# Shall We Collaborate? A Model to Analyse the Benefits of Information Sharing

Roberto Garrido-Pelaz
Computer Security Lab
Carlos III University of Madrid
Madrid, Spain
rgarrido@pa.uc3m.es

Lorena González-Manzano
Computer Security Lab
Carlos III University of Madrid
Madrid, Spain
lgmanzan@inf.uc3m.es

Sergio Pastrana
Computer Security Lab
Carlos III University of Madrid
Madrid, Spain
spastran@inf.uc3m.es

## ABSTRACT

Nowadays, both the amount of cyberattacks and their sophistication have considerably increased, and their prevention concerns many organizations. Cooperation by means of information sharing is a promising strategy to address this problem, but unfortunately it poses many challenges. Indeed, looking for a win-win environment is not straightforward and organizations are not properly motivated to share information. This work presents a model to analyse the benefits and drawbacks of information sharing among organizations that present a certain level of dependency. The proposed model applies functional dependency network analysis to emulate attacks propagation and game theory for information sharing management. We present a simulation framework implementing the model that allows for testing different sharing strategies under several network and attack settings. Experiments using simulated environments show how the proposed model provides insights on which conditions and scenarios are beneficial for information sharing.

## CCS Concepts

•**Networks** → *Network reliability;* •**Security and privacy** → *Trust frameworks;* •**Computer systems organization** → *Availability;*

## Keywords

Cybersecurity; Information sharing; Game theory

## 1. INTRODUCTION

In the last decade, cyber attacks have considerably increased and nowadays cyber-crime is considered a stable and growing industry [17, 15, 28]. Cybersecurity prevention, detection and response is an ongoing challenge that needs constant and new efforts to protect critical infrastructures, organizations, enterprises and individual welfare. After an intrusion or attack has succeeded, it is important to perform an incident investigation to determine causes and consequences, and to update the security measures that failed (e.g. updating blacklists). Information gathered in this process is a valuable asset, but unfortunately it is usually kept secret in the inner boundaries of the companies, organizations or even national governments.

Cooperation between different parties has emerged as an essential strategy to improve cybersecurity prevention. National and international efforts encourage the application of cooperation-based solutions to address cybersecurity problems. For example, the US National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 [31] was launched in 2008 to get effective cybersecurity environments. European Parliament has also agreed a Network and Information Security (NIS) Directive [8] that will enter into force in August 2016. The benefits of cooperation are even higher in case of critical infrastructures, which highly rely on Information and Communication Technologies (ICT) that also share services among them. The development of reliable and resilience infrastructures should be viewed as an overall strategy rather than a single, independent task. Sharing information related to cybersecurity can be helpful in this regard.

However, there are many challenges and drawbacks that discourage organizations from sharing information [24]. First, it is critical to look for a win-win environment in which all entities are benefited and where free-riders (i.e. those entities that benefit from others but do not cooperate) are avoided. Second, the reputation of targeted entities is an asset to protect, and one of the main drawbacks of sharing information is precisely the loss of privacy. Third, it is important to take into account some form of trust management, where companies can trust each other to share incentives [7].

Information sharing facilitates a common understanding of threats and thus, it benefits organizations in aspects like quality of risk management, incident response or recovery management. However, despite the clear benefits, neither private nor public organizations are prone to collaborate unless there are tangible incentives that motivate them to do it. Recent works have identified information sharing as a cost-benefit Prisoner's dilemma solved using game theory [29, 7]. However, these proposals focus on the mathematical analysis of games between two players, without taking into account the overall network of entities and their functional dependencies. Moreover, these works do not consider how

*WISCS'16, October 24 2016, Vienna, Austria*
© 2016 ACM. ISBN 978-1-4503-4565-1/16/10. . . $15.00
DOI: http://dx.doi.org/10.1145/2994539.2994543

cyberattacks affect other entities in the network due to their propagation and service dependencies.

In this work, we present a model for cybersecurity information sharing among dependent organizations being impacted by different cyberattacks. The model allows simulating real networks and different adversarial capabilities by establishing different attack patterns, assets and dependencies between partners. It applies a propagation algorithm to infer how the entire network is affected by independent cyberattacks, and it also simulates different sharing strategies. The output of the model refers to analytical results that may help security staff to determine under which circumstances it is interesting to share or not. The proposed model does not aim at providing the ground truth about sharing or not, but it helps organizations and governments to take this decision by simulation. In this work we present the following contributions:

1. We describe a model that considers the propagation of the impact of cyberattacks on a network and that applies different strategies for information sharing to mitigate such impact. The model applies Functional Dependency Network Analysis (FDNA) for attacks propagation and game theory for information sharing management.

2. We have developed a publicly available simulation framework that implements the model. This framework allow simulating and studying test cases by analysing results from both network point of view and particular nodes.

3. Using the simulation framework, we have applied the model in different scenarios having different adversarial settings. Our experimental work shows how the model can provide knowledge about which sharing strategies are better under different network conditions and attack patterns.

The rest of the paper is organized as follows. Section 2 reviews the literature. Section 3 presents some background on functional dependency network analysis and game theory. Then the model overview and description are presented in Section 4, and Section 5 details the implemented framework. Finally, Section 6 presents conclusions and future work.

## 2. RELATED WORK

Several works have proposed the use of game theory to analyse the trade-off in terms of incentives and costs of sharing information among entities. Naghizadeh et Liu [22] propose folk theorems and use an analytical method to study how the role of private and public monitoring through intertemporal incentives can support degree of cooperation. Similar to this work, we also propose a game theory based model where utilities of sharing information are calculated upon gains and costs. However, instead of using historical public available actions, we propose immunization factor and reputation as the main variables for incentiving sharing. Furthermore, the work in [22] identifies the cost of disclosure as one of the main drawbacks related to information sharing. While we also consider privacy and disclosure costs as two key drawbacks for sharing, we also introduce a third variable that affects costs, i.e. trust.

Tosh et al. [29] use game theory to help organizations to decide whether to share information or not, using the CYBEX framework [25]. Authors use evolutionary game theory in order to attain an evolutionary stable strategy (ESS) under various conditions. These conditions are extracted through simulation with synthetic data in a non-cooperative scenario with rational and profit-seeking firms. The main incentive for sharing is the information received, and thus the knowledge gained. In our work we also consider this knowledge as an incentive for sharing.

Khouzani et al. [18] present a two stage Bayesian game between two firms to help to decide how much to invest in searching vulnerabilities and how much of this information to share. Authors determine the Perfect Bayesian Equilibrium to extract analytically strategy conditions encouraging information sharing. In [18] a firm benefits from losses in another, namely due to exploited bugs. Moreover, they distinguished costs between: direct loss (of compromised firm), common loss by market shrinkage and competitive loss.

