Social Computational Trust Model (SCTM): A Framework to Facilitate the Selection of Partners

1st Ameneh Deljoo
Informatics Institute, Faculty of Science
University of Amsterdam
Amsterdam, the Netherlands
a.deljoo@uva.nl

2nd Tom van Engers
Leibniz Center for Law
University of Amsterdam
Amsterdam, the Netherlands
vanengers@uva.nl

3th Leon Gommans
AirFrance-KLM
Amsterdam, the Netherlands
leon.gommans@klm.com

4th Cees de Laat
Informatics Institute, Faculty of Science
University of Amsterdam
Amsterdam, the Netherlands
delaat@uva.nl

***Abstract*—Creating a cyber security alliance among network domain owners, as a means to minimize security incidents, has gained the interest of practitioners and academics in the last few years. A cyber security alliance, like any membership organization, requires the creation and maintenance of trust among its members, in this case the network domain owners. To promote the disclosure and sharing of cyber security information among the network domain owners, a trust framework is needed.**

This paper discusses a social computational trust model (SCTM), that helps alliance members to select the right partner to collaborate with and perform collective tasks, and encourages the sharing of incident data and intelligence. The social computational trust model combines benevolence and competence to estimate the risk of interaction. Benevolence is computed from personal experiences gained through direct interactions and competence is assessed on the base of the received feedback from the other members. An agent based model case study is presented to demonstrate our approach. The practicability of the proposed risk estimation is validated with a detailed experiment.

***Index Terms*—Computational trust, alliances, cyber security, information sharing, risk assessment**

I. Introduction

Cyber attacks are a serious threat to our networked society as organizations are depending on the well functioning of the IT-infrastructure, which is essential for the IT-systems supporting their processes. As attacks are becoming more and more organized, collaboration across public and private organizations is required to arrange technical counter measures. Sharing cyber intelligence among different parties, such as internet & cloud service providers and enterprise networks, becomes increasingly important. Additionally, networks have evolved over the time and became more complex and less connected, therefore the protection of such a complex network can often only be guaranteed and financed as a shared effort. One of the benefits of information sharing among the members in an alliance is improving the decision and policy making in the different levels of organization and facilitating the selection of optimal cyber defense tactics during the attack period. Another benefit is the reduction of uncertainties regarding the performance, competence and availability of each member in the alliance [1]. Because of the limitation of each organization such as resources and expertise, no organization can resilience on its own, therefore needs to join the alliance to address the cyber attacks.

As cyber attackers also have found ways to share their practices, their victims (e.g. organizations) are required to collaborate with other parties across multi-domain networks to avoid the negative impact on the organization and its services.

The RSA [2] report mentiones that victims of the cyber attacks are the largest company. Currently, more than 60 million different malware variants are indexed; one third of the indexed malware came up in the last year. Based on the evidence from the cyber security reports, the attackers become highly organized, customized and coordinated. Therefore, there is need for cyber security alliances where the organizations collaborate with the other members to reduce the impact of attacks by employing counter measures [1], [3]. In order to support such collaboration, we need to organize and manage trust among the members, enabling the organizations to share the cyber information with their trusted partners.

This work is funded by the Dutch Science Foundation project SARNET (grant no: CYBSEC.14.003/618.001.016) and the Dutch project COMMIT (WP20.11). Special thanks go to our research partner KLM. The authors would also like to thank anonymous reviewers for their comments.

Despite the significant amount of research on the technical solutions to improve the effectiveness of counter measurements [4], little research in this domain has addressed the trust among peers.
In this paper, we explain how cyber security alliances can be supported in the establishment of partnerships within cyber security alliances by providing an ability to computationally evaluate potential partnerships among a community of alliance members. We focus on the social aspect of trust and select the right partner in the network to collaborate in joint tasks. As we stated in our previous publication [5], to create a cyber security alliance we need to define:

- a common benefit as a strong incentive for members to join the alliance, and subsequently encourage partners to create agreements arranging sharing of information and cyber defense resources, whilst being ensured that benefits and cost are shared in a fair and economical way.
- a trust framework to create and organize trust among the members,
- a common governance model to create common policies, standards and admission criteria for alliance's members.

Considering the above requirement is important it comes to the potentially sensitive and company-internal data. A trust model helps in expressing member concerns, which then can act as a means to reduce risk during the creation and maintenance of relationships. To organize and maintain trust among the members we employ a social model of trust, explained in this paper. Traditionally, information sharing on a peer-to-peer basis is mostly established based on personal trust. But, the social network of organizations changes with time; therefore, it demands to define a more sophisticated method to select a right partner for sharing intelligence. We aim to define a model of cyber security alliance that transfer the mentioned issues to the cyber space on a large scale.
In our previous publication [5], we used the service provider group (SPG) framework as a governance framework to define a set of common rules for the SPG members, which are subsequently administered and monitored. In this work, we discuss the following contributions:

1) the Social Computational Trust Model (SCTM) representing social trust and its components, which are important for evaluating the partners.
2) risk assessment through the SCTM model. The SCTM facilitates risk-based partner selection by combining the benevolence and competence factors. We identified two common risks for the alliances' members.

The remainder of the paper is organized as follows. Section II shows challenges and the problem statement. Section III highlights the importance of trust model, and the control and risk mechanism as a way to establish trust in section IV. We present the social computational trust model and its components in section V. Then, in section VI, we introduce the risk assessment framework and risk estimation method. Section VII presents a case study and our agent-based model demonstration. We review some of the trust frameworks in section VIII. Finally, section IX concludes the paper.

