Organizational Participation in Cooperative Cyber Security

SAND 2012-1987C

30th International Conference of the System Dynamics Society
July 22th – 26th, 2012 – St. Gallen, Switzerland

Asmeret Bier
Sandia National Laboratories

Abstract

Cyber attacks pose a major threat to modern organizations. The effectiveness of cyber defense can likely be enhanced if programs are implemented that allow organizations that face similar cyber threats to share information and resources. To begin to understand the potential for cooperation to improve cyber security, we modeled a simple cooperative structure that allows resource sharing between two organizations whose defense teams do a significant amount of redundant work. This model is a first step toward understanding the social and operational issues involved in implementing a program of cooperative cyber defense between organizations.

Organizational Cooperation in Cyber Security

Cyber attacks pose a major threat to modern organizations. These attacks can have nefarious aims and serious consequences, including disruption of operations, espionage, identity theft, and attacks on critical infrastructure. Organizations must put substantial resources into protecting themselves and their customers, clients, and others against cyber attacks. Even with a substantial investment in cyber defense resources, however, the risk of harm from a cyber attack is significant for many organizations.

The effectiveness of cyber defense can likely be enhanced if programs are implemented that allow organizations that face similar cyber threats to share information and resources. The threats faced by different organizations may be similar or identical (figure 1), and much of the work done by cyber defenders at these organizations may be redundant (Hui et al. 2010). By sharing information about cyber attacks, effective defense strategies, and personnel with specific expertise, organizations may better protect themselves against cyber threats while maintaining or even reducing the resources dedicated to cyber security.

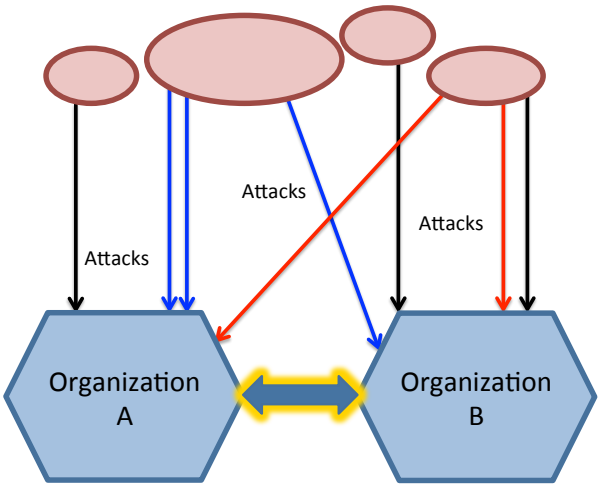

Figure 1: Cooperation can guard against attacks from similar sources and with similar traits

Despite these potential benefits, cooperative cyber defense strategies are not common. Cyber defense teams must balance the potential benefits of cooperation against motivations not to cooperate. For example, if its vulnerabilities are made publicly known, an organization might become more susceptible to cyber attacks and might face damage to its reputation. Trust in cooperating organizations is therefore necessary for successful cooperative cyber security programs. Since organizations that are likely to cooperate with each other are those that face similar threats, they might also be in similar industries and have competitive relationships. Competition for customers, clients, or funding may raise concerns about motive and competitive advantage, making organizations less likely to trust each other. Finally, group inertia is a significant factor to overcome, and individual habits may be even more difficult to change than organizational strategy.

Some work has considered the technical issues involved in cooperative cyber security (Hui et al. 2010), as well as potential program designs in cyber (Sandhu et al. 2010) and other information sharing (Luna-Reyes 2006) applications, but social and organizational aspects that will likely play a major role in cooperative dynamics have not been sufficiently analyzed. Cooperative relationships between organizations have been examined (Ring and Van de Ven 1994; Oliver 1990; Luna-Reyes et al. 2008), but these relationships may be substantially different when their purpose is cyber security rather than for commercial purposes.