A. K. Eric Luiijf. [7] has analysed the problem of free-riders, i.e. those entities that benefit from the shared information but do not cooperate. To minimize free-riding they propose two approaches: a) provide a quantitative analysis and show the benefits of reciprocity to incentive sharing; b) enforce sharing environments by means of regulations, similar to other works [19]. In our work, we consider that sharing information may not be always effective, and thus we adopt the first approach, i.e. to study cases in which information sharing benefits the overall network and where it only benefits some of the partners.

One of the main problems when analysing the costs and benefits of information sharing is the experimentation with real data. Whereas most of the proposed works [22][19][29] perform evaluation using analytical methods, Freudiger et al. [9] present a controlled data sharing approach and make empirical evaluation using a dataset of suspicious IP addresses. Authors in [9] use different similarity metrics to analyse benefits of sharing and compare different sharing strategies: sharing everything or just information about attack entities. They rely on a static scenario and provide useful metrics to mathematically predict benefits of info sharing. By contrast, using a simulated setting we empirically analyse how impacts are propagated through the network, at runtime, to afterwards analyse how information sharing is able to mitigate such impacts in the future.

## 3. BACKGROUND

This section describes Functional Dependency Network Analysis (FDNA) and game theory, as they are two core disciplines applied in the proposed model.

### 3.1 Functional Dependency Network Analysis

Functional Dependency Network Analysis (FDNA) was proposed first by Garvey et al. [11]. They proposed a methodology to assess the impacts derived from loss of supply in one provider to function operability of dependent services. Authors propose two metrics to quantify the dependencies between nodes: the Strength of Dependency and the Criticality of Dependency. Using these metrics, several works have analysed vulnerabilities, impacts and risks in system-of-systems scenarios [23, 5, 13].

Few works analyse the benefits of information sharing including dependences among players, as well as the propagation of impacts of cyberattacks. Laube et al. [19] refer to dependencies and impact of cyberattacks through direct costs (security breaches happened). By contrast, Hernandez et al. [14] use relationships among nodes inside a sharing community, focusing on knowledge flows and how they increase information value of nodes. We consider that dependencies between partners or entities are a key concept in order to decide whether to share information or not, and thus the proposed model uses functional dependencies. The main goal is to analyse the impact of cyberattacks through provided services in a hypothetical network and how information sharing can contribute to threat mitigation over time.

## 3.2 Game theory background

Game theory relies on four elements to define a game: players, rules or possible actions, information structure and game objective. In a sharing game, rules or actions are identified with two pure strategies, i.e. *share* or *not share*. Games are usually represented in normal form as a pay-off matrix. Pay-offs are numbers representing the outcome, through a measure of quantity or utility that a player gets as a result of playing specific actions [26]. Pay-offs are the mechanism to reflect the motivations to select pure strategies. Values in a pay-off matrix can be given by constant values or by formulas and they are closely related to the goal of the game, thus maximizing or minimizing gained pay-offs.

There are several approaches that develop a game-theory based solution. They go from classical game theory, focused on the analysis of equilibrium among players pay-offs; to evolutionary game theory, focused on the dynamics of strategy changes (in populations). New game-theory approaches are learning game theory [16], where players learn over time based on past decisions of other players, and behavioural game theory [4], based on psychological elements to describe human behaviour.

Regarding the classification of games, information sharing decisions fit well with the prisoner's dilemma [7], where cooperative behaviours are not very clear since players have to find a trade-off between benefits and costs of their actions. Moreover, games can be of perfect/imperfect and complete/incomplete information. Perfect information refers to the fact that each player, when making any decision, is informed of all the events that have previously occurred. Complete information refers to the fact that each player has knowledge about the pay-offs and strategies available to the remaining players.

# 4. THE MODEL

This section presents the proposed model. Section 4.1 presents an overview. Section 4.2 describes the model. Sections 4.3, 4.4 and 4.5 present respectively how cyberattacks propagation is performed, information is shared and decision variables are updated.

## 4.1 Model overview

Organizations and their assets are represented as a network composed of elements called *nodes*. Information/assets owned by nodes have a value. This value represents the information loss (e.g. economical, reputation, resources, etc.) due to the impact of a cyberattack. Accordingly, we consider this value as a combination of the Confidentiality, Integrity and Availability principles (CIA) since these properties are at the core of information security.

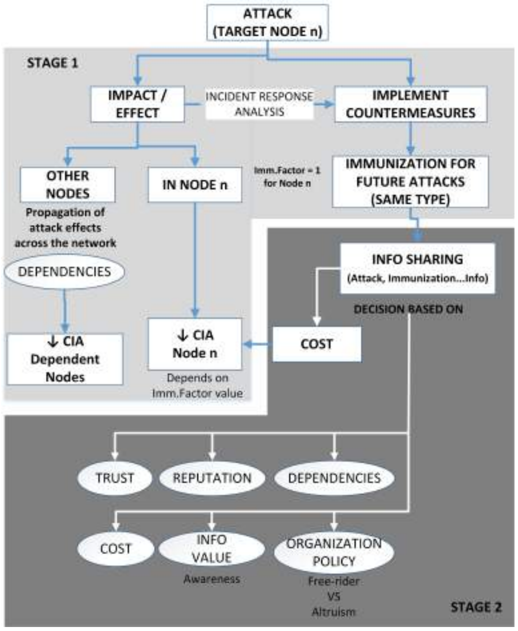
ATTACK (TARGET NODE n)
STAGE 1
IMPACT / EFFECT
INCIDENT RESPONSE ANALYSIS
IMPLEMENT COUNTERMEASURES
OTHER NODES
Propagation of attack effects across the network
IN NODE n
Imm.Factor = 1 for Node n
IMMUNIZATION FOR FUTURE ATTACKS (SAME TYPE)
DEPENDENCIES
INFO SHARING (Attack, Immunization....Info)
DECISION BASED ON
↓ CIA Dependent Nodes
↓ CIA Node n
Depends on Imm.Factor value
COST
TRUST
REPUTATION
DEPENDENCIES
COST
INFO VALUE
Awareness
ORGANIZATION POLICY
Free-rider VS Altruism
STAGE 2

**Figure 1: Model overview.**

The model considers different periods of time (*epochs*) concerning the emergence of a cyberattack. Fig. 1 presents an overview of the model in which a pair of stages are distinguished: 1) *propagation* of the attack, and 2) information sharing. Stage 1 shows that, when a node is targeted by an attack, its CIA value decreases proportionally to the impact of the cyberattack. As a consequence of an attack, dependent nodes on the targeted node are also affected according to service levels agreed among nodes. This process is what we call *propagation of cyberattacks*.