II. Challenges in Creating Alliances

In reality, there are several concerns, seen as risks for the organization, which result in the unwillingness of sharing information about the cyber incidents that they have experienced [6]. These factors include:

- Competition. Due to the conflict of interest among different organizations, they are often hesitant to share information with their competitors.
- Competence. Organizations may not want to rely on their partners' performance and become vulnerable to partners' choices and actions.
- Reputation. The reputation of organizations are often damaged by sharing the security information publicly.
- Privacy. Some shared data contains sensitive information about the victim or customer.
- Legal requirements, Rules and Policy. Alliances consist of different companies with different policies and subjected to different legal frameworks, which may operate in different countries or jurisdictions.

Our goal is to design a trust framework to facilitate the information sharing among the organizations, while taking into account the above-mentioned requirements .

III. Trust

Trust is seen as a key for any interactions in the social system. Trust has been studied in different areas from sociology to psychology [7][1]. Most trust definitions focus on exposing the given member to vulnerability. Luhmann [9] defined trust as having confidence that the expectation about the given member will be considered by the trustor [9], entails positive expectations regarding the other party's action in risky situations [10] and includes adopting a belief without having all information about the other party 's belief [11]. Trust among the alliances members has been empirically demonstrated to be important for alliance formation [12]. Trust has some benefits for the alliance such as can be seen as a substitute for formal control mechanisms, reduce transactions costs, facilitate dispute resolution, and allow more flexibility. When trust among partners is high enough, partners have enough confidence in each other and result in less opportunistic behavior [9].

In this work, we consider the following description given by Mayer: "*Trust is the willingness* of trustor to be vulnerable to the actions of trustee based on the expectation that the trustee will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other parties" [7]. We define trust as the expectation held by one member that the other member will not exploit

1. An elaborated overview of the concepts used in the organizational context can be found in studies performed by Bachmann [7], [8].

its vulnerabilities when faced with the opportunity to do so [5], [7], [13], [14]. This expectation is confirmed when the given member:

- Have the potential ability of a trustee to perform a given task (Competence),
- Adhere to the set of rules and act accordingly to fulfill the commitments (Integrity), and
- Act and do good even if unexpected contingencies arise (Benevolence).

The trust framework is depicted in Fig. 1. As we mentioned before, a member is trustworthy if he has an ability to perform a task in a given situation, his integrity, and a positive relationship with the trustor. Therefore, it is important to estimate the trustee's trustworthiness by considering each of these three dimensions individually and combine them in a dynamic way by considering different situations and stages of relations. However, most of the computational trust approaches evaluate the trustee trustworthiness as a block and does not consider different trustworthiness's dimensions. Our inter-organizational trust model is based on the three components: competence, integrity, and benevolence. In the following, we present a computational trust model grounded, on the multidisciplinary literature on trust [7], [8], [15], which is able to estimate the competence, integrity, and benevolence of the trustee under evaluation.

IV. Control and Risk

Control and risk have been studied and described as one of the steps towards establishing trust [7], [9]. The theoretical bases for the control concept of the alliance governance model derives from two sources: transaction cost economics and a key mechanism to control partner opportunism respectively [12]. Risk has been defined as one of the element of trust by different scholars [7], [16], [17]. Das *et al.* [17] and Mayer *et al.* [7] presented two types of risks (i.e. rational risk and performance risk) that involved in the process of creating and managing trust among the alliances members.

Some of the researchers show that due to the nature of the alliances members (i.e. self-interested) the relational risk in alliances is considerably high because the self-interested members act opportunistically to maximize the results of interactions for their organizations, rather than striving for optimal outcomes for the alliance. The alliance governance model has been proposed to prevent partners from abusing the alliance by taking advantage of opportunist possibilities. Adequate legal and ownership safeguards, detailed contracts, equity investments, and strict rules agreed between the partners are the example of governance models. We use the SPG as a governance model to present the adequate standards and policies for the members. This model also describes the need to monitor members to detect unwanted behavior such as opportunism, abuse or fraud. The SPG framework has been introduced in previous publication [5], [18], where we investigated the role of SPG in defining the set of common rules for the alliances and detecting undesirable behavior in the alliance. The detail of the SPG framework is beyond the scope of this paper.

The SCTM serves two purposes: It evaluates the trustworthiness of partners and estimates the risks involved in creating the alliance.

We use the basic concepts of SPG and combine these with ideas from the trust and risk literature to explain how these factors impact the structure of governance model and control mechanisms in alliances. The proposed model of relations is presented in Fig. 2. The SCTM framework with its antecedents that we use for the rest of the paper as trustworthiness components is depicted in Fig. 1. In addition, Fig. 3 depicts the proposed risk framework and its modules. We present that how the risk modules are functionally related to evaluate trustworthiness and risks.

V. Our Social Computational Trust Model

This section, introduces the proposed social computational trust model. This model provides the basis for the decision making process that each member has to perform when deciding on collaborating or not with other members. This process can be broken down into three sub-processes: (1) assess the members' integrity by introducing a compliancy check mechanism, (2) evaluate trust based on three distinctive factors (integrity, benevolence, and competence), and (3) estimate the rational risk and cost of entering the alliance according to the trust value. In this paper, we only focus on competence and benevolence factors; integrity will be addressed in a seperate publication.

In our previous work, we have presented an evaluation trust function that can evaluate the trustworthiness of each member based on the stage and type of relationship with trustor [19]. In the following sections, we present our social computational model to evaluate trust based on its components (i.e. competence and benevolence).

V.1. Notation

The proposed computational trust model is applied to environments where trustor agents choose the best trustees to interact with, with or without the posterior establishment of detailed agreements between partners.

