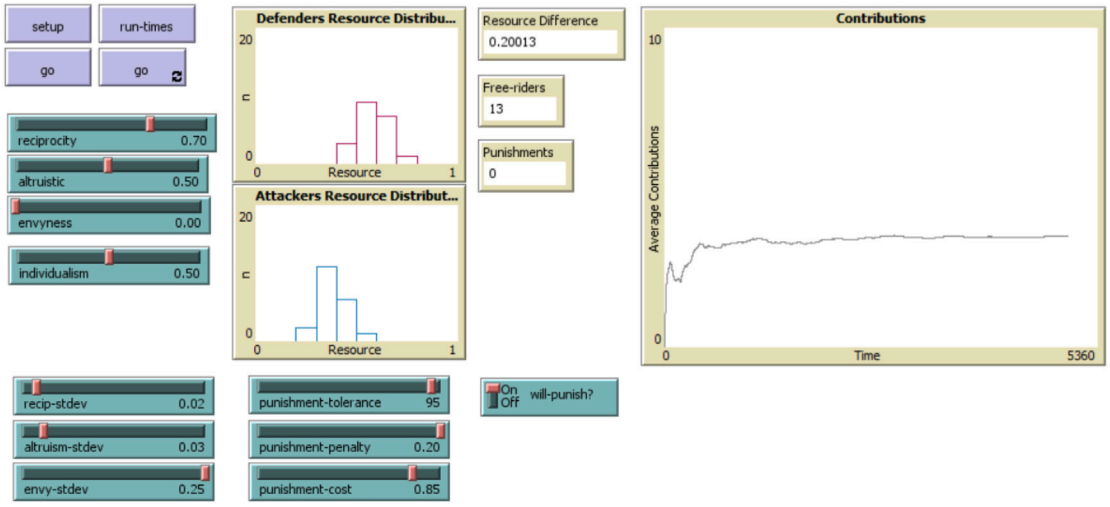


Fig. 2. A Screenshot of the agent-based model implemented in NetLogo 6.1.1.

Table 3
Parameter values for the attacks.

Attack	Probability of Attack	Attack Cost ($\times 10^3$\$)	Attack Impact ($\times 10^6$\$)
A1: Malware	0.25	50	2.6
A2: Web-based attacks	0.20	60	2.3
A3: Denial of service	0.20	70	1.7
A4: Malicious insider	0.15	65	1.6

Table 4
Parameter values for security measures.

Security Measures	Security Investment ($\times 10^3$\$)	Annual Cost ($\times 10^3$\$)	RM_{A1}	RM_{A2}	RM_{A3}	RM_{A4}
CM1: Security intelligence and threat sharing	100	25	0.6	0.5	0.4	0.5
CM2: Advanced identity and access management	80	30	0.4	0.6	0.4	0.6
CM3: Cyber and user behavior analytics	110	30	0.5	0.5	0.4	0.6
CM4: Cryptography technologies	100	5	0.4	0.5	0.3	0.4
CM5: Automated policy management	80	45	0.5	0.4	0.3	0.5
CM6: Enterprise governance, risk, and compliance	300	50	0.5	0.5	0.4	0.5

Fig. 2 shows the user interface of the implemented simulation which enables us to change the mean values of social preferences of the Defenders. The values that is assigned to each agent can be dispersed by using the standard deviation sliders. This interface also shows the distribution of resource among the Defenders and Attackers. This distribution changes over time due to successful or failed cyber-attacks, investment on security measures, and return on security investment. The number of free-riders and the spending on the punishment is also among the outputs that this interface shows. Tables 3 and 4 show the values for input parameters of cyber attacks and security measures, respectively.

5. Results

This section presents the results from the agent-based simulation. The results show that the model replicates the general features of public goods theory and presents the outcomes of the players decision in the game focusing on their social preferences. First, we look at pure social preferences (Reciprocity Ratio = 0) with and without punishment. Fig. 3 shows the average contributions made by the defenders to protect their environment and maintain their robustness in 15 years (5500 ticks). The figure shows that punishment dramatically promotes contribution. It also shows that altruistic preferences increases over time whereas the individual and aggressive preferences reach a constant level of contribution after the first five periods of the simulation.

Reciprocity affects the choice of those who choose later. Figs. 4 and 5 show the results of simulation run in cooperative and competitive modes, respectively, with different reciprocity ratio. As we observe, the possibility of punishment alters the results in both modes. In cooperative mode with punishment, increase in reciprocal behavior increases the average contribution. In contrast, without punishment, increase in reciprocal behavior decreases the contributions among the defenders. The reason of this phenomenon is inequity aversion which is described in [64,65].

Inequity aversion is the preference for fairness and resistance to incidental inequalities. With higher reciprocity ratio, defenders care more about interpersonal comparisons of their own payoff and the payoffs of others. Therefore, increase in contribution of

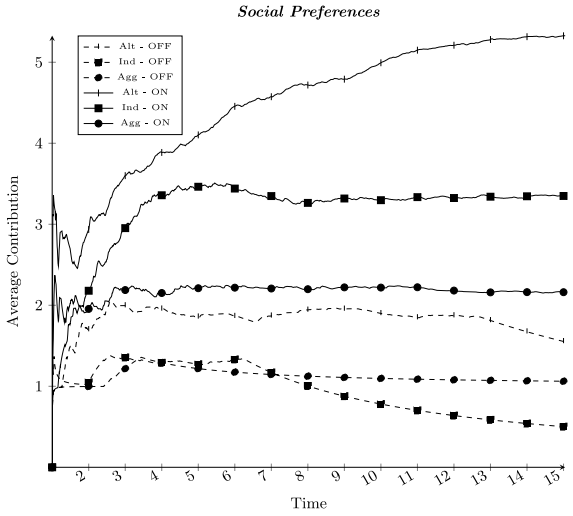


Fig. 3. Social Preferences with punishment (ON) and without punishment (OFF).