Upon receiving an attack, the targeted node is able to develop countermeasures (e.g. due to an incident investigation), thus being *immunized* for future attacks. Afterwards, attacked nodes must decide whether to share the information about attacks (and the associated countermeasures) with other nodes.

Information sharing steps are represented in the Stage 2 of Fig. 1. The sharing decision is based on several variables and environmental conditions. On the one hand, if one node decides to share information, it will incur a cost which is related to the risk of unwanted disclosure of shared information and privacy loss. This cost directly affects CIA value of the node with which information is shared. On the other hand, sharing may provide two main benefits: (1) to raise cybersecurity awareness level through immunization factor, (2) to improve enterprise reputation. In general, sharing decisions consist of several criteria and many related variables: with whom to share, cost of sharing, dependencies, trust and reputation among nodes, organization policy, information properties, level of resilience and knowledge acquired in sharing processes, among others. The problem is formulated as a trade-off between costs and benefits of sharing information. Presented in Section 5, simulations with this model can be used to analyse the scenarios where different sharing strategies are better, regarding different conditions and variables like the presence of free-riders.

## 4.2 Model description

Let $\Omega = (A, V, C, Y, I, S, T, R, W)$ be the set of variables representing the state of the model at each epoch. Sharing decisions and results obtained at each epoch are based on the values of variables in $\Omega$. In the following we describe these variables.

**Services and dependencies of the network ($A$)**

The model considers a network composed by nodes representing some ICT infrastructure. Each node encapsulates a relevant element or service where the state depends on information transmitted through links and operability of connected nodes, that is, functional dependencies. The network can be viewed as a labelled graph, represented as an adjacency matrix $A$ of size $n \times n$, being $n$ the number of nodes. An element $a_{i,j}$ in matrix $A$ represents the level of service that node $i$ offers to node $j$, or the degree of dependency of node $j$ on node $i$. Values of elements range from 0 to 1, where 0 means no service/dependency and 1 means total dependency for one node to other.

**CIA value of the nodes ($V$)**

Each node has a CIA value based on the three traditional information security properties: confidentiality (C), integrity (I) and availability (A). $V$ is a vector of size $n$ where each element $v_i$ is the value of the node $i$ inside the network. The values range from 0 to 1, where 0 means that the node has no value (i.e. useless asset) and 1 means that the node is an important asset for an entity. While this is an interesting and complex area on risk analysis and asset management, establishing asset values is out of the scope of this work.

**Costs of information sharing ($C$)**

When an entity or organization shares information, it may incur a cost. Costs of sharing are described by a vector $C$ of size $n$, where each element $c_i$ is the cost of sharing for node $i$. Similarly to giving values to assets, quantifying costs is not straightforward and it depends on the scenario of application. The cost of information sharing has a direct effect on the CIA value of nodes (e.g. due to loss of confidentiality or privacy). To simplify the model, in our current prototype these costs are calculated using a parameter $k \in [0, 1]$ that represents the percentage of loss in the CIA value of the node due to sharing information. The cost of sharing is directly proportional to the CIA value of the nodes. Summarizing, values in the vector $C$ are calculated as $c_i = k \cdot v_i$, where $v_i$ is the CIA value of node $i$ and $c_i$ its cost of sharing.

**Set of possible cyberattacks ($Y$)**

A cyberattack is any attempt to compromise the confidentiality, integrity or availability of an asset (node) in an organization. The caused damage can be viewed as an economic impact, but in our case, the impact decreases CIA value of the targeted node. Each cyberattack has specific properties and the organization should implement the correct countermeasures to solve problems as soon as possible. The set of cyberattacks is described by a vector $Y$ of size $n$, where each element $Y_i$ is the cyberattack received by node $i$ in a given epoch. The model manages $m$ possible cyberattaks[1], and it is assumed that cyberattacks have a default impact associated, that we note as $D$. The values of $m$ and $D$ can be modified during experimentation to simulate different attack scenarios.

The propagation of attacks causes two different damages. First, the targeted node suffers a *direct* impact which can be mitigated if the node was prepared for it (*immunized*). It depends on the immunization factor of this node for this attack, as it is explained below. Second, a *related* impact is applied on nodes that directly or indirectly depend on the targeted one. In this case, the CIA value is decreased according to the degree of dependency between the nodes and the *direct* impact of the targeted node.

**Immunization factors ($I$)**

The immunization factor indicates how well a node is prepared against a cyberattack, and thus, how it can mitigate its impact. It represents any mechanism or countermeasure such as knowledge about a particular attack (IDS rules, IoCs, blacklisting IPs, etc.), a piece of software (antivirus, SIEM), organization policies, etc. The immunization factor is specific for each attack and each node, and it is represented by a matrix $I$ of size $m \times n$, where $m$ is the number of available cyberattacks and $n$ is the number of nodes. An element $I_{p,i} \in [0, 1]$ represents the degree (factor) by which node $i$ is immunized for cyberattack $p$. Accordingly, a value $I_{p,i} = 0$ means that node $i$ is not immunized for cyberattack $p$, while a value $I_{p,i} = 1$ indicates that node $i$ is totally immunized for cyberattack $p$ and it will have no impact on CIA value of $i$.

An important point is the difference between the *direct* and *related* attack impact, as well as the relationship with their immunization factor. Once a node receives a cyberattack, it impacts the CIA value of the node, only mitigated according to the immunization factor of such node. However, if this node is not immunized against the attack, the corresponding impact will be propagated across the network based on dependences, no matter what the immunization of other nodes against this cyberattack is. As a result, sharing information becomes essential to avoid being affected by cyberattacks suffered by others.

**Sharing policy ($S$)**

Sharing policies determine with whom nodes want to share or not to share information. The decision bases on the properties of each node, network conditions and variables in $\Omega$. Each node chooses a fixed sharing policy along the whole game to select a pure strategy, namely, share or not share. These policies are described by $S$. $S$ is a vector where $S_i$ is the sharing policy of the node $i$. Examples of sharing policies are "*Share only with those on which I directly depend*" or "*Share with those nodes that provide more services*".

**Trust among nodes ($T$)**

In the cooperative cyber defense scenario, trust is a key aspect, since it is used to define collaborative security models [21]. Trust represents how nodes trust each other [10] and it is described by a matrix $T$ of size $n \times n$. An element $T_{i,j} \in [0, 1]$ is the trust value that node $i$ has on node $j$. $T_{i,j} = 0$ means node $i$ has no trust in node $j$ and $T_{i,j} = 1$ means node $i$ has full trust in node $j$. Trust between nodes increments or decrements the cost of sharing, i.e. sharing with those nodes that are more trustworthy is less costly.