The agent society denotes A, where it includes trustee and trustor $x, y \in A$. In this research, each member can be represented as a trustee or trustor. $T_{(x,y)}$ represents as the amount of trust x has in y in a situation S, where $S = \{s_1, s_2, ..., s_n\}$ is the set of all the possible situations in the society.

In order to define the situations that lead to an agreement, Abowd *et. al* define the context which consists of four main dimensions: identity, time, location, and activity [20]. Urbano *et. al* [21] extended the concept of context and identified eight dimensions of context $\{d_1, d_2, ..., d_8\}$, where dimensions d_1 and d_2 represent the agents : the trustor and the trustee, respectively; d_3 and d_4 represent time and the location of agreement; and d_5, d_6, d_7 and d_8 recognize and characterize the task type, its complexity, deadline,

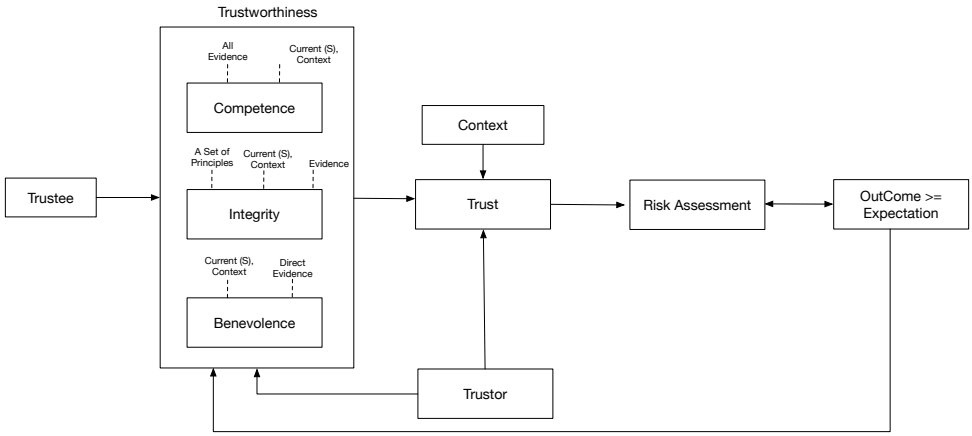

Fig. 1. Three trustworthiness components are benevolence, integrity, and competence is presented in this framework. We estimate trust, by combining the outcome of each component. Based on the outcome, the trustor makes a decision about the given trustee and their relationship.

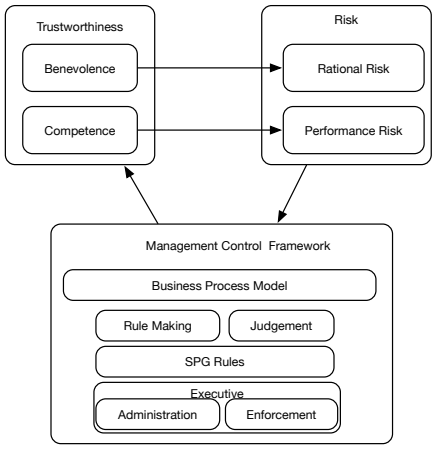

Fig. 2. Management control package. In the bottom of this figure, we have the SPG framework as the governance model, which is responsible for defining the rules and policies of the alliance. In the Risk module, we estimate the relational and performance risks based on the benevolence and competence components.

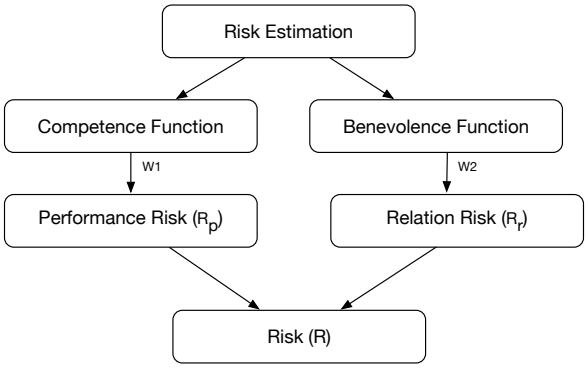

Fig. 3. Functional relationships between SCTM modules that are used to estimate the performance and relation risk.

and outcome of task, respectively. We adopted the context definition of Urbano et al. [21] in this paper. As for dimension (d_8), outcome, we distinguish three different values, $O = \{Fd, Fdd, V\}$, where Fd (fulfill duty) denotes that the trustor believes that the trustee performed the given task on time, Fdd (fulfill duty with delay) means that the trustee was performed the task (or duty) with an (un)expected delay, and V (violation) means that the trustee did not perform the given (agreed) task.

In this paper, we assume that all agreements among trustor and trustee refer to the same type of task t, but with different degrees of task complexity (d_6) and deadlines (d_7) for the (sub-)tasks.

- (d_6): The task complexity depends on different factors such as the attack type, a company size, number of resources that an organization needs to mitigate an attack. For simplicity, we exclude the task complexity from our formalization. Instead, we consider the importance of each task (i.e. how important or urgent task is.), which we explain in section VI.
- (d_7): The trustee needs to answer the trustor's request within a certain time window $Time_w$, therefore, we calculate the deadline of task (d_8) for each (sub)-tasks and it can be varied for different requests.
- (d_8): We employ algorithm1 to calculate the outcome of each task.

Algorithm 1 Calculate the Outcome Based on the Task Deadline.