The potential for cooperation to improve defense and reduce resources may outweigh the obstacles. This work is a first step toward understanding the social and operational issues involved in implementing a program of cooperative cyber defense between organizations. The model described here looks at a simple cooperative structure that allows resource sharing between two organizations whose cyber defense teams do a significant amount of redundant work. The model describes the social and organizational dimensions of a potential cooperative relationship for cyber security between simple, generic organizations, focusing on decisions about whether and how much an organization should participate in cooperative behaviors. This model is the first phase in a project intended to improve our ability to design effective programs that improve cyber defense with limited resources

A Two-Organization Model of Participation in Cooperative Cyber Security

An organization must consider many different factors when making decisions about participation in a cooperative cyber security program. The risks and benefits of such a program must be weighed against each other, which is a difficult task when such programs are not widespread and potential outcomes are thus not readily apparent. A system dynamics model might be useful in understanding how the dynamics of such a program might unfold, which could help potential participants to understand the potential costs and benefits of cooperation.

This model depicts a simple system in which two organizations face similar cyber threats and are considering sharing their cyber defense resources. Each organization does some amount of cyber defense work that is redundant with work done by the other organization. In other words, there is some amount of cyber defense work that must be done separately for each organization, but the rest could be shared, rather than completed by each organization separately.

Figure 3 shows the basic feedback structure of the resource allocation decisions faced by the two organizations (the stock and flow structure is shown in appendix A, figure A1). Each organization has some amount of resources that it devotes to cyber security, and allocates those resources between two types of tasks. The first type of task is non-redundant, and must be done separately for each organization. The second type of task is redundant. Redundant tasks are those that can be done once, by either organization, and results of the tasks can be shared with the other organization to reduce workload. Each organization uses the fraction of tasks (both non-redundant and redundant) being completed to decide whether more or fewer resources should be

allocated to cyber security. Each organization attempts to minimize the resources it allocates to cyber security while ensuring that the cyber tasks are completed to the maximum possible extent. This minimizes (but does not eliminate) the risk of a successful cyber attack, while maximizing the resources available for non-cyber-related organizational activities.

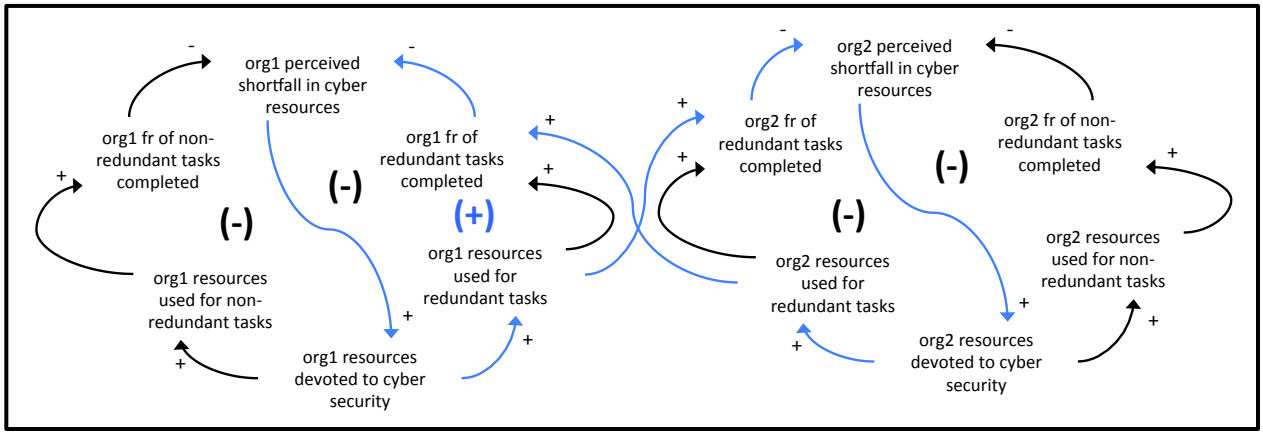

Figure 2: Feedback structure of resources sharing between organizations

A new feature of the causal structure is formed when cooperation becomes viable. In this case, resources allocated to cyber defense by one organization can augment the completion of redundant tasks for the other organization, allowing the second organization to reduce the resources it devotes to cyber security without losing effectiveness of cyber defense. If both organizations agree to cooperate to complete redundant tasks, both organizations may be able to devote fewer resources to cyber defense without sacrificing effectiveness.