**Reputation among nodes ($R$)**

Trust and reputation are related but different concepts [10]. Trust is the subjective probability that an agent will carry out a specific task as expected. By contrast, reputation represents the set of past opinions received by others users,

[1] We set a limited number of cyberattacks in our current prototype implementation, but these cyberattack may be viewed as a zero day if none of the nodes are immunized against them

that is, expectancy of behaviour based on past interactions [1]. Our approach represents reputation through a matrix $R$ of size $n \times n$ where an element $R_{i,j} \in [0,1]$ is the reputation value that node $i$ gets from node $j$. $R_{i,j} = 0$ means node $i$ receives no reputation from node $j$ and $R_{i,j} = 1$ means node $i$ receives full reputation from node $j$.

**Awareness ($W$)**

Awareness represents the degree of useful information received by a particular node, i.e. information which was unknown by the receiver and that increases the general awareness of the node at each epoch. We represent awareness through a matrix $W$ of size $n \times n$ where an element $W_{i,j} \in 0,1$ is the awareness that node $i$ gets from node $j$. $W_{i,j} = 0$ means node $i$ receives no valuable information from node $j$ and $R_{i,j} = 1$ means node $i$ receives valuable information from node $j$. As a first approach, we closely relate the awareness with immunization factors, since node $i$ gets $W_{i,j} = 1$ from node $j$ only if node $i$ gets new immunization factors for some cyberattack $p$ not yet immunized, thus $I_{p,i} = 1$ for cyberattack $p$ received by node $j$.

Alg. 1 shows the sequence of actions executed in the model. As input, it receives an initial state of the system represented by $\Omega$ as explained above, and as output, it provides a set of metrics and features regarding the final state and the sequence of actions from the simulation (e.g. which nodes have shared information, which nodes have been targets of cyberattacks, etc.). These metrics are used to perform an analysis both in the network and in particular nodes.

Note that in lines 3 and 4 of Alg. 1 we generate the attack vector $Y$, establishing nodes that are targeted at each epoch, the selected attacks and their impacts according to $D$.

**Algorithm 1** Cyber-attack Propagation and Information Sharing Simulation Model

```
 1: procedure CyberModel($\Omega = (A, V, C, Y, I, S, T, R, W)$)
 2:     for $t := 1 \rightarrow MAX\_EPOCH$ do
 3:         $Y \leftarrow$ Set Attack Vector
 4:         Calculate impact in nodes according to $Y$ and $D$
 5:         $I \leftarrow 1$ Set Immunization Factor = 1
 6:         Propagate impacts through the network
 7:         Set Sharing strategies
 8:         Play Sharing Game
 9:         Update CIA values according to sharing policies
10:         Update Reputation regarding sharing decisions
11:     end for
12: end procedure
```

## 4.3 Propagating cyber-attacks impacts

In the first step of the model, once a node is under attack, dependent nodes are somehow affected. The propagation of these impacts is the first process computed at each epoch (from line 4 in Alg. 1).

On one hand, the *direct* impact on targeted node decreases the value of this node according to Eq. 1,

$$\forall i \in V, V_i^t = V_i^{t-1} - \parallel V_i^{t-1} \cdot (D_{Y_i^t} \cdot (1 - I_{Y_i^t,i})) \parallel \qquad (1)$$

$Y_i^t$ is the cyberattack received by node $i$ at epoch $t$, and $D_{Y_i^t}$ is the default impact of such attack according to initialized values as described in previous section. $I_{Y_i^t,i}$ is the immunization factor of node $i$ for cyberattack $Y_i^t$. Note that if $I_{Y_i^t,i}$ is 0, then node $i$ is fully impacted by all $D_{Y_i^t}$, and if $I_{Y_i^t,i}$ is 1, then node $i$ is not impacted at all.

Without loss of generality, in the current implementation of the model nodes that are directly attacked get an immunization factor of 1 for that specific attack (thus $I_{Y_i^t,i} = 1$). This represents a total immunization for future attacks of the same type, due to a perfect incident response procedure (we discuss this assumption in Section 4.6).

On the other hand, the impact of each cyberattack, not the cyberattack itself, is propagated across the network (line 6 in Alg. 1). This way, the cyberattack reduces the operability of both the victim node and indirect nodes (i.e. those that depend on the victim node). Propagation of impact and their effects is based on dependencies or services levels as defined in 4.2. Direct dependent nodes are well represented in dependency network matrix $A$, while indirect dependent nodes are more difficult to get. To address this issue, we previously calculate indirect services matrix $B$, also using a Deep First Search algorithm on $A$. With this indirect service matrix we can calculate the impact of cyberattacks and the new CIA value for each node in the network, as showed in Eq. 2:

$$\forall j \in V, V_j^t = V_j^{t-1} - \parallel V_j^{t-1} \cdot (D_{Y_i^t} \cdot (1 - I_{Y_i^t,i})) \cdot (B_{i,j}) \parallel \qquad (2)$$

$i$ refers to the node directly attacked, and $j$ is the dependent impacted node. $B_{i,j}$ is the service weight that node $i$ offers direct or indirectly to node $j$. As aforementioned, immunization factor does not reduce the impact of the propagated effect of an attack, that is, if a node $j$ receives an impact derived from an attack on other node $i$, the effect on node $j$ only depends on the effect on node $i$ and the service weight defined in $B_{i,j}$.

## 4.4 Information sharing game

The second step of the model is to decide if nodes under attack share information or not. In this step, identified by lines 7 and 8 in Alg. 1, sharing strategies are established according to sharing policies and applied to calculate payoffs (benefits and costs) at each epoch.

### 4.4.1 Game definition

Players are the nodes of the network and the set of pure strategies is {Share,Not Share}. According to the number of players, our approach proposes a multiple two-players (pairs) game. Thus, we define an iterative 2-nodes multiple games, with $n \cdot (n-1)$ different games played with different results at each epoch. Moreover, the proposed game is dynamic due to the fact that participants play stages of the same game over time. We propose an instance of the Iterated Prisoner's Dilemma because decisions can vary over time and players have to decide their strategies without communicating them to others under free-riding conditions.

Non-cooperative and inefficient games can lead to efficient trade-off through repetition [22], but it is paramount to know if games are under perfect or imperfect information, and complete or incomplete information conditions, as well. Our approach follows an imperfect and complete information game, since every node knows about pay-offs configuration and strategies available to other players, but they do not know every action performed by the others.

Additionally, shown in Table 1, this is a non-zero sum game, while pay-off gained by one node is not exactly what the other losses. Furthermore, the game is asymmetric since two players can get different pay-offs even when applying the same strategy. This is because pay-offs depend on particular trust, information properties and the degree of dependency among nodes. Even though the prisoner's dilemma take symmetric configuration, it can take an asymmetric form [30]. Also it is noteworthy that some works [2] point out that asymmetry reduces cooperation rates in prisoner's dilemma games.