Require: $Time_w$: time window.
Require: Req_t: request time.
Require: Rep_t: report time.
1: $d_7 = Req_t - Rep_t$
2: **if** $d_7 <= Time_w$ **then**
3: $d_8 = Fd$
4: **else if** $d_7 > Time_w$ **then**
5: $d_8 = Fdd$
6: **else if** $d_7 = 0$ **then**
7: $d_8 = V$
8: **end if**
9: **return** d_8

The $Time_w$ window is defined by the trustor, and the trustor sends a request to the trustee, which is (Req_t). The trustee will answer the request, this time called report time, which is (Rep_t). In line 1, we calculate the deadline of task and following the algorithm report the outcome of task by comparing the deadline to the time window that has been set by the trustor. In line 2, the value of d_7 is compared with the $Time_w$ and if it is smaller then the outcome will be Fd. If the deadline is bigger than the $Time_w$, the the outcome will be Fdd for that task (line 4). Otherwise, the outcome will be V (line 6).

In table 1, we have summarized the notations that we use for the rest of the paper. In the following, we assign values

2. Dimension are: • d_1 = trustor, d_2= trustee • d_3 = time, d_4= location, d_5= task, d_6= complexity, d_7= deadline • d_8= Outcome

TABLE 1. NOTATIONS AND VALUE

Description	Representation	Value Range
Agent	x,y	
Situations	S	
Society of Agents	$x, y \in A$	
All the situations	$s_i = s_1, s_2, ..s_n$	
Tasks	t	
Sub-tasks	$\alpha 1, ...\alpha 4$	
Context	$D = d_1, d_2, ...d_8$ [2]	
d_8	FD, FDD, V	1, 0.5,0
Trust x on y in the situation S	$Tx_{(y,S)}$	[0,1]
All the available evidence on y	$Ex_{(*,y)}$	[0,1]
All the direct evidence on y	$E_{(x,y)}$	[0,1]

to each situation ($s_i \in S$). The outcome of interactions between trustor (x) and trustee (y) called evidence (E). In the current SCTM framework, we will only consider confirming evidence and neglect the fact that in reality both confirming and dis-confirming evidence plays an equally important role. We consequently define a set of evidence ($e_i \in E$) and assign the value to each evidence where ($e_i \in [0, 1]$). Finally, the set of all the existing evidence on a given trustee is represented by $Ex_{(*,y)}$. Following, $E_{(x,y)}$ shows all the evidence about the direct interactions between trustor (x) and trustee (y).

V.2. Social Computational Trust Model

The social computational trust model that we explain in this paper combines two distinct functions: the competence evaluation function ($Com_{(x,y)} : S \times Ex_{(*,y)} \in [0, 1]$), and the benevolence evaluation function ($Ben_{(x,y)} : E_{(x,y)} \in [0, 1]$). $T_{(x,y)}$ in Equation. 1 returns the estimated value of the trust that trustor x has in trustee y in situation S.

$$T_{(x,y)} : Ben_{(x,y)} + Com_{(x,y)}. \quad (1)$$

We illustrated the computational model in Fig. 4.

V.3. The benevolence function

Several scholars are considered the Benevolence as a one of the key elements of trust and the trustworthiness's antecedent (e.g. [22], [23]). The value of the benevolence, $Ben_{(x,y)}$, of trustee (x) toward trustor (y) is computed from their mutual interactions (i.e. $E_{(x,y)}$) in the situation S. The estimated value for the benevolence function which is in the interval of $[0, 1]$, is

$$Ben_{(x,y)} = \frac{1}{|S|} \sum_{s_i \in S} (val(E_{(x,y)})), \quad (2)$$

where S is the set of situations, in which x has interactions with y.

V.4. The competence function

The competence evaluation function $Com_{(x,y)}$ evaluates the given trustee ability in performing a given task t in the

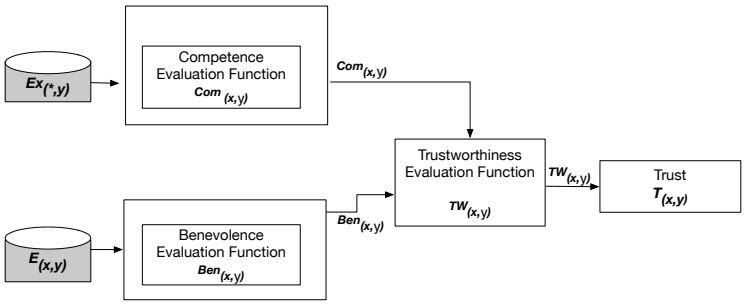

Fig. 4. Social computational model of trust.

specific situation $s_i \in S$. All the evidence available on the trustee under evaluation are taken as inputs, $Ex_{(*,y)}$. Similar to benevolence function, the estimated value for competence function of the agent, $Com_{(x,y)}$, is in the interval of $[0, 1]$.

$$Com_{(x,y)} = \frac{1}{|S|} \sum_{s_i \in S} (val(Ex_{*,y})), \tag{3}$$

where S is the set of all situations in which x has interactions with y.

The aim of the SCTM framework is to estimate the interaction risk among the alliance members. We evaluate the risk by using the computation of benevolence and competence of a given member. The risk estimation framework is presented in Fig. 3.

When a member (trustor) decide to estimate the interaction risk with the given member (trustee), trustor sends a request to the risk estimate block regarding the estimation of the interaction risk for the given member (e.g. a network domain). This block appoints the request to competence function and benevolence function and assign $W1$ and $W2$ as weights to each block to compute the relation's risk and performance risk, respectively. In the following we explain our risk estimation framework in details.