The resource allocation structure shown in figure 2 addresses the potential benefits of cooperation in cyber security, which are weighed against risks to determine whether such a program should be established. Figure 3 shows the feedback structure of the decision-making process for a single organization (the stock and flow structure is shown in appendix A, figures A1 and A2). This portion of the model determines the strength of the cooperative agreement between the two organizations. The first feedback loop in figure 3, shown in blue, includes a simplification of the structure shown in figure 2. This loop represents how the benefits of cooperation, especially the increase in efficiency when resources are shared for redundant tasks, encourage an organization to strengthen its cooperative agreements. If benefits of cooperation have been realized in the past, then the organization is more likely to support cooperation in the future.

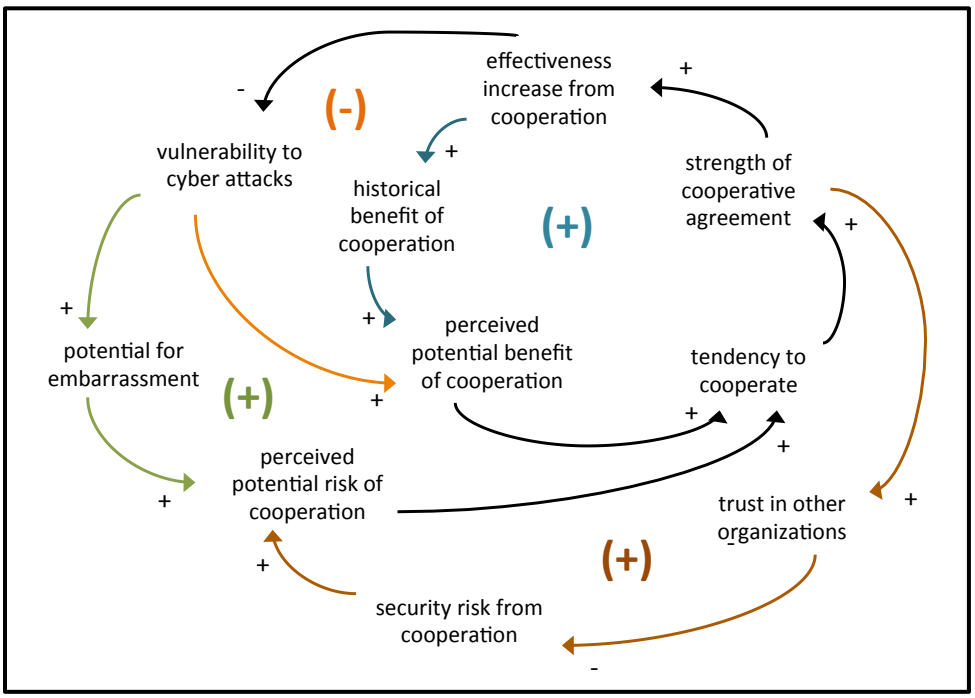

Figure 3: Feedback structure of decision-making process for one organization

Three feedback loops might counteract the benefit loop. First (shown in orange), if the cyber security of an organization is strengthened then it may feel less vulnerable to cyber attacks. This would encourage the organization to reduce its support for a cooperative agreement, since perceived vulnerability encourages cooperation. There are also two feedback loops in this system that concern the risks involved in cooperation. The first (shown in green) addresses the potential for embarrassment if it becomes known that the organization is vulnerable to cyber attacks. This could mean lost business, reduced trust from customers, or lost reputation for security practices, any of which could cause serious damage to the organization. However, if cooperation improves security, the risk of embarrassment from cyber attacks decreases.