### 4.4.2 Sharing strategy

Selecting the sharing strategy for each node is one of the most important decisions to take in cooperative scenarios. We distinguish between sharing strategy and sharing policy. Sharing strategies refer to share or not to share, that is the pure strategies. By contrast, sharing policies correspond to *"strategies"* that players use to decide what pure strategy to play. Sharing policies can be supported from basic to very complex decision processes. Classical and most common sharing policies applied to Iterative Prisoner's dilemma for behavioural analysis of players are [20]: AIIC (Always Cooperate); AIID (Defects on every move); RAND (Random player); TIT (Tit for Tat), that is, cooperate on the first move, then copies the opponent's last move; and Grim (Grim Trigger), cooperates, until the opponent defects, thereafter always defect. Sharing policies are particular for each scenario, as pointed out in Section 5.

### 4.4.3 Calculating pay-offs

Pay-off functions depend on reputation, awareness, trust and cost of sharing sensible information with others. Pay-off matrix is shown in Table 1, where $U_A$ and $U_B$ are respectively the pay-offs (utilities) of $A$ and $B$ obtained for each of four possible combination of players' actions. There are two factors in each equation mainly, values allocating benefits and values allocating costs according to the chosen strategy. In general terms, it indicates what players win and what players loss. In terms of notation, $R_{a \leftarrow B}$ is the reputation that node $A$ receives from $B$, $T_{A \rightarrow B}$ represents trust of node $A$ in node $B$ and $C_A$ is the cost of sharing for node $A$. These values are extracted from variables defined in Section 4.2.

$W_{A \leftarrow B}$ represents the awareness degree gained by node $A$ from node $B$. It is calculated as $W_{A \leftarrow B} = 1 \leftrightarrow$ ($B$ shares with $A$) $\wedge$ ($B$ is under attack) $\wedge$ ($A$ is not immunized for the attack received by $B$). That is, node $A$ gets immunized to a given attack due to information received from node $B$.

Also note how trust directly affects the cost of sharing. $\frac{C_A}{T_{A \rightarrow B}}$ means that the higher the trust from $A$ to $B$, the lower the cost of sharing from $B$ to $A$ and vice versa.

## 4.5 Updating decision variables

Once attacks have been propagated and the information has been (or not) shared, the final step is to update CIA value and reputation of all nodes.

In addition to the decrease of CIA value due to attack impacts, sharing information affects the CIA value as well, that is, the cost of information sharing as shown in Eq. 3. This reduction due to information sharing is only applied when a node has been targeted by a cyberattack, it is not previously immunized, it has shared information with any other node and the mean pay-off obtained by sharing information is less than 0.

$$\forall i \epsilon V, V_i^t = V_i^{t-1} - C_i \tag{3}$$

Reputation per node is also updated at each epoch. As Alg. 2 shows, the process for updating reputation depends on previous reputation scores, sharing actions, obtained awareness and whether nodes are under attack or not. In order to prevent free-riding behaviours, we identify three cases, formalized in lines 4 to 11 in Alg. 2: (1) if node $j$ increase its awareness by information shared by node $i$, that is, $j$ gets immunized by node $i$, then node $j$ rewards node $i$ reputation score by a constant $K_{reward}$; (2) if node $j$ does not increase its own awareness by node $i$ but the latter is determined to share, then it is difficult to know if the node $i$ is a free-rider or the information provided is not useful. In this case, we propose to do not modify previous reputation value; (3) if node $j$ does not increase its own awareness by node $i$ and the latter is not determined to share (free-riding behaviour), then reputation score of node $i$ decreases by punishing with $K_{punish}$.

**Algorithm 2** Updating reputation scores procedure

```
 1: for $n := 1 \rightarrow n$ do
 2:     for $j := 1 \rightarrow n$ do
 3:         if $j \neq n$ then
 4:             if $(Awareness(j, n) > 0)$ then
 5: $R^t_{n \leftarrow j} = R^{t-1}_{n \leftarrow j} + (K_{reward} \cdot R^{t-1}_{n \leftarrow j})$
 6:             else
 7:                 if SharingStrategy(n,j)=Share then
 8: $R^t_{n \leftarrow j} = R^{t-1}_{n \leftarrow j}$
 9:                 else
10: $R^t_{n \leftarrow j} = R^{t-1}_{n \leftarrow j} - (K_{punish} \cdot R^{t-1}_{n \leftarrow j})$
11:                 end if
12:             end if
13:         end if
14:     end for
15: end for
```

## 4.6 Assumptions

Due to limitations on simulation, during the definition of our model, we have made some assumptions that may be subject of discussion in real settings. First, value of nodes always decrease over time due to the impact of cyberattacks and the costs of information sharing. However, we do not consider mechanisms that may increase this value, such as contingency plans or asset restoration. Secondly, when a node has been targeted by an attack, we assume that it performs a proper incident response investigation and thus it implements countermeasures, gaining an immunization factor of 1. In this way, from that moment on, the node will be immunized to such cyberattack.

# 5. EXPERIMENTATION

This section presents a simulation framework based on the model described in Section 4. A few case studies are analysed using this prototype. First, goals and general conditions of the simulation framework are introduced in Section 5.1. Second, Section 5.2 presents the analysed scenarios and specific settings. In Section 5.3 used metrics and the results

**Table 1: Pay-off matrix for information sharing game**

|  |  | B |  |
|---|---|---|---|
|  |  | Share | Not Share |
| A | Share | $U_A : (R_{A\leftarrow B} + W_{A\leftarrow B}) - (\frac{C_A}{T_{A\rightarrow B}})$<br>$U_B : (R_{B\leftarrow A} + W_{B\leftarrow A}) - (\frac{C_B}{T_{B\rightarrow A}})$ | $U_A : R_{A\leftarrow B} - (\frac{C_A}{T_{A\rightarrow B}})$<br>$U_B : (C_B + W_{B\leftarrow A}) - R_{B\leftarrow A}$ |
|  | Not Share | $U_A : (C_A + W_{A\leftarrow B}) - R_{A\leftarrow B},$<br>$U_B : R_{B\leftarrow A} - (\frac{C_B}{T_{B\rightarrow A}})$ | $U_A : C_A - (R_{A\leftarrow B} + W_{A\leftarrow B}),$<br>$U_B : C_B - (R_{B\leftarrow A} + W_{B\leftarrow A})$ |