VI. Risk Estimation Through the SCTM Model

As stated before the aims of the SCTM is to help the alliance members to identify a "right" partner to collaborate with for the joined tasks. The term "right" implies that the alliances member has enough benevolence and competence. This reflects in a low perceived interaction risk. The authors in [17] defined the total perceived interaction risk as a summation of tow risks, which are relational and performance risk. The perceived interaction risk is given as:

$$R = R_r + R_p, \tag{4}$$

where, R_r denotes relational risk and R_p is performance risk. Das *et al.* [24] defined relational and performance risks as follows:

- Relational risk. The probability [3] and consequence [4] of not having a successful cooperation. Therefore, because of potential opportunistic behavior the relational risk will be increased.
- Performance risk. The probability and consequences that alliance objectives are not realized despite satisfactory cooperation among the partner.

Based on the definition of relational risk, we can conclude that this type of risk and the opportunistic behavior of partners increases in the alliances, in the case of lack of trust among the partners [17]. We demonstrate our assumption through the following propositions.

Proposition 1. benevolent [5] behavior of partners increases trust and reduces former perceived relational risk in the alliance. We formulate this proposition as follow:

$$R_r(x, y) \propto \frac{1}{Ben_{(x,y)}}, \tag{5}$$

where, $Ben_{(x,y)}$ is the benevolence of x towards y.

We defined competence as the ability of the partner within the alliance to perform according to the specified agreement or contract. Higher competence will consequently result in a lower perceived performance risk. Competence is key to achieving the alliance's goal. Therefore, we formulate the following proposition to show this relation.

Proposition 2. The perceived performance risk will be reduced if the competence of the given member is high.

Proposition 2 can be represented as:

$$R_p(x, y) \propto \frac{1}{Com_{(x,y)}}, \tag{6}$$

where, $Com_{(x,y)}$ is the competence of x with respect to y. We drive the perceived interaction risk as:

$$R_r(x, y) = w_1 \frac{1}{Ben_{(x,y)}} + w_2 \frac{1}{Com_{(x,y)}}. \tag{7}$$

3. Probability is defined as the possibility of an adjusted asset. In the cooperative network, it depends on parameters such as opportunistic behavior (relational risk) of the alliance or commercial/technological/strategic hazards (performance risk).

4. Consequence is translated as the effect of unfavorable occurrence (like an unauthorized usage of resources) on the organization revenue.

5. Some of the scholars consider faith and good intentions instead of benevolence.

The motive underlying the opportunistic behavior has been studied by many researchers [24]–[26]. In [24], the authors stated that the context of interaction is the rational motive behind the opportunistic behavior. The opportunistic behavior counts as a reason that increases the relational risk. The relational risk in any alliance increases if one of the partners finds it difficult to protect its own resources from other members, this act can be seen as the opportunistic behavior [17].

In contrast, performance risk occurs if one of the members has a higher return on the investment (or utility) expectation by performing a different task than the one that would meet the alliance objective.

March et al. [27] describe how decision-makers apply weighing potential gains and losses to estimate risk. In their view, a higher expectation on the irrecoverable investment leads to the perception of higher performance risk.

Therefore, we assign the context importance as W_1 and utility benefits as W_2 respectively, which also used by Marsh's risk model [27].

We formalize the importance as: function (I_c) that calculates the important degree of the context from trustor x perspective. The importance degree of the context is a subjective judgment of any context defined in $[0, 1]$. Marsh stated that the negative concept of importance has been discarded, as the cooperation game among agents is directed towards getting the job done.

While this may not be realistic in every concrete situation, e.g. betrayal or invasion by trolls may require a different conception, but for simplicity reasons we will limit ourselves to positive importance for now. We define utility as a function $U_c(\alpha)$ that measures the amount of utility that the trustor expects to gain from the context α. The utility values are in the interval of $[0, 1]$.

Substituting the context importance and utility benefits in Equation 7 reads:

$$R_r(x, y) = I_c(\alpha) \times \frac{1}{Ben_{(x,y)}} + U_c(\alpha) \times \frac{1}{Com_{(x,y)}}. \quad (8)$$

The SCTM contains various factors, including benevolence and competence. We expressed the functional relationship between the importance of context and relational risk, and the relationship between utility benefits and performance risk in a computational form. Trust is resulting from the perceived interaction risk that is the combination of the relational and performance risk. In the next section, we will demonstrate how this SCTM can be used in deciding on transactions between alliance members. For this demonstration we used an Agent-Based Modeling (ABM) based simulation.

VII. Result and Discussion

We have implemented the proposed framework using ABM in the Jadex platform [28]. We have defined a case that has the main characteristics of typical alliances. The ABM simulation demonstrates how the risk assessment mechanism based upon our SCTM supports the partner selection.

VII.1. Case Study

We use the ABM simulation to test **Proposition 1** and **Proposition 2**.

We have set up an alliance network, a collaborative network of organizations, shown in Fig. 5. This social network represents a collaborative network of organizations like the ones we study in our SARNET [6] research project [7] where service providers collaborate and act on behalf of partners, acts that may harm the individual interests, all in order to protect the collaborative network against cyber attacks. Each node represents an autonomous organization that needs to build trust with other parties and share incident information within the alliance network based on the agreement among the members. Basically, we considered that there was only one task being negotiated by all members, which mitigates and defend the alliance against a certain attack (d_5). Let us consider that at present, six partners of SARNET Alliance collaborate to perform the tasks. The domains' members are denoted as N, X, Y, M, D, and Z respectively. One of the SARNET member N, is under attack and requested its neighbors to perform certain tasks. N wants to choose ideal domains for collaboration in order to mitigate and defend against a certain attack. We define four different sub-tasks ($\alpha_1 ... \alpha_4$) respect to the context definiation that we presented in section V.I. In this case study, the d_5 dimension, which is the task type consists of the following sub-tasks: α_1 provide resources within a certain time window, α_2 monitor certain traffic, α_3 block a certain link, and α_4 implement a certain counter measurement. As mentioned in sectionV.I, each task contains the task complexity (d_6^t), deadline (d_7^t) and outcome of task (d_8^t). The task complexity (d_6^t) and deadline (d_7^t)values defined based on the scenarios and we calculate the deadline (d_7^t) and task outcome (d_8^t) by using the algorithm 1.