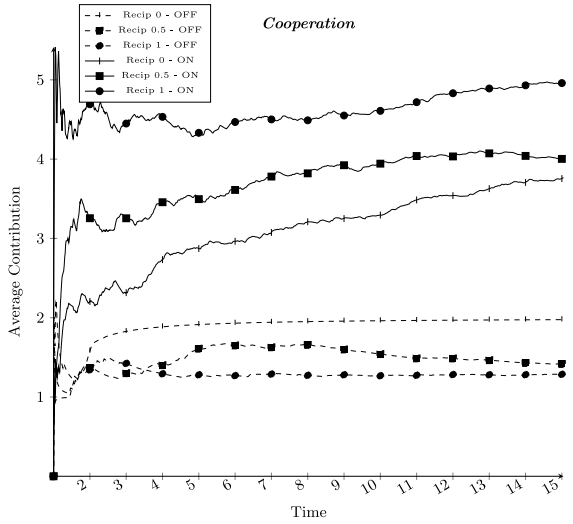


Fig. 4. Cooperation with punishment (ON) and without punishment (OFF).

others motivates an agent to contribute more, and vice-versa. Moreover, the results show that despite the heterogeneous preferences among the agents, the fluctuation in contributions occur in the first 6 decision periods, then, Defenders settle onto a homogeneous behavior to contribute in provision of cybersecurity and maintain the resiliency of the environment. To put it more generally, we observe that in a dynamic and stochastic environment, logic at the level of the system cannot be easily inferred from logic at the level of the agents.

From the pattern in Fig. 6, we can see that the cooperative defenders gain and protect more resources by contribution in the deployment of security measures. On the contrary, individualistic behavior cannot protect the defenders' resources, as a result, the advantages of contribution would be further strengthened. By analogy, with changing the behavior from individualistic to other-regarding preferences, the Defenders get resistance against the attacks impacts. Thereby, the environment will form a dominant strategy which will promote the cooperation efficiently.

From a theoretical perspective, it is important to explore whether decaying contributions converge to the free-riding level (i.e., Nash Equilibrium). However, determining the range of contributions in final decision periods is a difficult task and there are no experimental research, to our best knowledge, that have conducted public goods game similar to our game design (i.e., conditional cooperation with repetition and dynamic marginal per capital return and the presence of exogenous factors such as cyber-attacks that might change individual behavior). Hence, we cannot explore the degree of corroboration between our simulations and empirical experiments. Nevertheless, we refer to two significant experimental studies by Ledyard [66] and Fischbacher et al. [67] due to their substantial number of experiments conducted on public goods in the former and incorporation of social preferences in the latter.

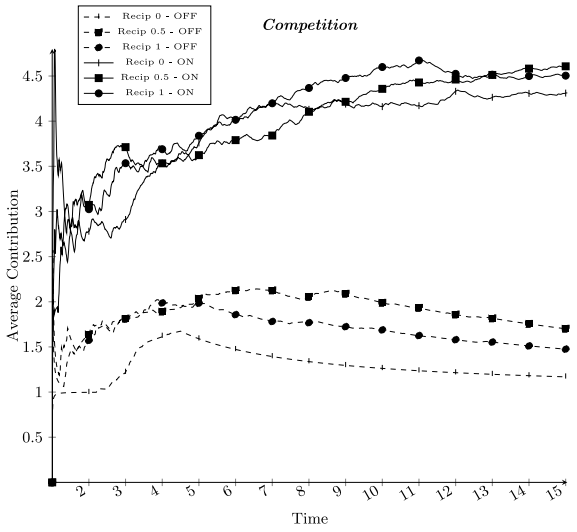


Fig. 5. Competition with punishment (ON) and without punishment (OFF).

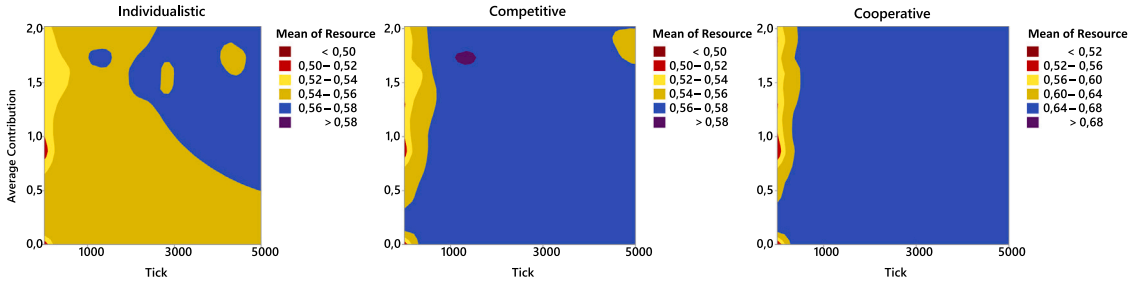


Fig. 6. The distribution of the agents' resource level in three different behavior. All results are obtained for $N = 20, \gamma = 2, \lambda = 3$. Increasing the average resource shows that deployment of the security measures has been successful in mitigation of the attacks impacts. We found the same pattern of change as the cost and penalty of punishment increased.