The other risk-based loop (shown in brown) addresses the possibility that cooperating organizations may not fully trust one other. Cooperative agreements may involve sharing sensitive information, such as details of organizational structure, vulnerabilities, and information about cyber attacks and strategies for counteracting those attacks. This information could be dangerous if used for the wrong purposes. Furthermore, organizations that are likely to cooperate with each other are those that face similar threats, and are thus likely to be in similar industries and perhaps have competitive relationships. Trust may be difficult to build in these situations. This model assumes that trust between organizations is stronger when cooperative agreements have existed and produced benefits over some period of time. If trust grows, organizations become more likely to promote cooperation.

The model described here uses the same decision making structure to represent each of the two organizations in the system (future work will include more detailed and varied structures). Each organization determines its desire to cooperate, and the two desires govern the

strength of the cooperative agreement. The strength of that agreement and the risks and benefits that it produces then support future decision-making processes for each organization.

Results

The model was used to simulate two scenarios, where the primary difference was the intensity of cyber attacks experienced by the two organizations. This intensity is an important driver of the system because it helps to determine the organizations' perceived vulnerabilities to cyber attacks. In the base case scenario, both organizations face similar threats, and the intensity of attacks faced by the two organizations is equal. The second scenario involves uneven threats; in this simulation organization 2 faces a substantially more intense threat than organization 1. This alters the risk/benefit calculations for the two organizations as described below, changing the organizations' desires to participate in a cooperative agreement.

Figure 3 shows the strength of the cooperative agreement that results from each scenario. The simulation begins with no cooperative agreement in place. In the similar threats (base) case, the strength of the agreement builds slowly over the first year and a half. This growth depends on both organizations having some baseline belief that cooperation is likely to help with the effectiveness of cyber defense. After the first year and a half, both organizations begin to see significant benefits resulting from the cooperative agreement. The perceived benefits of cooperation encourage more cooperation, and the strength of the cooperative agreement grows more quickly in the next few years before leveling off with a strong agreement.

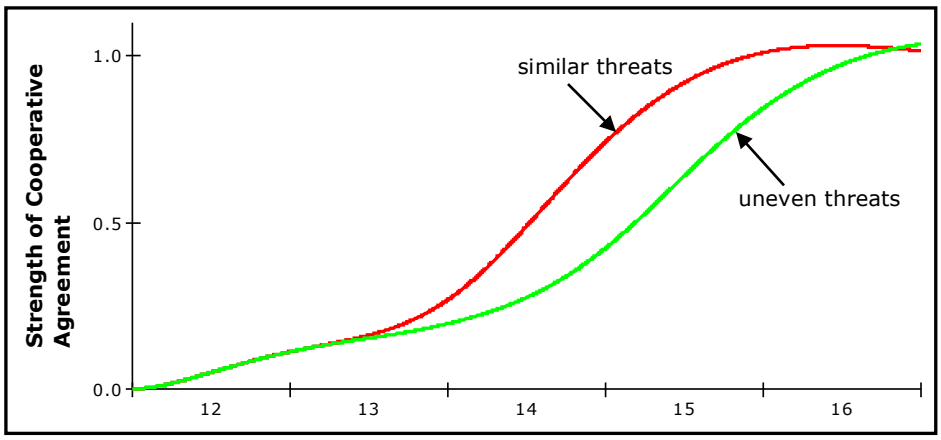

Figure 3: Strength of cooperative agreements for the base case and uneven threat simulations

The uneven threats case exhibits similar behavior to the base case at the beginning of the time horizon. For the first two years of the simulation, the cooperative agreement grows slowly based on a pre-existing belief that cooperation may help cyber defense. In the uneven threats case, the organization that faces a smaller cyber threat has less to gain from cooperation. This

organization is less enthusiastic about strengthening the cooperative agreement, and the agreement grows much more slowly than in the similar threats case.