In our simulation, each task has two factors: importance (I_c) and utility (U_c) (see Equation 8). The values assigned to these levels are $0.25, 0.15$, respectively [8]. These values have been given as the input to the SCTM framework.

The SCTM focuses on the three possible results of trustee, being the agents that is supposed to respond on a request of the trustor. This trustee may fulfill its duty according to the agreement (Fd) fulfill the agreement with delay (Fdd) or retaliate, resulting in a breach of the agreement (V). The trustor can decide that a delivery with delay should be treated as delivery (Fd), a failure (V) or it can leave it as is (Fdd) when communicating about the experience to others. SCTM estimates benevolence (see Section V.III) and competence (see Section V.IV) for all the members under the four sub-tasks (α_1,..,α_4).

The interaction risk is evaluated by using Equation 8. It may be observed in Sections V.I that multiple parameters (called dimensions) are required to evaluate trustworthiness. However, to estimate trustworthiness, we do not have to input all

6. SARNET: Secure Autonomous Respond NeTwork

7. The technical details about the SARNET project can be found in http://delaat.net/sarnet/index.html

8. The values are adopted from [21], [29]

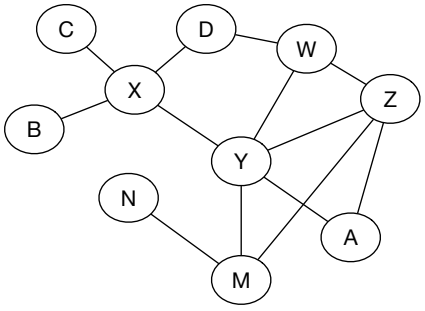

Fig. 5. Social Network Schema.

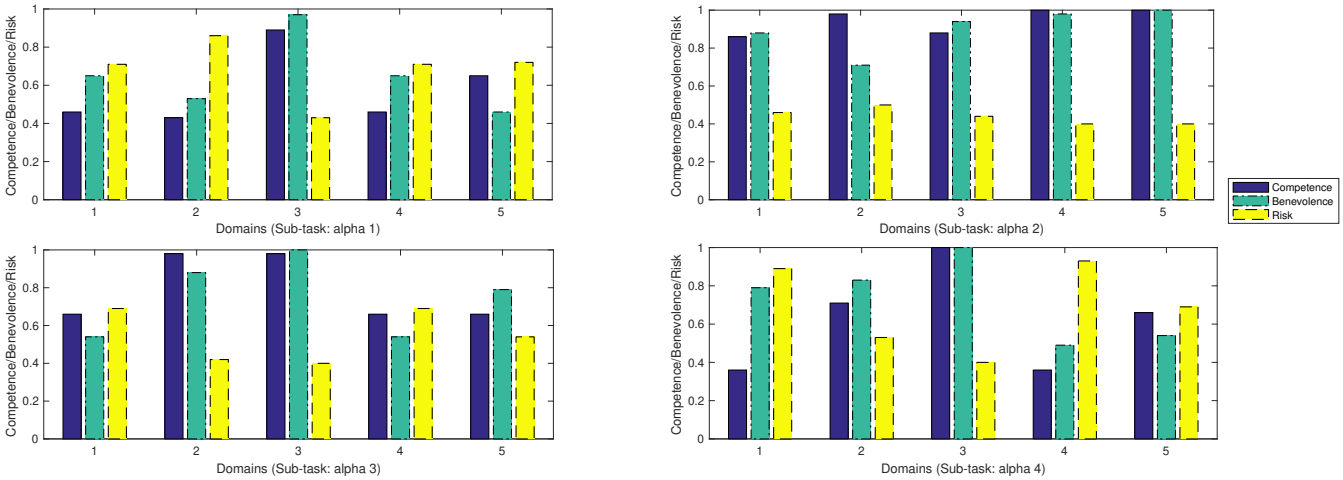

Fig. 6. Variation of Benevolence, Competence, Risk Under Different Sub-Tasks.

TABLE 2. COMPETENCE, BENEVOLENCE AND PERCEIVED INTERACTION RISK FOR DIFFERENT SUB-TASKS PER DOMAIN

Context	Domains	Competence	Benevolence	Risk
Alpha1	X	0.65	0.46	0.71
	M	0.53	0.43	0.86
	Y	0.97	0.89	0.43
	Z	0.65	0.46	0.71
	D	0.65	0.46	0.72
Alpha2	X	0.86	0.88	0.46
	M	0.98	0.71	0.50
	Y	0.88	0.94	0.44
	Z	0.86 0.88	0.45	
	D	0.86	0.88	0.46
Alpha3	X	0.79	0.36	0.88
	M	0.88	0.98	0.42
	Y	1	0.98	0.40
	Z	0.54	0.66	0.69
	D	0.54	0.66	0.69
Alpha4	X	0.79	0.36	0.88
	M	0.83	0.71	0.53
	Y	1	1	0.40
	Z	0.49	0.36	0.93
	D	0.79	0.66	0.54

these parameters. The majority of these parameters as input are subjective or selective (selected based on initially defined inputs set such as time and location of the agreements). For the risk estimation scheme the values for importance (I_c) and utility (U_c) are given from subjective judgment. In Fig. 6 the risk, benevolence, and competence values for all sub-tasks are presented As explained before, one of the goals of our trust framework is to estimate the interaction risk for any alliance's member based on the member's benevolence and competence value. Therefore, based on the given task, SCTM recommends the member to collaborate with those who have the minimum interaction risk.

