Heterogeneous Preferences and Patterns of Contribution in Cybersecurity as a Public Good

Mazaher Kianpour[a]

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

Keywords: Cybersecurity Economics, Social Preferences, Public Goods, Agent-based Modeling.

Abstract: This paper presents an agent-based model of contribution to 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. Hence, different doctrines and thesis have been suggested to explore how this domain should be treated by the public and private stakeholders. Cybersecurity as a public good is one of these doctrines that accordingly, cybersecurity is non-rivalrous and non-excludable. In this paper, we present a model of social preferences reflecting the concepts of altruism, individualism, aggressiveness, and reciprocity. It describes an agent-based model simulating 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 on the social context. The results of this simulation show that, over time, defenders update their preferences in reaction to the behavior of other defenders and the experience of cyber-attacks. Moreover, they indicate a high level of contribution to the provision of cybersecurity as a public good and the effectiveness of punishment on increasing the contributions. This paper demonstrated how agent-based models can be used to examine this doctrine and investigate whether this doctrine complies with the unique characteristics of cybersecurity.

1 INTRODUCTION

Behavioral economics has discovered systematic human behavior in many domains including cybersecurity. These behaviors, such as nonlinear probability weighting, conditional cooperation, and loss aversion, show that human behavior is inherently noisy and heterogeneous. Recent research gives a nuanced view of the results from experimental games[1] in which the notion that humans are purely self-regarded is rejected. Although this is not a new discussion among experimental economists, we believe that this notion has not been studied in the context of cybersecurity economics. The results from (Kianpour et al., 2019) show that social preferences in cybersecurity decision making is not insignificant and have a moderating effect on the behavior of actors.

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. All these are essential requirements of societies that rely on digital infrastructure. Moreover, it is estimated that more than \$5trillion assets will be at risk in the next five years due to the rapid digitalization. Hence, investment in cybersecurity and how this domain should be treated by the public and private sectors has been a hot topic among the business leaders.

In 2011, Mulligan and Schneider proposes to frame and manage cybersecurity as a public good (Mulligan and Schneider, 2011). 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, and has not explored the aspects of both cybersecurity and public goods that contribute on efficiency and effective-

[a] https://orcid.org/0000-0003-2804-4630

[1] The ultimatum game, the gift exchange game, trust game and the public goods game are among the widely replicated experimental games to build this evidence.

Kianpour, M.
Heterogeneous Preferences and Patterns of Contribution in Cybersecurity as a Public Good.
DOI: 10.5220/0010336204140421
In *Proceedings of the 13th International Conference on Agents and Artificial Intelligence (ICAART 2021) - Volume 1*, pages 414-421
ISBN: 978-989-758-484-8

ness of cybersecurity provision. Accordingly, 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. Therefore, the aim of this study is *to construct an agent-based model that captures the main elements of public goods theory (i.e. free-riders problem, effectiveness of punishment, and network effects) 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).* In this study, 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 considering the heterogeneous social preferences of agents. Introduction of social preferences into standard models in economic theory provides us with a better understanding of different phenomena.

This paper proceeds first by reviewing cybersecurity as a public good. Therefore, in Section 2, we review the previous research on cybersecurity as a public good. We present our ABM in Section 3. Section 4 demonstrates the results of the simulation and sensitivity analysis. Finally, this paper is concluded in Section 5 with suggestions for future work.

2 CYBERSECURITY AS A PUBLIC GOOD

Samuelsen defines public goods as non-rival and non-excludable goods in consumption (Samuelson, 1954). 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. Goods with these characteristics are often produced with some form of public assistance (e.g. tax). Accurate production and provision of these goods compared to the level that would be best for society is the main challenge of policy makers. 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.

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. From an economic point of view, cybersecurity has been treated as a club good, in that it is non-rivalrous (i.e. it is not exhausted by its use), but excludable (i.e. its access is regulated by its cost). The failure of the market to produce adequate investments in cybersecurity is documented in (Rowe and Gallaher, 2006; Etzioni, 2011) and addresses the challenges of managing cybersecurity as a club 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 (Taddeo, 2019). 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 (Asllani et al., 2013). 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 adopt the doctrine of public cybersecurity (Sedenberg and Mulligan, 2015).

Reviewing the literature shows that there are different arguments favoring treating cybersecurity as a public good and 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 the such dynamic and stochastic environment in presence of various externalities.