The benefits of cooperation play a large role in decision-making, particularly in the later part of the simulations. These benefits result from the fact that cooperation allows organizations to achieve strong cyber defense while significantly reducing the resources they dedicate to cyber security. Figure 4 shows the resources dedicated to cyber security and used for cyber security by organization 1 for the similar threats (base) case. The results for organization 2 are identical. In this scenario, both organizations begin with a baseline level of cyber resources. As the cooperative agreement is strengthened, much of the redundant work is eliminated. This allows both organizations to achieve the same level of cyber security they would without cooperation, but at a reduced investment. Even though fewer resources are now allocated by organization 1 for cyber defense, more resources are actually used for the cyber defense of organization 1, because organization 2 contributes resources through the cooperative agreement. Since the tasks being eliminated are redundant, both organizations can reduce their investments in cyber defense resources, yet see more cyber defense work being done.

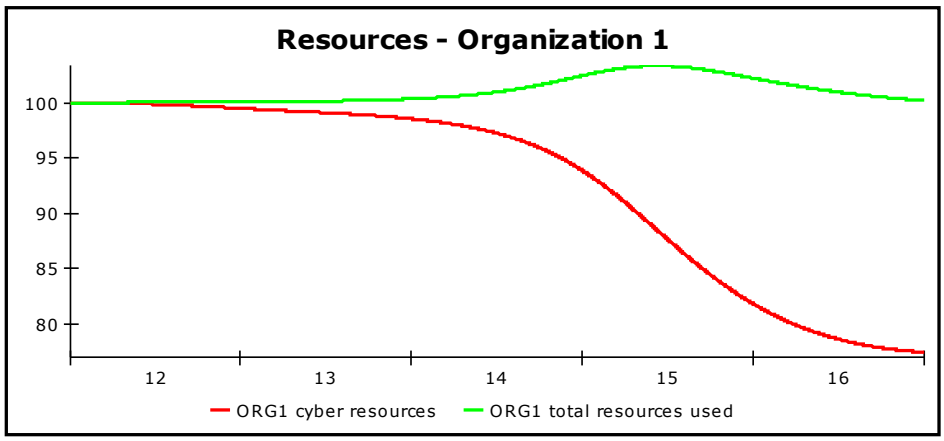

Figure 4: Resources contributed and used by one organization

When the risks faced by the two organizations are uneven, the risks and benefits of cooperation that each perceives (figure 5) also differ. In the uneven threats scenario, organization 2 faces a substantially more intense cyber threat than organization 1. Both organizations begin with low perceived benefits of cooperation; since no benefits of cooperation have yet been realized, these are based on a pre-existing belief that cooperation may be helpful. When benefits from cooperation do become apparent, organization 2 realizes that cooperation could provide a very large benefit. This perception also relies on the intensity of the cyber threat. Since organization 1 faces a less intense threat than organization 2, its perception of the potential benefits of cooperation is smaller. The intensity of the cyber threat also directly impacts each organization's perception of the potential risks involved in cooperation. Organization 2 sees a stronger threat, and thus considers itself more vulnerable and understands that the risks it faces

(from security or embarrassment) are quite large. Since it faces a less intense threat, organization 1 perceives a smaller risk of cooperation than organization 2.