In Fig. 6, the risk values for each member with varying context have been shown. By assuming the recommendations by SCTM on the member with the minimum interaction risk, the following members will be chosen for four sub-tasks:

- Y. For sub-tasks $(\alpha_1), (alpha_2), (alpha_3), and (alpha_4)$.
- X, Y, Z, D. For sub-task $(alpha_2)$.
- M. For sub-task $(alpha_3)$.

We can observe from Fig. 6 that domains with the higher benevolence and competence values having the minimum risk and SCTM will recommend them to other alliance members.

As illustrated in Fig. 6, the risk value rises/falls if benevolence and/or competence of domains' members decreases/increases. However, the significant observation is that even if two domains have the same competence value (e.g. X, M in the $alpha_1$), the one with higher benevolence result in lower interaction risk. Another example of such behavior, is seen in $alpha_2$, where X and Z have the similar competence values. We conclude that for interactions, benevolent domains with less competence are favorable over those (non-benevolent) with higher competence. This is explained by the fact that competent member with lower benevolence values are capable to damage their partner with higher impact than those who are benevolent but incompetent. In table 2, we have summarized competence, benevolence and the total perceived interaction risk for four different sub-tasks, which performs by different domains in our alliance network.

VIII. Related work

Many computational trust models have been presented by different scholars, nevertheless, only a few models are actually social computational models. One of the conceptual models of social trust developed by Adalie *et al.* [30] is based on Kelton *et al.*'s model [31] which takes ability, positive intentions, ethics, and predictability as the trustworthiness components [31]. They used a probabilistic approach in their model, however, by realizing the limits of the approach in the treatment of the social concepts their model was not implemented [30].

Among all the presented computational trust models [32], the only computational approach that includes a complete set of features established based on the theory of trust is the socio-cognitive model developed by Castelfranchi and Falcone [15]. The model defines a trustor and trustee, where the former has a goal that can be achieved by the later. In their view, trust is made by considering the different beliefs that the trustor has about the trustee, both internal (beliefs on competence, disposition, and harmfulness) or external (opportunities and dangers). The importance of these beliefs is further adjusted by meta-beliefs about the relative strength of each belief. In practice, it is difficult to implement due to its richness. The present implementation of such a model (e.g., [15]) includes many simplifications in the theoretical model and needs extensive manual configuration by a domain experts for each trustee and task under assessment. Another constraint is the necessity of explicit information about the competence and disposition (or similar beliefs) of the agent under evaluation, which is usually difficult to get in dynamic agent-based environments.

Another social trust model was presented by Urbano *et al.* [21] called situation-aware social computational trust Model (SOLUM). Their computational model consists of two parts: 1- a general framework of computational trust, which is based on two fundamental characteristics of trust, the trustor's disposition and emotional state. The Mayer's trustworthiness dimension that includes the ability, integrity, and benevolence was adapted to determine the trust. For the second part, they proposed a set of distinct techniques to extract information about the individual dimensions of the agent's trustworthiness from the set of structured evidence available to the agent. The main difference between our model and Urbano's model is that we consider different stages of relationships for the competence function. We slightly adapted and modified the Marsh [27] competence formulization by considering three different situations for trustor to make a decision about the (future) collaboration with the trustee.

Finally, Herzig *et al.* [33] formalized the model of Castefranchi and Falcone, in multi-modal logic, adding the notions of occurring trust and dispositional trust (i.e., trust in a general disposition of the trustee to perform a similar task some point in the future). Skopik *et al.* [6] purposed a semi-distributed information sharing platform where different organizations can share the incidents information with their trusted peers. Skopik *et al.*, proposed a fuzzy method to evaluate trust among members. The major aim of social trust in their model is to personalize online interactions and prioritize collaboration with trustworthy individuals. The author claimed that trusted relations can be defined manually by users, e.g., by declaring "friend-relations" or can be determined automatically through mining of interactions. However, their social model is based on personal experience of each member and suffers from the scalability issue.

IX. Conclusion and Discussion

The development in cyber security paradigm results in existence of new incidents. Most of the domain owners are not able to defend against them without collaborating with other members of alliance. One of the main challenges for a business under attack is choosing appropriate partners from

the different service providers to support its demands.
The aim of this paper was to elucidate the concept of cyber defense alliances. The overall goal of this approach is to assist the organization in sharing their critical information on security incidents among trusted parties in a way that the efficiency enhances. To have a perception over attacks and new malwares in alliance members and detection of their vulnerabilities, information sharing plays a crucial role.
In this work we presented a social computational trust model (SCTM) to help the alliances' members to evaluate the trustworthiness of a given trustee and make corresponding decisions. The proposed model considers two components called competence and benevolence; this computational model helps different members to evaluate trust more accurately.
The trustworthiness in this framework is estimated in terms of context-specific, benevolence and competence of domains in performing tasks. These entities are implemented to model interaction risk to give an estimation of risk level involved in an interaction. Such estimate helps a member to make decisions for choosing a partner for a given context of the interaction. The ABM case study is presented to evaluate the applicability of the framework. We aim at using the risk estimation framework to support the partner selection in multi-domain collaboration scenarios in cyber security alliances.

References

[1] T. A. Cellucci, M. C. C. Officer, Innovative public private partnerships.