3 MODEL

In the model, there are $N \geq 2$ organization which each of them has an initial resource $R \geq 0$, expressed in monetary units. The organizations simultaneously decide on their respective contributions $c_i \geq 0$ to invest on security measures (SM). The total contributions towards the cybersecurity provision using these measures is given by $C = \sum_{i=1}^{n} c_i$. The monetary gain of organization $i \in N$ is given by

$$g_i = \begin{cases} R - c_i + (ROSI \times Cost_{SM}) & W/O\ punishment \\ R - c_i + (ROSI \times Cost_{SM}) - Cost_p \sum_{j \neq i} p_{ij} - \sum_{j \neq i} p_{ji} & W/\ punishment \end{cases} \tag{1}$$

where $Cost_{SM}$ is the annual cost of deployment and maintenance of the security measure (SM), and ROSI is the return on security investment by the all organizations arising from implementation of security measures. In the public goods theory literature, this private benefit is called the marginal per capita return (MPCR). In our model, we calculate this variable as follows

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

where ALE, RM and AC are the annual loss expectancy, mitigated risk by implementation of the security measure, and annual cost of it, 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. An experimental game played in western countries, where the rule of law and the norm of civic cooperation are high, shows that punishment of non-contributors by contributors is common (Herrmann et al., 2008). Hence, in Equation 1, we added investigate two situations; with and without punishment. Punishment incurs expenses on both sides. Therefore, it is likely that contributors ignore punishment considering the cost of punishment ($Cost_p$) and their social preferences. For example, altruistic defenders are willing less, in compare to aggressive defenders, to punish the non-contributor.

Considering our discussion in introduction, 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:

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

where α_i and β_i are constant elasticity of substitution in this function to exhibit the elasticity of the ratio of altruism and individualism, respectively. Figure 1 depicts these two elements. In our model $-100 \leq \alpha_i \leq 100$ and $0 \leq \beta_i \leq 100$.

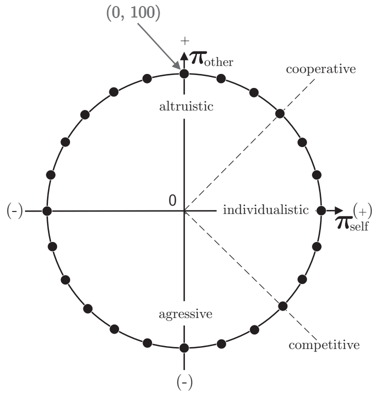


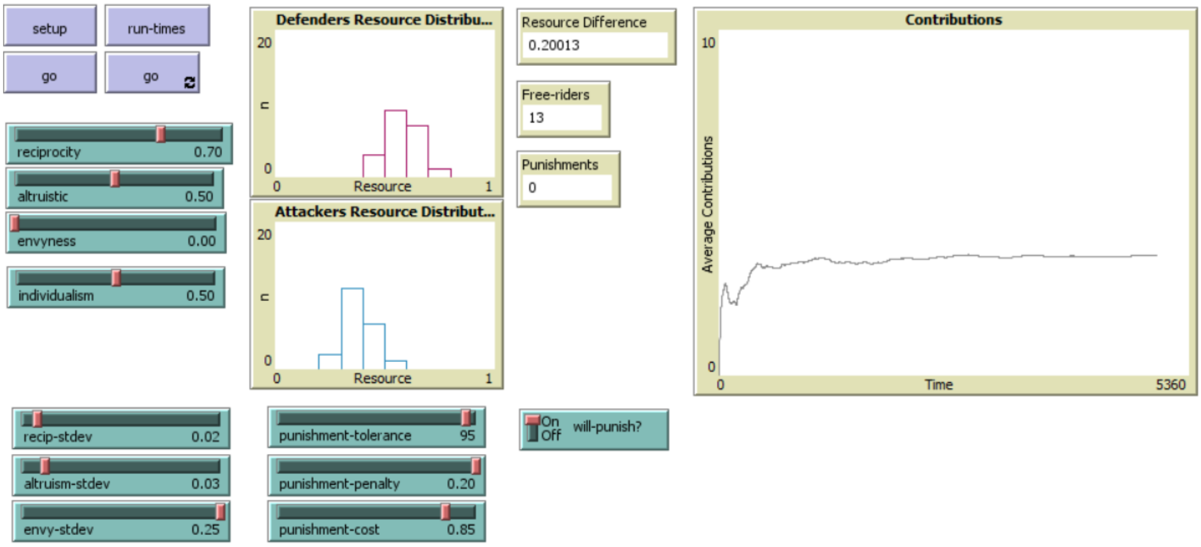
Figure 1: Social Orientation Value Ring.