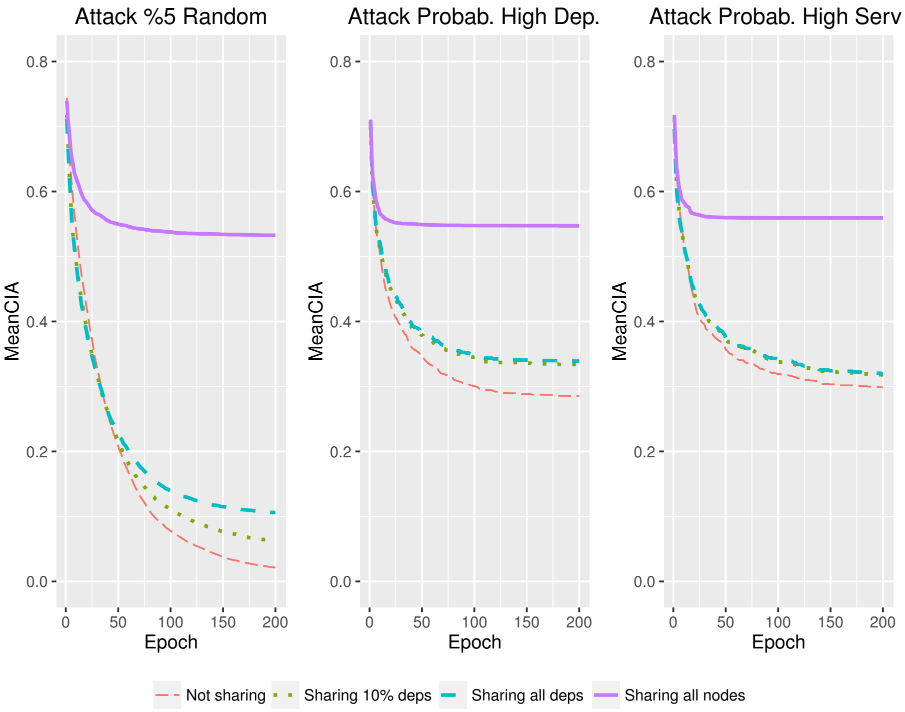

**Figure 2: Evolution of mean CIA value of nodes for each attack and sharing scenario**

of the analysis for both general welfare and specific nodes viewpoints, are described.

## 5.1 Simulation framework

Empirical evaluation in real large-scale cybersecurity information sharing environments is hard to carry out. This is due to the highly diverse and dynamic conditions of the existing scenarios [27]. Thus, we have implemented a simulation framework using GNU Octave [6] based on the proposed model. This framework allows simulating specific cyberattacks and information sharing scenarios, as well as the study of the behaviour and evolution of nodes (assets) over time. The main goal is to show how the model can help in decision-making problems by analysing test cases.

We aim to build a flexible framework with configurable settings, namely network size and topology, attack scenarios, sharing policies and initial trust, reputation and CIA.

To foster research on information sharing, an open-source version of the prototype[2] is provided in GitHub.

## 5.2 Experimental set-up

We carry out a series of experiments to analyse specific network topology behaviours over time based on Monte Carlo simulations method. We aim to compare network and nodes evolution according to different sharing policies in three different adversarial models. Hereafter we describe our experimental set-up. It is important to note that the main goal of our experimental work is to show up the benefits of using the proposed model and how it can be used in different case studies. Established settings may not represent real scenarios, but they aim to simulate general idiosyncrasies of current networks.

**Network sampling.** We set a random scale-free directed network composed by 50 nodes. We consider that 50 nodes represent a medium-sized sharing community. Also, we choose a scale-free network since it has a similar topology than the Internet [3]. Note that in scale-free networks some nodes are highly connected, while most of the nodes have low connectivity. In the proposed network one node has an input degree of 14, and most of them have 2 or 3. Output degrees have similar properties. Regarding weight

[2] https://github.com/rguseg/infosh-framework

of dependencies, we simulate a network where dependencies values are fixed to 0.5 among every connected node, so each node is equally dependent of its neighbours. For simplicity, we set this fixed value for all the dependencies to represent a midpoint level of dependency between nodes, since we do not aim to simulate total dependency scenarios. However, in real settings, these values should be properly chosen based on how much each node or service depends on its neighbours.

**Attack scenario**. It represents the degree of threat to which a sharing community is exposed, and it is determined by the different cyberattacks, their impact, their frequency and which nodes are targeted. We randomly choose attacks from a predefined catalogue with an associated impact.

In particular, we assume the existence of a catalogue composed of 10 attacks ($m = 10$) to give the simulation enough variability according to networks size (50 nodes) and give nodes the opportunity to get immunized due to information sharing. While we do not aim to simulate cyberattacks with very high impact, the impact of each cyberattack follows a normal distribution with mean 0.4 and standard deviation 0.2. It means that cyberattacks incur an impact rated between 0.2 and 0.6 on the targeted node.

At each epoch, 30% of the attacks from the catalogue are randomly selected. Then, a subset (vector) of nodes $Y$ become the targets. Selection of targeted nodes depends on many specific conditions, and it may be variable in real settings (e.g. the knowledge of the adversary about the network topology or the available vulnerabilities to exploit). In the experimentation we use the following criteria:

- Random selection. We randomly select 5% of nodes of the network to be attacked. We conduct experiments using such a low rate of attacked nodes given that information sharing is more useful in scenarios with lower attack rates than scenarios where the network is highly targeted.

- Attack to those with higher dependencies. We first calculate the number of inputs degrees for each node and sort them in descendent order. For each node, we estimate the probability of being attacked as $p = \frac{Degree_{Input}}{n}$, where $n$ is the number of nodes in the network. Consequently, the higher the weight of inputs (dependencies), the higher the likelihood of being targeted.

- Attack to those providing highest number of services. It applies the same procedure as for dependencies, but taking nodes outputs degrees instead of inputs ones. The probability of being attacked is estimated as $p = \frac{Degree_{Output}}{n}$.

When the degree of a node is 0, it means that it has no dependencies or services to offer. Still yet, they may be target of cyberattacks, so in these cases we set a default (minimum) probability of being targeted equal to 2 % ($p = 0.02$).

**Sharing policies**. We set-up four available sharing policies in each simulation as presented in Section 4.4. Since our goal is to show how the model helps in deciding which sharing strategies are better (independently of local policies), in our experimental work sharing policies are static and global, i.e. they do not change over time and they are the same for all the nodes. These strategies are: a) no-one shares; b) nodes share with 10% of nodes who they most depends on (weight of dependencies); c) nodes share with all the nodes they depends on (100%); d) nodes share with all nodes in the network (broadcast).

**Initialization of values**. Our experiments consider that the assets protected in the network have a rather high value for the organizations. Thus, CIA value of nodes is set to 0.8 in a range [0,1]. Given the difficulties of establishing trust values [12], initial trust values are set to 0.5, being in the range [0,1]. This decision represents a neutral position which remains static over time.

