Becoming Cybercriminals

Incentives in Networks with Interdependent Security

Aron Laszka and Galina Schwartz

University of California, Berkeley

Abstract. We study users' incentives to become cybercriminals when network security is interdependent. We present a game-theoretic model in which each player (i.e., network user) decides his type, honest or malicious. Honest users represent law-abiding network users, while malicious users represent cybercriminals. After deciding on their types, the users make their security choices. We will follow [29], where breach probabilities for large-scale networks are obtained from a standard interdependent security (IDS) setup. In large-scale IDS networks, the breach probability of each player becomes a function of two variables: the player's own security action and network security, which is an aggregate characteristic of the network; network security is computed from the security actions of the individual nodes that comprise the network. This allows us to quantify user security choices in networks with IDS even when users have only very limited, aggregate information about security choices of other users of the network.

Keywords: interdependent security, cybercrime, security economics, game theory, Nash equilibrium, security investments

1 Introduction

Due to technological reasons, network security features multiple layers of interdependencies. Interdependent security has been extensively studied, see [20] for a recent survey; however, most of the existing literature does not address the strategic reasons of the losses; i.e., there is no explicit modeling of attackers' incentives to become engaged in cybercrime. In this paper, we look at users' incentives for becoming attackers (malicious users), and study how users' security choices and utilities are affected by the number of attackers.

Another distinctive feature of our setup, which is non-standard for the IDS literature, is that our model can deal with large-scale IDS networks. In many cases, the IDS papers do not emphasize the effects of large-scale games. Notable exceptions closely related to our work are [24] and [1]. In the latter, the authors consider a model with multiple IDS players similar to our setup, and in the former, large-scale networks with different topologies are studied. Ideas from [24] were further developed in [29], whose setup we expand to study incentives for becoming a cybercriminal.

We consider a large-scale IDS network with strategic players (i.e., network users or nodes), who choose to which type they will belong, honest or malicious; the players also make choices of their security investments; we allow continuous security choices.

A common trend in numerous papers approaching economic aspects of cybercrime is inquiry into the "production technology" of cybercrime.[1] Our approach is complementary: we give virtually no details about the implementation side of cybercrime. We take a large-scale, macro perspective, and reduce the problem to the following base level parameters: risk aversion, loss size, degree of IDS, and costs of improving security. In this paper, we consider a more aggregate perspective. We build on the framework of risk assessment for large-scale IDS networks, developed by [29], and model users' incentives to become cybercriminals. While at present our model is minimalistic and stylized, it could be extended to include more parameters, such as different costs of attacking, and attacks with different IDS features.

Following a seminal contribution of Tullock [31], we approach incentives for cybercrime in the perspective of rent seeking. The core idea of rent seeking was originally coined by Tullock to study any non-productive wealth redistribution. Rent seeking was demonstrated to be useful methodology for the analysis of diverse subjects, ranging from monopolist's (over)pricing and losses from imposition of tariffs to corruption, fraud, theft, and other criminal endeavors. The distinguished feature of rent seeking is its wasteful and oftentimes openly coercive nature. The propensity of rent-seeking activities depends on institutions and enforcement capabilities. The prevalence of inefficient, corrupt institutions results in higher rent-seeking activities, and it is associated with poor economic performance and growth.

In [26,27], Olson connected an increase of rent-seeking activities with increased severity of the problem(s) of collective action. In the cybersecurity economics literature, this problem is studied under the name of free riding. The problem arises when individually and socially optimal actions differ, and a large number of dispersed players is present, with each player's gains or losses being trivial in size. In such cases, mechanisms to align individually and socially optimal actions are hard to find. Investments in cybersecurity are well known to have a marked presence of free riding ([32,2,3]), and thus, in general, suboptimal. Proliferation of rent seeking (in our case, cybercrime) negatively affects growth, as it shifts resources away from productive activities.

Consider for example the papers modeling one of the most widespread cybercrimes – phishing. The modeling literature originated by [7] looks at specific costs (number of targets, strength of the attack, probability of being caught, and the size of the fine) and the benefits (revenues resulting from the losses of the targets, such as stolen bank account information). The authors discuss the difficulties of designing effective countermeasures. From their analysis, increased penalties have limited impact. They advocate that improving the controls to prevent trading of stolen data will be more impactful. Followup papers introduce

[1] For example in [18,4,22], cybercrime is approached from value-chain perspective.

additional considerations and tools, such as risk simulation approach [17]. At the same time, the literature acknowledges practical complications: while preventing trading will be highly effective, it is questionable that this recommendation can be achieved in practice: it requires global enforcement institutions with novel legal rights and technological capabilities.