The static equilibrium of this game, when all the quantities have unchanging values and organizations are self-regarded, is zero contributions ($\forall i \in N : c_i = 0$). Furthermore, (Isaac et al., 1982) shows that the social optimum will be achieved under $\forall i \in N : c_i = R$. However, in presence of externalities and other-regarding preferences which are highly feasible in our study and the context of cybersecurity, these fundamental theorems need not hold. Assuming that the preferences of all the agents are separable, Dufwenberg proposed a general equilibrium for the conditions that other-regarding preferences exist in the market, particularly if it is competitive (Dufwenberg et al., 2011). Presence of externalities also does not necessarily result in a socially desirable distribution of resources. Therefore, to investigate all these possible conditions, we implement an agent-based model to investigate the feasible development of outcomes.

3.1 Agent-based Model

The ABM presented in this paper models the importance of an agent's social preferences on the decision to cooperate or not cooperate in providing cybersecurity in the environment as a participatory public good (i.e. requires the beneficiaries to participate in creation of the good). In this model, defenders play a standard public good game where in each period, each defender makes the decision to contribute to implement the security measures with specific cost and applications. In case of attack, if the measure is implemented adequately, the attack fails and at the end of period, the calculated ROSI shares equally among all the defenders. Otherwise, the impact of conducted attack will be reduces of the attack target's resource and adds to the attacker resource.

Five cyber attacks with different levels of impact occur in each period. These attacks and their corresponding impacts and costs are extracted from (Bis-



reciprocity 0.70
altruistic 0.50
envyness 0.00
individualism 0.50
Resource Difference 0.20013
Free-riders 13
Punishments 0
recip-stdev 0.02
altruism-stdev 0.03
envy-stdev 0.25
punishment-tolerance 95
punishment-penalty 0.20
punishment-cost 0.85
On Off will-punish?

Figure 2: A screenshot of the implemented model using NetLogo 6.1.1.

sell et al., 2019). 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.

The model is written in NetLogo (see Figure 2) and each step of the simulation represents one day and the simulation period is 365 steps, equivalent with one year. The probability of cooperation of 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, the are able to observe if any contribution is made or any attack has occurred. Thus, the game is implemented with incomplete and imperfect information among the agents.

4 RESULTS

This section discusses the results of the implementation of our ABM. 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. Firstly, we look at pure social preferences (Reciprocity Ratio = 0) with and without punishment. Figure 3 shows the average contributions made by the defenders to protect their environment and maintain their robustness in 15 years. The figure shows that punishment dramatically promotes contribution. It also shows that altruistic preferences increases over time whereas the individual and and aggressive preferences reach to a constant level of contribution after first five periods of the simulation.

Reciprocity affects the choice of those who choose later. Figures 5 and 4 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 (Fehr and Schmidt, 1999; Bolton and Ockenfels, 2000). 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 motivates them more to contribute and vice-versa. Moreover, these results show that despite the heterogeneous preferences among the agents, they gradually change to 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 can not be easily inferred from logic at the level of the agents.

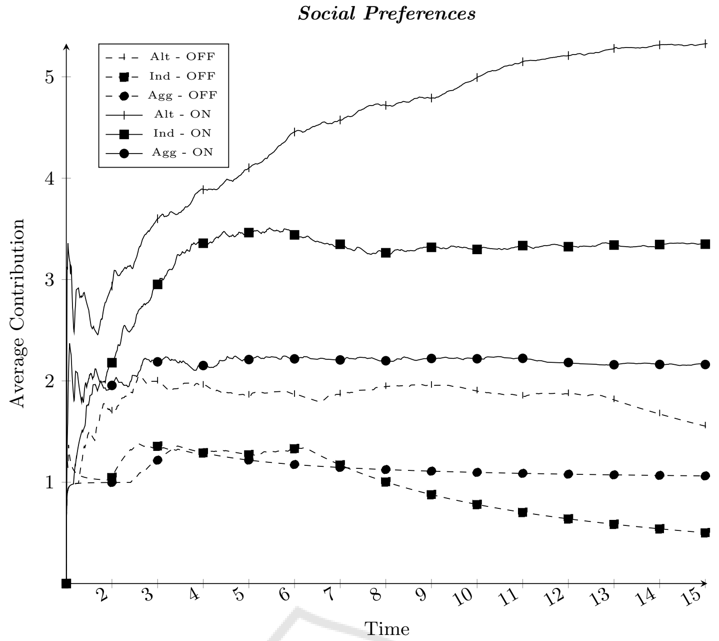


Figure 3: Social Preferences with punishment (ON) and without punishment (OFF).