**Other Parameters**. For each particular scenario, we run 30 simulations of 200 epochs. Without loss of generality, the percentage of loss in CIA value $k$ of each node due to information sharing (i.e. the cost) is set to 0.2 and the level of punishment ($K_{punish}$) and reward ($K_{reward}$) are set to 0.3 respectively.

## 5.3 Results

We focus the analysis on two areas: 1) the evolution of the general welfare of the network during time, due to the application of different sharing policies; and 2) the analysis and identification of particular nodes that have different benefits under similar conditions, so as to extract useful information from them. To this end, we define three metrics, named **MeanCIA**, **Gain** and **Information Quality**.

Definition 1. *$\bar{V^t}$ is the **MeanCIA** metric that represents the general welfare of the network at epoch t. It is calculated as the average value of CIA of all nodes and all simulations.*

The **MeanCIA** is calculated according to Eq. 4.

$$\bar{V^t} = \frac{1}{sims} \cdot \sum_{s=1}^{sims} (\frac{1}{n} \cdot \sum_{i=1}^{n} V_i^{s,t}) \tag{4}$$

where $t$ is the epoch which we want to process, $sims$ is the number of simulation runs, $n$ is the number of network nodes, then $V_i^{s,t}$ is the CIA value of node $i$ in simulation $s$ and epoch $t$.

Definition 2. *$G_i^t$ is the **Gain** metric that indicates the degree of CIA value gained or lost by each node because of information sharing. It is calculated as the difference in the CIA values of each node after applying two policies (sharing with all the nodes and not sharing) in two similar scenarios with the same conditions.*

The **Gain** is calculated according to Eq. 5.

$$G_i^t = V_i^{sh2,t} - V_i^{sh1,t} \tag{5}$$

where $t$ is the epoch which we want to process, $i$ is the node, $V_i^{sh1}$ is the CIA value of node $i$ while applying the sharing policy $sh1$ (not sharing), and $V_i^{sh2}$ is the CIA value of node $i$ while applying the sharing policy $sh2$ (sharing with all the nodes).

Definition 3. *$Q$ is the **Information Quality** metric that represents the amount of information that is useful to increase the awareness of the nodes. Concretely, $Q_i^{in}$ is the amount of quality information sent and $Q_i^{out}$ is the amount of quality of information received by node $i$ .*

Based on these metrics, we next present the results obtained and the analysis performed on the three attack scenarios and applying the different sharing policies.

### *5.3.1 Analysis of the general welfare of the network*

In this section, we provide an analysis of welfare evolution over time for the four sharing policies applied in each of the three attack scenarios as described in Section 5.2, thus a total of 12 different scenarios.

Fig. 2 shows time evolution of **MeanCIA** during 200 epochs for the four sharing policies. It can be observed that at the beginning of the simulation, all sharing policies have rather similar **MeanCIA**, but it decreases faster when applying policies that do not share or perform selective sharing. Besides, applying sharing policies based on dependences does not produce too much benefits. Concretely, sharing with 10% of dependent nodes improves not sharing policies in a ratio of 5%, 6% and 2% on the three attack scenarios respectively, while sharing with all the dependent nodes improves 10%, 7% and 3%. Sharing with all nodes in the networks gives improvements rates over not sharing of 64%, 33% and 32%. Thus, it can be concluded that only the policy of sharing with all nodes is substantially beneficial for the general welfare of the network in the terms and conditions established during our experimentation.

Regarding the effects of different attack scenarios on the **MeanCIA**, we can observe that, in general, “Attack 5% Random” has higher impacts than “Attack Probab High Deps” and “Attack Probab High Servs.”, no matter what the information sharing policy is being applied. Thus, from the adversarial point of view, it is better to attack randomly if he knows that no information sharing or sharing only with dependent nodes, is being applied.

### *5.3.2 Analysis and identification of critical nodes*

In this section, we provide an analysis to detect nodes that are more important to the community in terms of the **Information Quality**. We analyse these relevant nodes according to the **Gain** metric defined above.

First, we calculate $G_i^t$ for every node $i$ in the network and simulation, focusing only in the last epoch $t = 200$. We only compare sharing scenarios with more relevant differences found in Fig. 2, that is, scenarios applying sharing policies a) and d) as defined en Section 5.2. This means *sh1* and *sh2* described in Eq. 5 are *not sharing* and *sharing with all nodes*, respectively. Nodes that benefit from scenario *sh2* respect to scenario *sh1* are those with $G_i^{200} > 0$. Nodes that do not benefit from scenario *sh2* respect to scenario *sh1* are those with $G_i^{200} \leq 0$.

Second, we conduct the analysis in terms on how many pieces of *quality* information are sent $Q_i^{out}$ and received $Q_i^{in}$ to/ from each node. Fig. 3 shows the distribution of nodes in terms of how many pieces of *quality* information is provided (y-axis = $Q_i^{out}$) and received (x-axis = $Q_i^{in}$). Red triangles represent those nodes that do not obtain benefits because of information sharing ($G_i^{200} \leq 0$), and blue circles represent the opposite ($G_i^{200} > 0$). In general, nodes that do not obtain any benefit usually provide more pieces of *quality* information than they receive. This may occur because they receive attacks that are new to the network (e.g. zero day exploits) and afterwards they notify (and immunize) the remainder nodes about them, but they do not receive information regarding other attacks. While this obviously depends on the specific settings and the attack scenario, the analysis provided with this simulation framework allows the identification of nodes whose information is relevant for the health of the entire network. Moreover, since these nodes may not benefit from the sharing community, in real settings they could be rewarded by other means (e.g. providing extra economical benefits) to incentive their cooperativeness.

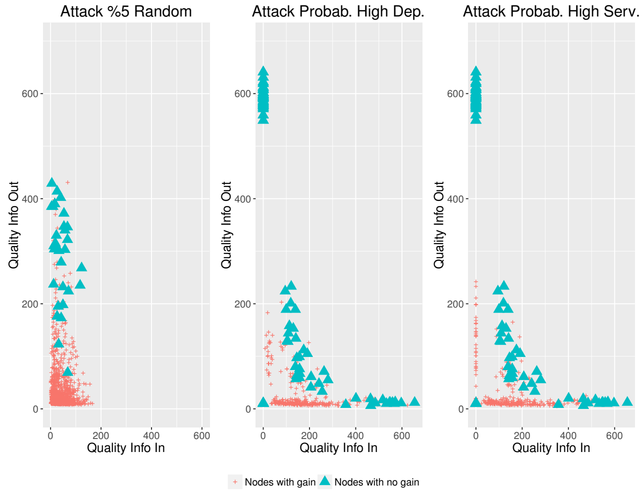

**Figure 3: Distribution of nodes that gain (red circles) and lose out (blue triangles) because of information sharing, in terms of number of pieces of quality information shared and received**