While Ledyard shows that final period contributions may be as low as 4% and as high as 37%, Fischbacher et al. report the range from 10% to 15% of the endowment. Fig. 7 shows the probability distribution of contributions (average of the final 5 decision periods in 100 simulation runs) for $N = 20$. About 25% of the Defenders have contributions of 10% or less above the free-riding level. Almost 75% of them between 10% to 30%, and the contribution of 5% of the Defenders reaches more than 30% of the free-riding level. We conducted sensitivity analysis on the number of Defenders and repeated the simulation for $N = 4$. The results show more contributions than group size $N = 20$. Therefore, the results indicate that contributions do not reach the free-riding level and most of the Defenders have contributions between 5% and 15% above free-riding level.

5.1. Sensitivity analysis

Sensitivity analysis (parameter variability) technique consists of changing the values of the inputs and parameters of a model to determine the effect upon the model's behavior or output. We used the quantitative approach to investigate both direction and magnitudes of the outputs. The outputs that we examined in this study are the number of free-riders, the spending on punishments by contributors, and change of preferences through the time. Fig. 8 show the result of our analysis on the number of free-riders in cooperative mode, with and without punishment. As this figure shows, the number of free-riders increases with the increase in reciprocity ratio if contributors do not punish the non-contributors. We observed the same trend in competition mode. As we pointed out earlier, this shows the change of preferences in this highly interdependent and dynamic environment.

We further investigated the punishment behavior in detail. Fig. 9 shows the average amount that contributors spend on punishment over 15 periods. This is the average amount of 100 runs of the simulation. In all conditions, the differences between the amount of punishment is not significant. This indicates that punishment functions to facilitate contribution. However, this tendency was weaker for individualistic Defenders. We derived a hypothesis based on this observation: the punishment expenditure of the individualistic agents ($\beta > 25$) is lower than other agents regardless of the cost of punishment and preference of other agents. To test the statistical significance, the difference in punishment expenditure of all preferences was calculated and analyzed using

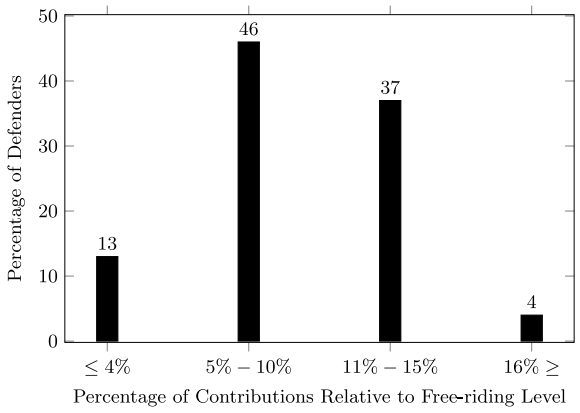


Fig. 7. Probability distribution of average contributions during the last five decision periods of 100 simulation runs ($N = 20$).

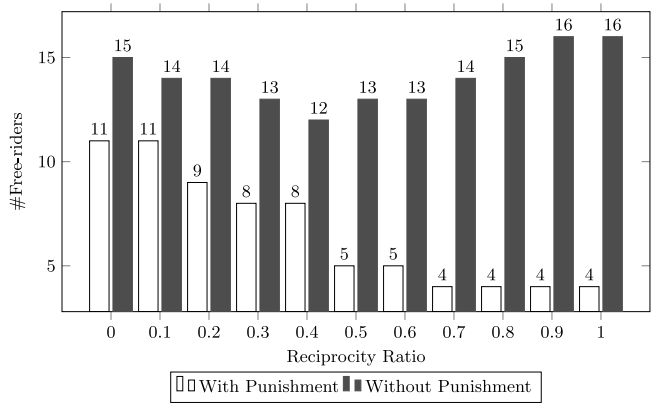


Fig. 8. Impact of reciprocal behavior on the number of free-riders in cooperative mode ($N = 20$).

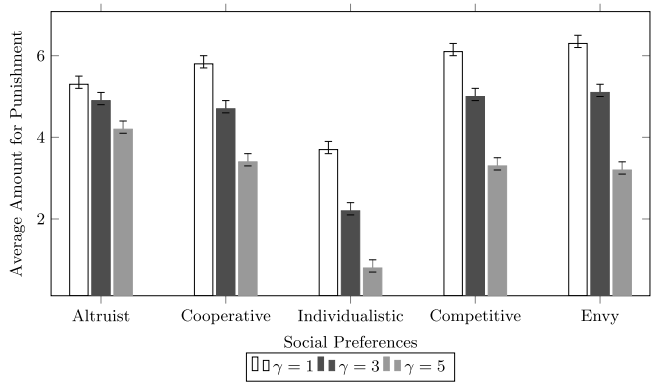


Fig. 9. The average spending on punishment by the contributors over 15 periods. ($N = 20$, Reciprocity Ratio = 0.5, Average of amounts in 100 runs of simulation).

the Mann–Whitney U test with Bonferroni correction. The punishment expenditure of the individualistic agents was significantly lower than altruistic ($Z = 2.711, p = 0.006$), cooperative ($Z = 3.181, p < 0.001$), competitive ($Z = 3.264, p < 0.001$), and envy ($Z = 2.793, p = 0.034$) agents. Therefore, this hypothesis is supported. In addition, we examined how the agents change their punishment expenditure level after increasing the cost of punishment. The results show that the cost functioned to change agents' willingness to punish, however this function was weaker in Altruistic preference than in other preferences. This finding provides support for the theory of "altruistic punishment" [68], which posits that individuals punish, although the punishment is costly for them and yields no material gain.