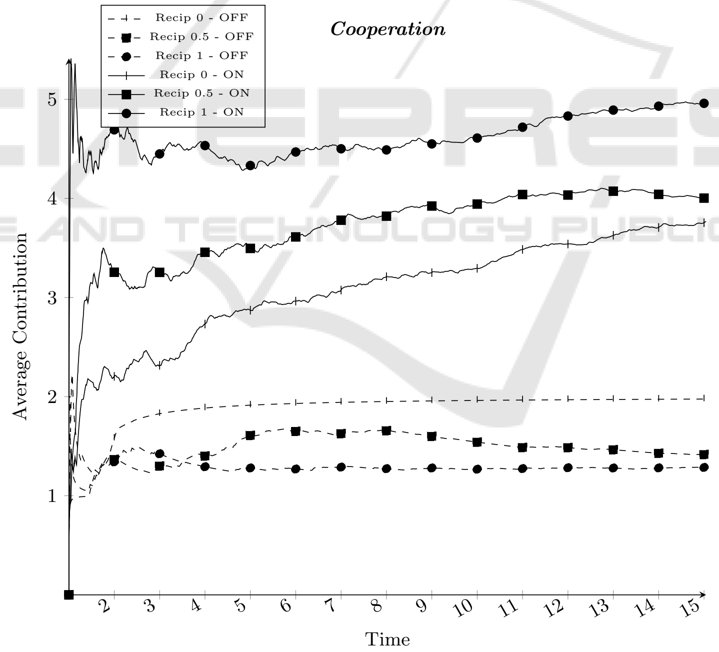


Figure 4: Cooperation with punishment (ON) and without punishment (OFF).

4.1 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, resource difference between defenders and attackers, and the spending on punishments by contributors. Figure 6 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 ob-

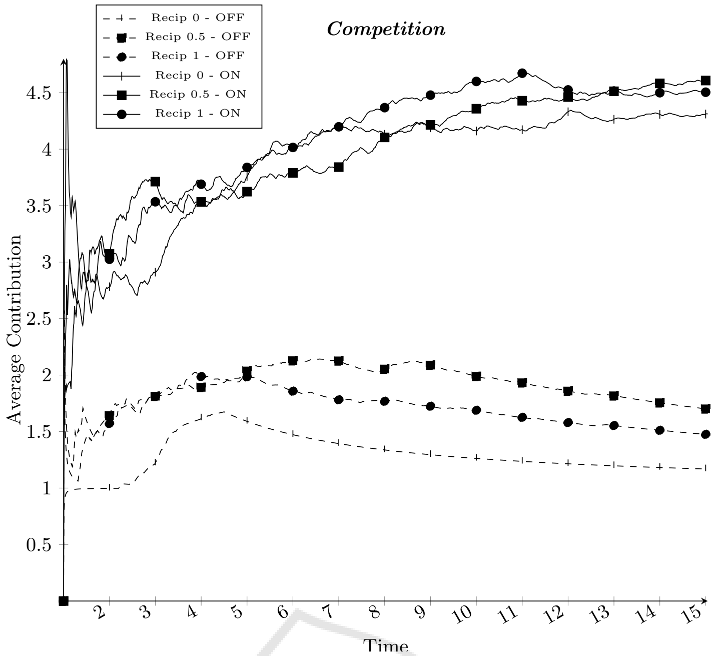


Figure 5: Competition with punishment (ON) and without punishment (OFF).

served the same trend in competition mode. As we pointed out earlier, this shows the change of preferences in this highly interdependent and dynamic environment.

In our model, resource difference between defenders and attackers shows the resilience of the environment against the cyber attacks, in that positive value means that defenders were able to maintain the robustness of their systems by taking advantage of the implemented security measures, and negative value means attackers were successful in breaching into the defenders' systems. Our sensitivity analysis shows that cooperation mode with medium reciprocity ratio has the best results to maintain the environment resilient. Furthermore, punishments arise out of dissatisfaction towards the contribution of other defenders and imposes cost to both sides (See equation 1). Therefore, defenders can choose whether they are willing, and they are able to punish those who under contribute less in each period. Spending on the punishments in aggressive mode with lowest reciprocity behavior has the highest value in our repeated games. These results show the importance of reciprocal behavior in interactions among defenders and change of preferences based on the experience and behavior of other peers.