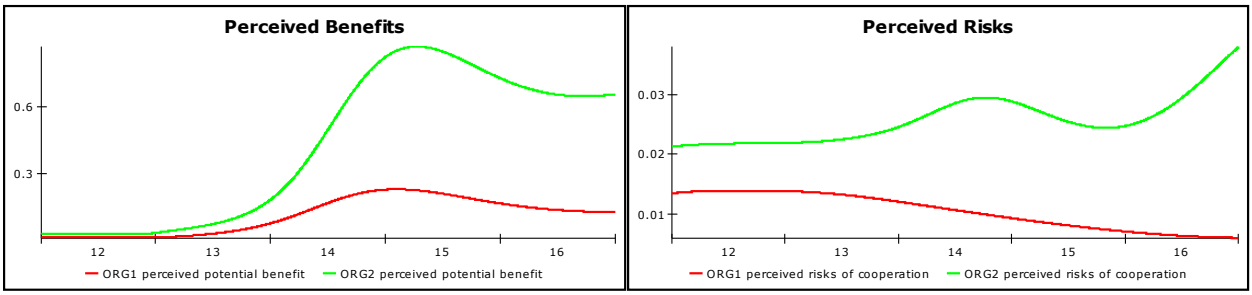

Figure 5: Perceived benefits and risks for each organization in the uneven threats case

For both organizations, the potential benefits of cooperation are substantially larger in magnitude than the risks. Organization 2 is therefore much more eager to strengthen the cooperative agreement than organization 1. Both parties must agree in order for the agreement to be strengthened, so diminished interest from organization 1 in the uneven threats scenario (as compared to the similar threats scenario) results in a weaker agreement.

Conclusions

This model indicates that in a simple system where redundant cyber security work can be reduced through cooperation, the benefits of a cooperative agreement can be substantial. Rather than duplicating work to detect, understand, and defend against cyber threats, energy can be deferred into more useful defensive strategies or other organizational goals. Stronger defense can be realized without increasing the resources dedicated to cyber security.

These results also suggest that cooperative cyber agreements are likely to work best when participating groups face threats at similar intensities. An organization that faces fewer threats is likely to be less interested in a cooperative agreement than an organization that faces many serious cyber threats. Differences in the intensity of threats to cooperating organizations could cause distrust and a high perceived risk of cooperation.

In the first few years of a program of cooperation, organizations are likely to participate minimally. They might declare support for a cooperative program, but substantial resources will likely not be contributed until the benefits of cooperation are apparent. The success of these programs is thus likely to depend on whether benefits are realized before the organizations involved lose interest. Once benefits are apparent, participation will likely be influenced by the threats faced by each organization. The success of an agreement will depend on there being sufficient threat to make cooperation attractive. Full participation is also likely to depend on trust between the organizations; low-trust or competitive relationships will make a cooperative agreement less successful.

This model simulates the potential outcomes and decision-making processes involved in cooperative cyber security agreements designed to reduce redundant work. It is the first step in a project designed to understand the potential for organizational cooperation to improve cyber defense. A substantial amount of work remains to be done to understand this problem. Future adaptations of this model will incorporate cognitive models of the individuals and groups involved in decision-making about cooperation in cyber defense. The model will be used to explore likely outcomes of these systems when the organizations involved have different characteristics and tendencies. We will also explore cooperative agreements with more than two participating organizations. Validation data will be collected from cyber security training exercises, historical data, and subject matter experts. Further psychological and economic theory, including cognitive dissonance (Festinger 1957), the theory of planned behavior (Ajzen 1991), bounded rationality (Simon 1957), qualitative choice theory (McFadden 1982), and prospect theory (Tversky & Kahneman 1974) will be incorporated to enhance the decision-making model. Cooperative agreements in contexts other than redundant work will be analyzed, and potential program designs will be studied. We will also explore likely changes in attitudes toward these programs as they become widespread, including tipping points that affect whether an organization will be willing to participate. We hope that this work will lead to a better understanding of the decision-making processes involved in cooperative agreements between organizations for cyber security, and will contribute to successful design of these programs.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179–211.

Festinger, L. (1957). *A Theory Of Cognitive Dissonance*. Stanford University Press.

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., & Endert, A. (2010). Towards efficient collaboration in cyber security. *Collaborative Technologies and Systems (CTS), 2010 International Symposium on* (pp. 489–498).

Luna-Reyes, L. F. (2006). Trust and Collaboration in Interagency Information Technology Projects. *Proceedings of 2006 International Conference of the System Dynamics Society, Nijmegen, The Netherlands*.