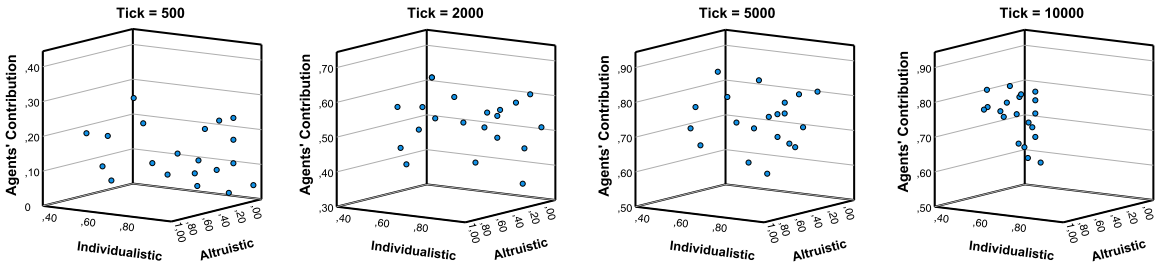


Fig. 10. Change of preferences over the time ($N = 20$, With Punishment).

Since the introduction of punishment promotes the level of contribution, it is meaningful to detect the potential reason for this phenomenon. In order to analyze the inherent nature of this promotion, we describe the density of contribution under the time series by plotting the change of proportion of individualistic and altruistic agents in Fig. 10. In the first 500 ticks, the non-contributors are in a dominant position to the contributors. In fact, we know that every agent tend to choose defection because they would have a high payoff value in the first steps. As time goes, the individualistic strategy will gradually disappear and the level of contribution rises to a certain level. This shows that the temptation of defection cannot compete with the dominating force with intensive externalities, and causes collective action towards provision of cybersecurity as a public good.

5.2. Validation

The model validation is a process of assessing the degree to which the model is a reasonable representation of the real world from the perspective of the model's intended applications. A clear understanding of the phenomena to be described by the model and testing the simplest behavior rules are the key to reliable ABM validation [69]. Validation has a rigorous-relevance issue. The most rigorous validation is data based, however, in order to conduct a rigorous validation for such a complex problem, we require collection of data for many years. Therefore, we employ other methods of validation in this study. Sargent proposed different methods of validity for simulation models [70]. This paper mainly studies the result of framing and managing cybersecurity as a public good, rather than specifically predicting the agents behavior in the environment. Therefore, we only test replicative validity (i.e. comparison to other models and determining the internal stochastic variability in the model).

There are four levels of model performance for replication validity [71]. Since, it would not be realistic to achieve the highest level (i.e. the model behavior is in quantitative agreement with empirical micro-structures, actual human behavior) due to inherent uncertainty in human behavior and the random events in reality, we satisfy the criteria of the third level which is quantitative agreement with empirical macro-structures. The results of this simulation model are compared with empirical data from previous studies [67,72,73]. The presented results show that the agents behavior in this model under all the conditions (i.e. with punishment, without punishment and reciprocity) is in line with the empirical data. For example, our results presented in Fig. 8 replicates the experimental results in [64]. Fehr and Schmidt show that only one free-rider can cause a large number of inequity-averse conditional contributors to behave selfishly, and therefore, cause the emergence of the free-riding behavior in the population.

6. Discussion and practical implications

In this section, we reflect on the central points of this work and combine the various findings into a general discussion. First, this paper provided a quantitative analysis to capture the main elements of public goods theory and investigated whether it complies with the characteristics of cybersecurity. We delineated that treating cybersecurity as a public good under a polycentric governance structure and decentralized punishment mechanism, enhances the cybersecurity posture of the environment. As discussed in Section 3 cybersecurity posture is an important macro-level metric to measure the success of collective actions undertaken by operating agents to provide cybersecurity as a public good. The lack of formalized and quantitative studies constitutes a substantial shortcoming in the studies focused on cybersecurity as a public good. We tackle this problem by integrating a variant of public goods game into the design of an agent-based model.

Admittedly, this approach does not provide a general solution to the missing formalization of this notion. However, incorporation of several well-established concepts in the game such as social preferences, evolutionary elements of strategies, and heterogeneity of the boundedly rational agents enabled us to computationally model this notion. Our results are based on the assumption that agents change their strategies and their social preferences are not stable. In the literature of cybersecurity economics, previous studies have included the learning and evolutionary dynamics in their models [74,75]. However, this is the first study that has incorporated these principles in the settings that agents treat cybersecurity as a public good. Moreover, the agents in this study are programmed to be responsive to factors such as marginal per capita return, punishments, and the contribution of other agents in addition to cyber attacks and their payoffs. Therefore, this study adopts a multi-paradigmatic approach (i.e., a process to systematically and thoughtfully listen, understand, appreciate, and learn from multiple paradigms and perspectives, and bring them together on research projects that we are working on), drawing knowledge from behavioral economics and evolutionary economics to make the results more prosperous and reliable.

The classic public goods game assumes that selfish and rational behavior of the players leads to suboptimal outcomes. Therefore, the unique Nash Equilibrium is not to contribute anything. However, there is no work that developed or tested a formal statement of this conjecture in the context of cybersecurity with the presence of negative and positive externalities, social preferences, and cyber-attacks. Incorporating these factors into our model leads to inconsistencies with prediction based solely on the induced utility. The results presented here support that contribution for provision of cybersecurity as a public good does not adequately reflect the Nash equilibrium of the game implied purely by self-interested and utility-maximizer agents. Far-from-equilibrium or out-of-equilibrium features have been articulated in complex adaptive systems and computational sociology literature [76]. Agent-based modeling has proved particularly useful in representing these systems and formalizing and testing explanations of cooperative/competitive dynamics. Comparing to variable-based approaches like statistical or mathematical modeling, ABM allows us to simulate emergence of macroscopic regularities, including change of preferences or increased contribution even in competitive mode, over time from interactions of autonomous and heterogeneous agents.