## 6. CONCLUSIONS

Attack prevention and detection are essential tasks in cybersecurity management. Organizations suffer multiple cyberattacks and information sharing can help to develop early prevention mechanisms. However, organizations are not willing to share information unless incentives are achieved. In this regard, this paper presents a model for cybersecurity information sharing among dependently organizations being impacted for different cyberattacks. Functional Dependency Network Analysis is used for attacks propagation and game theory for information sharing management. A framework has been developed and the model has been tested in a particular scenario. Results using the simulation framework suggest that information sharing generally improves the general welfare. Moreover, we elucidate that nodes that receive new attacks in the network provide information with higher quality even though they do not benefit from the sharing community, so they should be rewarded and motivated to share such information. In general, our experimental work shows that the proposed model can help to simulate network conditions and adversarial settings to analyse beneficial sharing policies, both in terms of particular nodes and in terms of the general welfare of the sharing community. It can be used as a part of a decision support system or during countermeasure allocation processes. Future work will focus on the development of new and assorted scenarios to get more general outcomes. Moreover, other techniques like agent-based simulation or genetic algorithms could be applied for identifying the best sharing policies for each node.

# 7. ACKNOWLEDGEMENTS

We want to thank the anonymous reviewers for their meaningful comments. This work was partially supported by the MINECO grant TIN2013-46469-R and the CAM grant S2013/ICE-3095 CIBERDINE -CM funded by Madrid Autonomous Community and co-funded by European funds.

# 8. REFERENCES

[1] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *System Sciences, 2000. Proc. of the 33rd Annual Hawaii Intl. Conf. on*, pages 9–pp. IEEE, 2000.

[2] M. Beckenkamp, H. Hennig-Schmidt, and F. P. Maier-Rigaud. Cooperation in symmetric and asymmetric prisoner's dilemma games. *MPI Collective Goods Preprint*, (2006/25), 2007.

[3] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang. Complex networks: Structure and dynamics. *Physics reports*, 424(4):175–308, 2006.

[4] C. Camerer. *Behavioral game theory*. New Age International, 2010.

[5] B. Drabble. Information propagation through a dependency network model. In *Collaboration Technologies and Systems (CTS), 2012 Intl. Conf. on*, pages 266–272. IEEE, 2012.

[6] J. W. Eaton, D. Bateman, S. Hauberg, and R. Wehbring. *GNU Octave version 4.0.0 manual: a high-level interactive language for numerical computations*. 2015.

[7] A. K. Eric Luiijf. Sharing cyber security information. (March), 2015.

[8] E. U. European Parliament. Directive of the european parliament and of the council concerning measures for a high common level of security of network and information systems across the union, 2016. PE 26 2016 INIT - 2013/027 (OLP).

[9] J. Freudiger, E. De Cristofaro, and A. E. Brito. Controlled data sharing for collaborative predictive blacklisting. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 327–349. Springer, 2015.

[10] D. Gambetta et al. Can we trust trust. *Trust: Making and breaking cooperative relations*, 13:213–237, 2000.

[11] P. R. Garvey and C. A. Pinto. Introduction to functional dependency network analysis. In *The MITRE Corporation and Old Dominion, Second International Symposium on Engineering Systems, MIT, Cambridge, Massachusetts*, 2009.

[12] J. e. a. Granatyr. Trust and reputation models for multiagent systems. *ACM Computing Surveys*, 48(2):27, 2015.

[13] C. Guariniello and D. DeLaurentis. Communications, information, and cyber security in systems-of-systems: Assessing the impact of attacks through interdependency analysis. *Procedia Computer Science*, 28:720–727, 2014.

[14] J. L. Hernandez-Ardieta, J. E. Tapiador, and G. Suarez-Tangil. Information sharing models for cooperative cyber defence. In *5th Intl. Conf. on Cyber Conflict*, pages 1–28. IEEE, 2013.

[15] P. Institue. 2016 cost of data breach study: global analysis. Technical report, Ponemon Institute, 2016.

[16] L. R. Izquierdo, S. S. Izquierdo, and F. Vega-Redondo. Learning and evolutionary game theory. In *Encyclopedia of the Sciences of Learning*, pages 1782–1788. Springer, 2012.

[17] C. Karsberg and C. Skouloudi. Annual incident reports 2014. Technical report, ENISA, 2015.

[18] M. Khouzani, V. Pham, and C. Cid. Strategic discovery and sharing of vulnerabilities in competitive environments. In *Decision and game theory for security*, pages 59–78. Springer, 2014.

[19] S. Laube and R. Böhme. Mandatory security information sharing with authorities: Implications on investments in internal controls. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pages 31–42. ACM, 2015.

[20] J. Li. How to design a strategy to win an ipd tournament. *The iterated prisoner's dilemma*, 20:89–104, 2007.

[21] G. Meng, Y. Liu, J. Zhang, A. Pokluda, and R. Boutaba. Collaborative security: A survey and taxonomy. *ACM Computing Surveys*, 48(1):1, 2015.

[22] P. Naghizadeh and M. Liu. Inter-temporal incentives in security information sharing agreements. In *Position paper for the AAAI Workshop on Artificial Intelligence for Cyber-Security*, 2016.

[23] G. Oliva, S. Panzieri, and R. Setola. Agent-based input–output interdependency model. *International Journal of Critical Infrastructure Protection*, 3(2):76–82, 2010.

[24] B. Petrenj, E. Lettieri, and P. Trucco. Information sharing and collaboration for critical infrastructure resilience–a comprehensive review on barriers and emerging capabilities. *International Journal of Critical Infrastructures*, 9(4):304–329, 2013.

[25] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, et al. Cybex: The cybersecurity information exchange framework (x. 1500). *ACM SIGCOMM Computer Communication Review*, 40(5):59–64, 2010.

[26] M. Shor. "payoff," dictionary of game theory terms. http://www.gametheory.net/dictionary/Payoff.html. Accessed: 2016-07-11.

[27] L. B. Spijkervet. Less is more. Master's thesis, Delft University of Technology, 2014.

[28] S. Subramanian and D. e. a. Robinson. 2014 deloitte-nascio cybersecurity study. state governments at risk: time to move forward. Technical report, Deloitte, NASCIO, 2014.

[29] D. e. a. Tosh. An evolutionary game-theoretic framework for cyber-threat information sharing. In *IEEE Intl. Conf. on Communications*, pages 7341–7346. IEEE, 2015.

[30] Y. WANG and C. Ng. Asymmetric payoff mechanism and information effects in water sharing interactions: A game theoretic model of collective. In *International Komosozu Society, Mt. Fuji, Japan, 2013*, page 68. IASC, 2013.

[31] U. S. A. White-House. National and homeland security presidential directives, 2008. NSPD-54/HSPD-23.