Luna-Reyes, L. F., Black, L. J., Cresswell, A. M., & Pardo, T. A. (2008). Knowledge sharing and trust in collaborative requirements analysis. *System Dynamics Review*, *24*(3), 265-297. doi:10.1002/sdr.404

McFadden, D. (1982), "Qualitative Response Models," in Advances in Econometrics, Ed. Werner Hildenbrand, Cambridge University Press, New York.

Oliver, C. (1990). Determinants of interorganizational relationships: Integration and future directions. *Academy of management review*, 241–265.

Ring, P. S., & Van de Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. *Academy of management review*, 90–118.

Sandhu, R., Krishnan, R., & White, G. B. (2010). Towards secure information sharing models for community cyber security. *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on* (pp. 1–6).

Simon, H.A. (1957). Administrative Behavior (2nd ed.). New York, NY: Macmillan

Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185, 1124-1131.

Acknowledgements

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Appendix A: Stock and flow structure of decision-making about cooperation for one organization in the system

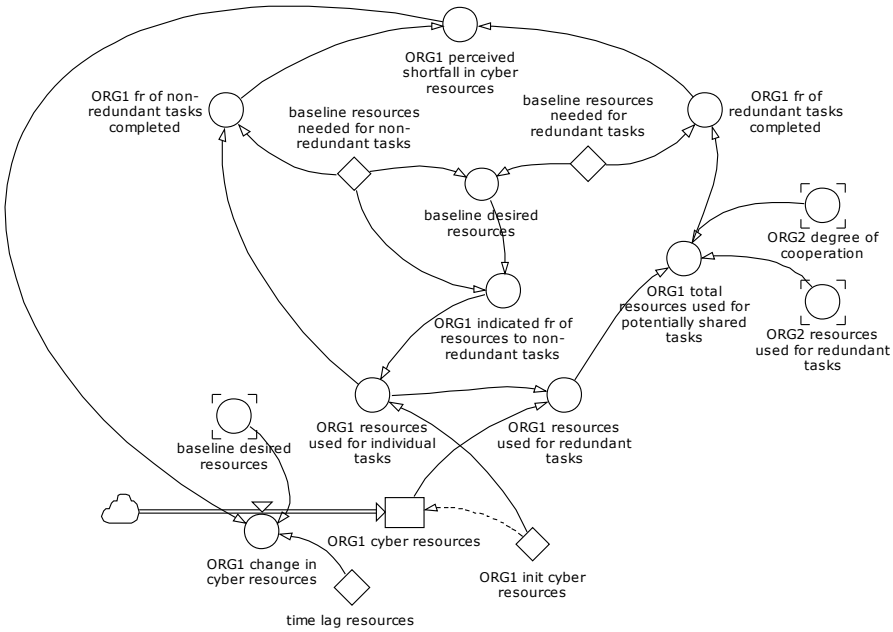

Figure A1: Distribution of cyber resources for one organization

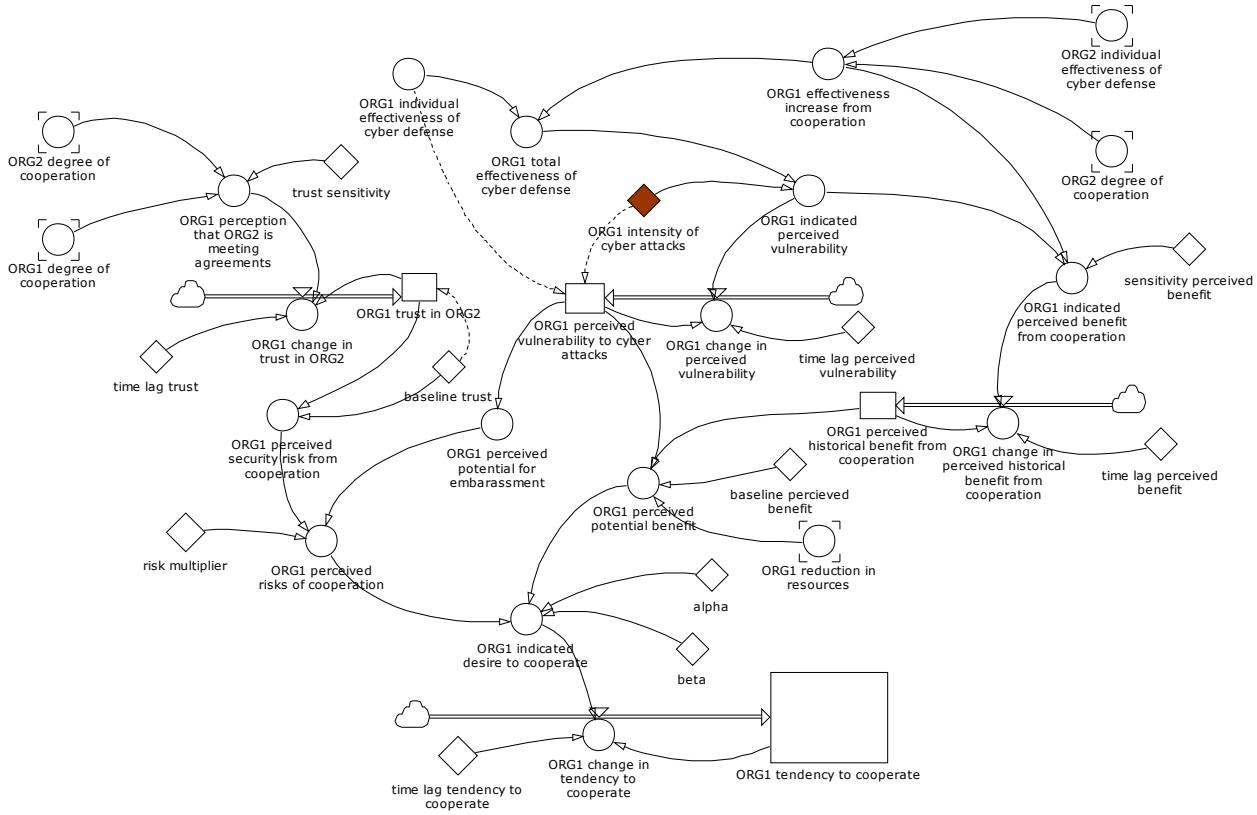

Figure A2: Decision making structure for one organization

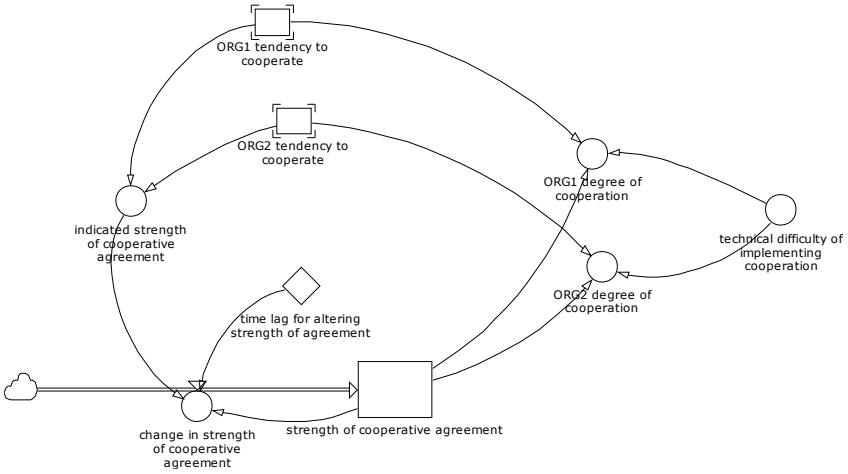

Figure A3: Determination of cooperative agreement