By systematically analyzing the influence of different model parameters, we gained further important insights: First, the results demonstrate that the decay to free-riding occurs only if agents are not able to punish the non-contributors and reciprocity is the dominant behavior of the agents. However, with possibility of punishment, the simulations demonstrate that agents adopt an evolutionary strategy towards the provision of cybersecurity as a public good and create a robust environment. In other words, the simulation results for our baseline model suggest that the environment forms a dominant strategy which promotes the cooperation efficiently. Furthermore, our simulations have been able to exhibit altruistic punishment and inequity aversion preferences in the agents' decisions. In this connection, it is important to mention that the success of providing cybersecurity as a public good was predominantly enabled by the dynamic level of contributions based on the agents' experience of being a victim, punished, or number of existing free-riders. We implemented this parameter (i.e., level of contribution) time-dependent. This allowed the agents to recover if too many successful attacks targeted their resources.

Drawing on our findings and discussions, we may now compile several practical implications for future debates promoting cybersecurity as a public good. Note that these implications are far from being exhaustive and should be regarded as an initiative for in-depth analysis.

1. **Cybersecurity as a multi-dimensional and complex process:** The nature of the goods or services being offered by institutional market agents such as businesses, unions, and nonprofits directly influences the scale of the institutions' market participation, ranging from global to local. For example, the contemporary telecommunications market is more efficient at the global and national scale. The global market in this sector is dominated by global institutions. On the other hand, the certain markets that require regional or local planning and expertise are inappropriate for a wide stage. However, a particular type of market, for example cybersecurity, is not limited to a single scale of operation with different institutional agents serving different customers (people or other institutions) territories.
   Cybersecurity requires the support and active participation of authorities at different levels (local, regional, national, and international) [77]. The authorities have a duty to develop sustainable policies and plans, and to cooperate with many stakeholders in different sectors (e.g., civil society, public services, academia, financial institutions, etc.). Within this cooperation, contradictory interests are predictable since cybersecurity is unavoidably burdened with many uncertainties. These uncertainties may entail opportunities for some stakeholders, and simultaneously, may pose risks for others.
   This is just one of the multi-dimensional aspects of institutions within the context of cybersecurity. Another aspect is that agents might take an adversarial stance against each other in pursuit of opposing goals. We see this phenomenon playing out in state-sponsored attacks against other states under cyber-enabled economic wars [78]. Alternatively, considering the collective response to a cyber attack as a public good, as stakeholders have their own interests, they may choose to misreport their private information to improve their own benefits. For example, if the general goal is to ensure fairness among stakeholders in terms of recovery from a recent cyber attack, the victims can report more damage in order to receive more resources than they deserve. To our best knowledge, no existing work has addressed the utility maximization problem under such private information misreport settings.
2. **Limitations of the definition of public goods:** Considering the aforementioned aspects and changes and evolution to which institutions are subject over time, it is necessary to determine the path and arrangements that promote transition towards sustainability[1] and avoid dysfunctional markets. Research conducted in the area of cybersecurity as a public good is grounded in Public Goods Theory. However, from a theoretical perspective, the Samuelson's narrow definition of public goods presents several conceptual and operational limitations within the context of cybersecurity that leaves it prone to dysfunctionality:

   - Excludability/rivalry criteria do not consider the social construction of the problems and decision-making processes related to the cybersecurity strategies to be implemented.
   - Territorial and collective dimensions of the cybersecurity strategies to be implemented are ignored and therefore, collective action problems or social dilemmas emerge.
   - The technical and institutional innovation, and the knowledge and competencies that are required to effectively implement the policy tools are not recognized adequately.

[1] Sustainability transitions refer to "long-term, multi-dimensional and fundamental transformation processes through which established socio-technical systems shift to more sustainable modes of production and consumption" [79].

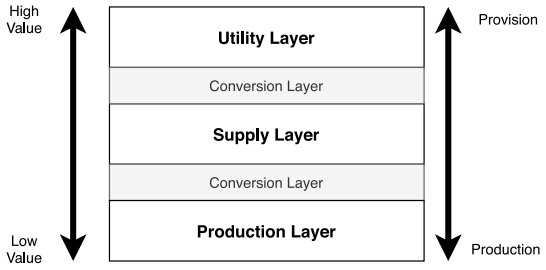


Fig. 11. Cybersecurity as a public good: Distinguishing between layers.

3. **Production vs. Provision:** Oakerson and Parks [80] defined the provision as public decisions about which goods and services to provide by public means, which private activities to regulate, how much public revenue to raise and how to raise it, what quantities of each service to provide and what quality standards to apply, and how to arrange for and monitor production. They also defined production as transforming input resources to make a product or render a service. The key insight of Ostrom et al. was that public provision did not require public production by the same governmental unit [81]. As the technology became more complex, vendors and third-party maintainers have started to play a role, along with regulators, each of which can be governed in quite different ways depending largely on the institutional arrangements. Therefore, a multi-layered perspective can improve the understanding, translating and deploying this insight.
   Fig. 11 illustrates the three main layers that we suggest to distinguish when treating cybersecurity as a public good. The utility layer corresponds to the cybersecurity itself with the characteristics of non-excludability and non-rivalrous. At this layer, the society as a whole drives utility from cybersecurity collectively. The supply layer determines the manner in which cybersecurity is offered. Finally, the production layer transforms the resources into products or services that are critical for the security of a digital ecosystem. An example of this is when a new cybersecurity product or service is produced, it will be certified in accordance with certain certification schemes (nation-wide or region-wide) and supplied by operational infrastructure providers. Then, the potential utility that is enabled by the supply layer will be accessed by the society as a whole. The characteristics of public goods at the supply or production layer might be different. For instance, the patent of the products or services can transform them into a private good. Therefore, these two layers are mostly affected by organizational and policy-related changes. These layers can be linked in various ways. In any case, the value, effectiveness and usability of cybersecurity relies on the value-added processes, scarcities and vulnerabilities of the ecosystem. Therefore, conversion layers draw a path associated with the efficiency in the use of cybersecurity to follow by the all actors over time.