[2] RSA, Current state of cybercrime.
URL https://www.rsa.com/content/dam/en/white-paper/2018-current-state-of-cybercrime.pdf

[3] R. Koning, A. Deljoo, S. Trajanovski, B. de Graaff, P. Grosso, L. Gommans, T. van Engers, F. Fransen, R. Meijer, R. Wilson, et al., Enabling e-science applications with dynamic optical networks: Secure autonomous response networks, in: Optical Fiber Communications Conference and Exhibition (OFC), 2017, IEEE, 2017, pp. 1–3.

[4] R. Koning, B. de Graaff, G. Polevoy, R. Meijer, C. de Laat, P. Grosso, Measuring the efficiency of sdn mitigations against attacks on computer infrastructures, Future Generation Computer Systems.

[5] A. Deljoo, T. van Engers, R. Koning, L. Gommans, C. de Laat, Towards trustworthy information sharing by creating cyber security alliances, in: IEEE TrustCom-18, IEEE, 2018, pp. 1506–1510.

[6] F. Skopik, D. Schall, S. Dustdar, Modeling and mining of dynamic trust in complex service-oriented systems, in: Socially Enhanced Services Computing, Springer, 2011, pp. 29–75.

[7] R. C. Mayer, J. H. Davis, F. D. Schoorman, An integrative model of organizational trust, Academy of management review 20 (3) (1995) 709–734.

[8] R. Bachmann, Trust, power and control in trans-organizational relations, Organization studies 22 (2) (2001) 337–365.

[9] N. Luhmann, Trust: And, Power : Two Works, John Wiley & Sons, 1979.

[10] D. Gambetta, Trust: Making and breaking cooperative relations.

[11] C. Tomkins, Interdependencies, trust and information in relationships, alliances and networks, Accounting, organizations and society 26 (2) (2001) 161–191.

[12] P. S. Ring, A. H. Van de Ven, Structuring cooperative relationships between organizations, Strategic management journal 13 (7) (1992) 483–498.

[13] J. B. Barney, M. H. Hansen, Trustworthiness as a source of competitive advantage, Strategic management journal 15 (S1) (1994) 175–190.

[14] R. Krishnan, X. Martin, N. G. Noorderhaven, When does trust matter to alliance performance?, Academy of Management journal 49 (5) (2006) 894–917.

[15] C. Castelfranchi, R. Falcone, Trust theory: A socio-cognitive and computational model, Vol. 18, John Wiley & Sons, 2010.

[16] M. Sako, Price, quality and trust: Inter-firm relations in Britain and Japan, no. 18, Cambridge University Press, 1992.

[17] T. K. Das, B.-S. Teng, Trust, control, and risk in strategic alliances: An integrated framework, Organization studies 22 (2) (2001) 251–283.

[18] A. Deljoo, L. Gommans, C. de Laat, T. van Engers, The service provider group framework., in: Looking Beyond the Internet: Workshop on Software-defined Infrastructure and Software-defined Exchanges,2016, Flux Research Group, University of Utah, 2016.

[19] A. Deljoo, T. van Engers, L. Gommans, C. de Laat, The impact of competence and benevolence in a computational model of trust, in: IFIP International Conference on Trust Management, Springer, 2018, pp. 45–57.

[20] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, P. Steggles, Towards a better understanding of context and context-awareness, in: International Symposium on Handheld and Ubiquitous Computing, Springer, 1999, pp. 304–307.

[21] J. Urbano, A. P. Rocha, E. Oliveira, The impact of benevolence in computational trust, in: Agreement Technologies, Springer, 2013, pp. 210–224.

[22] D. Z. Levin, R. Cross, L. C. Abrams, E. L. Lesser, Trust and knowledge sharing: A critical combination, IBM Institute for Knowledge-Based Organizations 19.

[23] T. R. Koscik, D. Tranel, The human amygdala is necessary for developing and expressing normal interpersonal trust, Neuropsychologia 49 (4) (2011) 602–611.

[24] T. Das, B.-S. Teng, Risk types and inter-firm alliance structures, Journal of management studies 33 (6) (1996) 827–843.

[25] P. M. Fandt, G. R. Ferris, The management of information and impressions: When employees behave opportunistically, Organizational Behavior and Human Decision Processes 45 (1) (1990) 140–158.

[26] A. Zaheer, B. McEvily, V. Perrone, Does trust matter? exploring the effects of interorganizational and interpersonal trust on performance, Organization science 9 (2) (1998) 141–159.

[27] S. P. Marsh, Formalising trust as a computational concept.

[28] L. Braubach, W. Lamersdorf, A. Pokahr, Jadex: Implementing a bdi-infrastructure for jade agents.

[29] N. Ghosh, S. K. Ghosh, S. K. Das, Selcsp: A framework to facilitate selection of cloud service providers, IEEE transactions on cloud computing 3 (1) (2015) 66–79.

[30] S. Adali, W. Wallace, Y. Qian, P. Vijayakumar, M. Singh, A unified framework for trust in composite networks, Proc. 14th AAMAS W. Trust in Agent Societies, Taipei (2011) 1–12.

[31] K. Kelton, K. R. Fleischmann, W. A. Wallace, Trust in digital information, Journal of the American Society for Information Science and Technology 59 (3) (2008) 363–374.

[32] I. Pinyol, J. Sabater-Mir, Computational trust and reputation models for open multi-agent systems: a review, Artificial Intelligence Review 40 (1) (2013) 1–25.

[33] A. Herzig, E. Lorini, J. F. Hübner, L. Vercouter, A logic of trust and reputation, Logic Journal of IGPL 18 (1) (2009) 214–244.