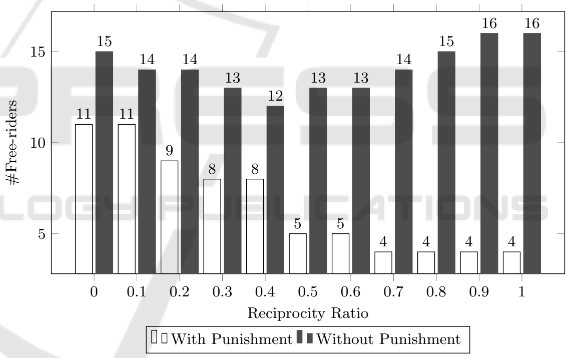


Figure 6: Impact of reciprocal behavior on the number of free-rider in cooperative mode (N = 20).

4.2 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 the testing the simplest behavior rules are the key to reliable ABM validation (Ormerod and Rosewell, 2006). 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 (Sargent, 2013).

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 (Axtell and Epstein, 1994). 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 (Falk and Fischbacher, 2001; Fischbacher and Gachter, 2010; Lacomba and López-Pérez, 2015). The evidence shows 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.

5 CONCLUSION

This study shows that agent-based modeling of complex socio-technical systems can be valuable for testing fundamental theories which are difficult to inspect mathematically and experimentally. We presented a model to explore the interdependence of individual decisions in a repeated public goods game that treats cybersecurity as a public good. This model maps agents' preferences to choices of contribution and punishment. Repeated interactions among the defenders that are able to remember their experience of cyber attacks, punishments and contributions by others lead to a convergence of individual preferences and emergence of a cooperative behavior as a result. 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 on the probability of the contribution and punishment of non-contributors.

We acknowledge that numerous externalities in the context of cybersecurity and difficulty in assessing the cybersecurity value and cyber risks cause misaligned incentives and information asymmetry which all 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 the 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.

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 meant as a starting point for research in quantitatively analysis of the doctrine of public cybersecurity. In future, we investigate the different types of economic efficiencies in this domain and explore the factors that define the efficient situations in this context.

REFERENCES

Asllani, A., White, C. S., and Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, 16(1):7.

Axtell, R. and Epstein, J. (1994). Agent-based modeling: Understanding our creations. *The Bulletin of the Santa Fe Institute*, 9(4):28–32.

Bissell, K., LaSalle, R., and Cin, P. (2019). Ninth annual cost of cybercrime study. *Ponemon Institute: Dublin, Ireland*, 6.

Bolton, G. E. and Ockenfels, A. (2000). Erc: A theory of equity, reciprocity, and competition. *American economic review*, 90(1):166–193.

Dufwenberg, M., Heidhues, P., Kirchsteiger, G., Riedel, F., and Sobel, J. (2011). Other-regarding preferences in general equilibrium. *The Review of Economic Studies*, 78(2):613–639.

Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, 28(1):58–62.

Falk, A. and Fischbacher, U. (2001). A theory of reciprocity.

Fehr, E. and Schmidt, K. M. (1999). A theory of fairness, competition, and cooperation. *The quarterly journal of economics*, 114(3):817–868.

Fischbacher, U. and Gachter, S. (2010). Social preferences, beliefs, and the dynamics of free riding in public goods experiments. *American economic review*, 100(1):541–56.

Herrmann, B., Thöni, C., and Gächter, S. (2008). Antisocial punishment across societies. *Science*, 319(5868):1362–1367.

Isaac, R. M., McCue, K. F., and Plott, C. R. (1982). Public goods provision in an experimental environment.

Kianpour, M., Øverby, H., Kowalski, S. J., and Frantz, C. (2019). Social preferences in decision making under cybersecurity risks and uncertainties. In *International Conference on Human-Computer Interaction*, pages 149–163. Springer.

Lacomba, J. A. and López-Pérez, R. (2015). Cooperation. In *Experimental Economics*, pages 105–123. Springer.

Mulligan, D. K. and Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, 140(4):70–92.

Ormerod, P. and Rosewell, B. (2006). Validation and verification of agent-based models in the social sciences. In *International Workshop on Epistemological Aspects of Computer Simulation in the Social Sciences*, pages 130–140. Springer.

Rowe, B. R. and Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Samuelson, P. A. (1954). The pure theory of public expenditure. *The review of economics and statistics*, pages 387–389.

Sargent, R. G. (2013). Verification and validation of simulation models. *Journal of simulation*, 7(1):12–24.

Sedenberg, E. M. and Mulligan, D. K. (2015). Public health as a model for cybersecurity information sharing. *Berkeley Technology Law Journal*, 30(3):1687–1740.

Taddeo, M. (2019). Is cybersecurity a public good?