Cybersecurity is characterized by interdependencies among people, organizations and governments, and it varies in the scale at which those interdependencies occur. Hence, with regard to the implications of our research, we posit that this multi-layered perspective enables the balance in cybersecurity from bottom-up voluntary approaches and collaboration, and avoids from heavier regulations. New institutional arrangements by distinguishing between the good itself, the provision and the production of the good, and the efficiency related to the path from production to provision of the good, should be designed to create a secure and resilient environment.

7. Conclusion

We presented a model that explores the interdependence of individual decisions in a repeated public goods game, in which cybersecurity is a public good. This model, under a polycentric governance structure, maps agents' preferences to choices of contribution and punishment. Repeated interactions among the defenders that remember their experience of cyber attacks, punishments, and contributions by others, results in a convergence of individual preferences and emergence of a cooperative behavior. Heterogeneity of agents is represented by heterogeneous social preferences with different reciprocal behavior, various level of resources, and different source of incentives. All these parameters affect the probability of the contribution and punishment of non-contributors.

The numerous externalities in the context of cybersecurity and difficulty in assessing the cybersecurity value and cyber risks cause misaligned incentives and information asymmetry. These, in turn, contribute to poor cybersecurity investment and management. However, this study suggests that the theory of public goods should play a more significant role in how we treat cybersecurity in the fast developing societies to maintain robust and resilient digital ecosystems. Moreover, it shows that maintaining the resilience of the systems promotes the collective actions among the defenders to combat the future attacks. This highlights the importance of experience and strongly interdependent decisions that changes the status of the environment radically. In addition, a sensitivity analysis revealed that the average contribution is markedly influenced by an effective decentralized punishment mechanism. The consistency of the pattern of our results across different empirical studies lends us some reassurance that our model behavior is in quantitative agreement with empirical macro-structures.

This is the first implementation of a public goods game in the context of cybersecurity to investigate whether the theory of public goods complies with this domain. This study is a starting point for research in quantitative analysis of the doctrine of public

cybersecurity. Although the results of our study show that a polycentric governance structure has been effective to achieve collective action in the face of fluctuations and disturbance changes, development of a feasible plan for the private and public sectors to effectively manage cybersecurity as public good is beyond the scope of this article. However, we offer several avenues for future research.

In the future, we aim to investigate different types of economic efficiencies in this domain and explore the factors that define the efficient and optimized situations (e.g., optimized resource allocation to security measures) in this context. Moreover, by employing the social structure and institutional economics, future work can focus on the design and analysis of utility, provision, and production layers of cybersecurity, and propose a constructive and practical institutional arrangement to treat cybersecurity as a public good. Moreover, our model could be extended in several ways, for instance, by implementing more complex attack and defense scenarios, creating alliances of defense, or by capturing the impact of the attackers' dynamic pattern of behavior. Yet, a series of additional analyses could be done using the present model, for example, to shed light on the actual role of different distributions for resources or probabilities of cyber attacks.

References

[1] D. Geer, E. Jardine, E. Leverett, On market concentration and cybersecurity risk, J. Cyber Policy 5 (1) (2020) 9–29.
[2] R. Anderson, C. Barton, R. Bölme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore, M. Vasek, Measuring the changing cost of cybercrime, 2019.
[3] M. McLennan, The Global Risks Report 2021, World Economic Forum.
[4] U. Nations, Resolution Adopted by the General Assembly on 6 July 2017. Work of the Statistical Commission Pertaining to the 2030 Agenda for Sustainable Development, United Nations New York, NY, 2017.
[5] F. Filgueiras, V. Almeida, The digital world and governance structures, in: Governance For The Digital World, Springer, pp. 7–42.
[6] S.J. Shackelford, Cyber War And Peace: Toward Cyber Peace, Cambridge University Press, 2020.
[7] D.K. Mulligan, F.B. Schneider, Doctrine for cybersecurity, Daedalus 140 (4) (2011) 70–92.
[8] F.B. Schneider, E.M. Sedenberg, D.K. Mulligan, Public Cybersecurity and Rationalizing Information Sharing, Technical Report, International Risk Governance Center (IRGC), 2016.
[9] M. Kianpour, Heterogeneous preferences and patterns of contribution in cybersecurity as a public good, in: Proceedings Of The 13th International Conference On Agents And Artificial Intelligence (ICAART 2021), Scitepress, 2021.
[10] D. Schatz, R. Bashroush, J. Wall, Towards a more representative definition of cyber security, J. Digit. Forensics Secur. Law 12 (2) (2017) 53–74.
[11] M. Milgate, Goods and Commodities, Palgrave Macmillan UK, London, 2008, pp. 2512–2516.
[12] P. Rosenzweig, Cybersecurity, the Public/Private'Partnership,'and Public Goods, Hoover Natl. Secur. Law Task Force (2011).
[13] P.A. Samuelson, The pure theory of public expenditure, Rev. Econ. Stat. (1954) 387–389.
[14] J.K. Galbraith, The Affluent Society, Houghton Mifflin Harcourt, 1998.
[15] E. Krahmann, Security: Collective good or commodity? Eur. J. Int. Relat. 14 (3) (2008) 379–404.
[16] E. Gal-Or, A. Ghose, The economic incentives for sharing security information, Inf. Syst. Res. 16 (2) (2005) 186–208.
[17] I. Kaul, P. Conceicao, K. Le Goulven, R.U. Mendoza, Providing Global Public Goods: Managing Globalization, Oxford University Press, 2003.
[18] K. Hagedorn, Particular requirements for institutional analysis in nature-related sectors, Eur. Rev. Agric. Econ. 35 (3) (2008) 357–384.
[19] I. Kaul, R.U. Mendoza, Advancing the concept of public goods, Provid. Glob. Public Goods: Manag. Glob. 78 (2003) 95–98.
[20] T. Tropina, Public–private collaboration: Cybercrime, cybersecurity and national security, in: Self-And Co-Regulation In Cybercrime, Cybersecurity And National Security, Springer, 2015, pp. 1–41.
[21] M. Kianpour, Knowledge and Skills Needed to Craft Successful Cybersecurity Strategies, in: Norsk IKT-Konferanse For Forskning Og Utdanning. No. 3, 2020.
[22] J.H. Choi, K. Han, Implications of false alarms in dynamic games on cyber-security, 2020, Available at SSRN 3660197.
[23] R. Pittiglio, F. Reganati, F. Ricci, C. Tedeschi, Cybersecurity, personal data protection and crime prevention from an Italian perspective, in: The Palgrave Handbook Of Corporate Sustainability In The Digital Era, Springer, pp. 131–156.
[24] M. Taddeo, Is Cybersecurity a Public Good?, Springer, 2019.
[25] A. Asllani, C.S. White, L. Ettkin, Viewing cybersecurity as a public good: The role of governments, businesses, and individuals, J. Legal Ethical Regul. Issues 16 (1) (2013) 7.
[26] E.M. Sedenberg, D.K. Mulligan, Public health as a model for cybersecurity information sharing, Berkeley Technol. Law J. 30 (3) (2015) 1687–1740.
[27] D.R. McCarthy, Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order, Politics Gov. 6 (2) (2018) 5–12.
[28] D. Assaf, Models of critical information infrastructure protection, Int. J. Crit. Infrastructure Prot. 1 (2008) 6–14.
[29] M. Shore, Y. Du, S. Zeadally, A public-private partnership model for national cybersecurity, Policy & Internet 3 (2) (2011) 1–23.
[30] M. Dunn-Cavelty, M. Suter, Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection, Int. J. Crit. Infrastructure Prot. 2 (4) (2009) 179–187.
[31] M. Carr, Public–private partnerships in national cyber-security strategies, Int. Aff. 92 (1) (2016) 43–62.
[32] A.D. Givens, N.E. Busch, Realizing the promise of public-private partnerships in US critical infrastructure protection, Int. J. Crit. Infrastructure Prot. 6 (1) (2013) 39–50.
[33] R.J. Harknett, J.A. Stever, The new policy world of cybersecurity, Public Adm. Rev. 71 (3) (2011) 455–460.
[34] S.J. Shackelford, Toward cyberpeace: Managing cyberattacks through polycentric governance, Am. UL Rev. 62 (2012) 1273.
[35] J.M. Bauer, M.J. Van Eeten, Cybersecurity: Stakeholder incentives, externalities, and policy options, Telecommun. Policy 33 (10–11) (2009) 706–719.
[36] H. Varian, System reliability and free riding, in: Economics Of Information Security, Springer, 2004, pp. 1–15.
[37] J. Grossklags, N. Christin, J. Chuang, Secure or insure? A game-theoretic analysis of information security games, in: Proceedings Of The 17th International Conference On World Wide Web, 2008, pp. 209–218.
[38] B. Johnson, R. Böhme, J. Grossklags, Security games with market insurance, in: International Conference On Decision And Game Theory For Security, Springer, 2011, pp. 117–130.
[39] E. Bonabeau, Agent-based modeling: Methods and techniques for simulating human systems, Proc. Nat. Acad. Sci. 99 (suppl 3) (2002) 7280–7287.
[40] S. Nicholls, B. Amelung, J. Student, Agent-based modeling: A powerful tool for tourism researchers, J. Travel Res. 56 (1) (2017) 3–15.
[41] E. Kiesling, M. Günther, C. Stummer, L.M. Wakolbinger, Agent-based simulation of innovation diffusion: a review, Cent. Eur. J. Oper. Res. 20 (2) (2012) 183–230.
[42] E. Bruch, J. Atwell, Agent-based models in empirical social research, Sociol. Methods Res. 44 (2) (2015) 186–221.
[43] R. Willer, K. Kuwabara, M.W. Macy, The false enforcement of unpopular norms, Am. J. Sociol. 115 (2) (2009) 451–490.

[44] S. Bistarelli, F. Fioravanti, P. Peretti, F. Santini, Evaluation of complex security scenarios using defense trees and economic indexes, J. Exp. Theor. Artif. Intell. 24 (2) (2012) 161–192.
[45] M. Kianpour, H. Øverby, S.J. Kowalski, C. Frantz, Social preferences in decision making under cybersecurity risks and uncertainties, in: International Conference On Human-Computer Interaction, Springer, 2019, pp. 149–163.
[46] H.P. Young, Social Norms, University of Oxford, 2007.
[47] B. Morsky, E. Akçay, Evolution of social norms and correlated equilibria, Proc. Nat. Acad. Sci. 116 (18) (2019) 8834–8839.
[48] M. Kandori, The erosion and sustainability of norms and morale, Jpn. Econ. Rev. 54 (1) (2003) 29–48.
[49] B.C. Eaton, M. Eswaran, The evolution of preferences and competition: a rationalization of veblen's theory of invidious comparisons, Can. J. Econ. 36 (4) (2003) 832–859.
[50] R.M. Isaac, K.F. McCue, C.R. Plott, Public goods provision in an experimental environment, California Institute of Technology, 1982.
[51] D.T. Kenrick, V. Griskevicius, J.M. Sundie, N.P. Li, Y.J. Li, S.L. Neuberg, Deep rationality: The evolutionary economics of decision making, Soc. Cogn. 27 (5) (2009) 764–785.
[52] M. Olson, The Logic Of Collective Action: Public Goods And The Theory Of Groups, Second Printing With A New Preface And Appendix, vol. 124, Harvard University Press, 2009.
[53] E. Ostrom, J. Walker, R. Gardner, Covenants with and without a sword: Self-governance is possible, Am. Political Sci. Rev. 86 (2) (1992) 404–417.
[54] B. Herrmann, C. Thöni, S. Gächter, Antisocial punishment across societies, Science 319 (5868) (2008) 1362–1367.
[55] M. Dufwenberg, P. Heidhues, G. Kirchsteiger, F. Riedel, J. Sobel, Other-regarding preferences in general equilibrium, Rev. Econ. Stud. 78 (2) (2011) 613–639.
[56] L. Hurwicz, Outcome functions yielding Walrasian and Lindahl allocations at Nash equilibrium points, Rev. Econ. Stud. 46 (2) (1979) 217–225.
[57] T. Kim, A stable Nash mechanism implementing Lindahl allocations for quasi-linear environments, J. Math. Econom. 22 (4) (1993) 359–371.
[58] F. Vega-Redondo, Implementation of lindahl equilibrium: an integration of the static and dynamic approaches, Math. Social Sci. 18 (3) (1989) 211–228.
[59] T. Saijo, T. Yamato, Fundamental impossibility theorems on voluntary participation in the provision of non-excludable public goods, Rev. Econ. Des. 14 (1) (2010) 51–73.
[60] M.D. McGinnis, Costs and challenges of polycentric governance: An equilibrium concept and examples from US health care, 2011, Available at SSRN 2206980.
[61] K. Carlisle, R.L. Gruby, Polycentric systems of governance: A theoretical model for the commons, Policy Stud. J. 47 (4) (2019) 927–952.
[62] K. Bissell, R. LaSalle, P. Cin, Ninth Annual Cost of Cybercrime Study, vol. 6, Ponemon Institute, Dublin, Ireland, 2019.
[63] C. Hasan, Making sound security investment decisions, J. Inf. Priv. Secur. 6 (1) (2010) 53–71.
[64] E. Fehr, K.M. Schmidt, A theory of fairness, competition, and cooperation, Q. J. Econ. 114 (3) (1999) 817–868.
[65] G.E. Bolton, A. Ockenfels, ERC: A theory of equity, reciprocity, and competition, Amer. Econ. Rev. 90 (1) (2000) 166–193.
[66] J.O. Ledyard, 2. Public Goods: A Survey Of Experimental Research, Princeton University Press, 2020.
[67] U. Fischbacher, S. Gachter, Social preferences, beliefs, and the dynamics of free riding in public goods experiments, Amer. Econ. Rev. 100 (1) (2010) 541–556.
[68] E. Fehr, S. Gächter, Altruistic punishment in humans, Nature 415 (6868) (2002) 137–140.
[69] P. Ormerod, B. Rosewell, Validation and verification of agent-based models in the social sciences, in: International Workshop On Epistemological Aspects Of Computer Simulation In The Social Sciences, Springer, 2006, pp. 130–140.
[70] R.G. Sargent, Verification and validation of simulation models, J. Simul. 7 (1) (2013) 12–24.
[71] R. Axtell, J. Epstein, Agent-based modeling: Understanding our creations, Bull. Santa Fe Inst. 9 (4) (1994) 28–32.
[72] A. Falk, U. Fischbacher, A theory of reciprocity, in: CEPR Discussion Paper, 2001.
[73] J.A. Lacomba, R. López-Pérez, Cooperation, in: Experimental Economics, Springer, 2015, pp. 105–123.
[74] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, A. Martin, An evolutionary game-theoretic framework for cyber-threat information sharing, in: 2015 IEEE International Conference On Communications (ICC), IEEE, 2015, pp. 7341–7346.
[75] H. Hu, Y. Liu, C. Chen, H. Zhang, Y. Liu, Optimal decision making approach for cyber security defense using evolutionary game, IEEE Trans. Netw. Serv. Manag. 17 (3) (2020) 1683–1700.
[76] W.B. Arthur, Out-of-equilibrium economics and agent-based modeling, Handb. Comput. Econ. 2 (2006) 1551–1564.
[77] S. Kowalski, IT Insecurity: A multi-disciplinary inquiry, 1996.
[78] M. Kianpour, Socio-technical root cause analysis of cyber-enabled theft of the US intellectual property–the case of APT41, 2021, arXiv preprint arXiv:2103.04901.
[79] J. Markard, R. Raven, B. Truffer, Sustainability transitions: An emerging field of research and its prospects, Res. Policy 41 (6) (2012) 955–967.
[80] R.J. Oakerson, R.B. Parks, The study of local public economies: Multi-organizational, multi-level institutional analysis and development, Policy Stud. J. 39 (1) (2011) 147–167.
[81] V. Ostrom, C.M. Tiebout, R. Warren, The organization of government in metropolitan areas: a theoretical inquiry, Am. Political Sci. Rev. 55 (4) (1961) 831–842.