In the world with global connectivity, crime is becoming global as well due to the increased proliferation of the cybercrime. The global world is facing new threats, with meager existing institutions to counteract them. This situation requires developing novel tools to reduce user incentives for becoming malicious. Designing new economic institutions to be charged with mitigating rent-seeking incentives to engage in cybercrime is socially desirable as only such institutions will preclude the formation and syndication of organized international cybercrime. Our work permits quantifiable assessment and comparative analysis of various policy tools and institutions.

1.1 Applications

Our analysis can be applied to address robustness of large-scale cyber-physical systems (CPS). In [16], Knowles et al. present a comprehensive review of security approaches for CPS, and survey methodologies and research for measuring and managing cyber-risks in industrial control systems.

Since modern CPS are increasingly networked, achieving robust performance requires addressing the problem of interdependencies (see Section 6.2.3 of [16]). The authors identify the importance of system-wide risk assessment for CPS, and discuss three difficulties: (i) scant data availability, (ii) lack of established framework for defining and computing risk metrics, and (iii) lack of reliable performance evaluation of security measures. The focus of our paper is (ii). We use IDS framework, and demonstrate how system security evolves when the attacker choices are endogenous.

For example, the perpetrators of the Energetic Bear (a.k.a. Dragonfly) cyberespionage campaign exploited interdependence between energy companies and industrial control system (ICS) manufacturers [30]. In order to penetrate highly-secure targets (e.g., energy grid operators, major electricity generation firms, petroleum pipeline operators in the U.S., Germany, Turkey, etc.), the attackers compromised ICS manufacturers and inserted malware into software updates distributed by these manufacturers, which were downloaded and applied by the targets, leading to their compromise.

While Knowles et al. discuss the problem of interdependencies, they also express skepticism about the realistic options of improving the current state of cybercrime reality [16]. In fact, the authors expect slow progress due to lack of incentives for private entities to share information about risks. Our setup allows circumventing the problem of data limitations as our analysis relies on aggregate information about network security only.

The remainder of this paper is organized as follows. In Section 2, we discuss related work on interdependent security. In Section 3, we introduce our model of interdependent security and incentives for malicious behavior. In Section 4,

we study the Nash equilibria of our model. In Section 5, we present numerical illustrations for our theoretical results. Finally, in Section 6, we offer concluding remarks and outline future work.

2 Related Work

In this section, we provide a brief overview of the most related papers from the interdependent security literature. For a more detailed review of the relevant literature, we refer the interested reader to [20].

The interdependent security problem was originally introduced in the seminal paper of Kunreuther and Heal, who initially formulated an IDS model for airline security. They extended their model to cover a broad range of applications, including cybersecurity, fire protection, and vaccinations [19]. They study the Nash equilibria of the model, and examine various approaches for incentivizing individuals to invest in security by internalizing externalities, such as insurance, fines, and regulations. In follow-up work, they extend their analysis to study tipping (i.e., when inducing some individuals to invest in security results in others investing as well) and coalitions of individuals that can induce tipping [10,11]. Other authors have also used this model to study various phenomena, including uncertainty and systematic risks [13,21,14].

Öğüt et al. introduce an interdependence model for cybersecurity, which they use to study the effects of interdependence on security investments and cyber-insurance [24]. Similar to the model of Kunreuther and Heal, the model of Öğüt et al. is based on the probabilistic propagation of security compromises from one entity to the other. In follow-up work, the authors extend their analysis by considering subsidies provided by a social planner, and find that subsidies for security investments can induce socially optimal investments, but subsidies for insurance do not provide a similar inducement [25].

Varian introduces and studies three prototypical interdependence models for system reliability: total effort, weakest link, and best shot [32]. In these models, the overall level of reliability depends respectively on the sum of efforts exerted by the individuals, the minimum effort, and the maximum effort. Later, these models have been widely used for studying security interdependence.

For example, Grossklags et al. compare Nash equilibrium and social optimum security investments in the total effort, weakest link, and best shot models [8]. In another example, Honeyman et al. address investment suboptimalities when users cannot distinguish between security failures (weakest link), and reliability failures (total effort) [12].

Khouzani et al. consider security interdependence between autonomous systems (AS), and study the effect of regulations that penalize outbound threat activities [15]. The authors find that free-riding may render regulations ineffective when the fraction of AS over which the regulator has authority is lower than a certain threshold, and show how a regulator may use information regarding the heterogeneity of AS for more effective regulation.

In most interdependent security models, adversaries are not strategic decision-makers. Nonetheless, there are a few research efforts that do consider strategic adversaries. Hausken models adversaries as a single, strategic player, who considers the users' strategies and substitutes into the most optimal attack allocation [9]. This substitution effect creates negative externalities between the users' security investments, which are fundamentally different from the positive externalities considered in our model. Moscibroda et al. consider malicious users [23] in the inoculation game, which was introduced originally by Aspnes et al. [5,6]. In the model of Moscibroda et al., malicious users are byzantine: they appear to be non-malicious users who invest in security, but they are actually not secure at all. Furthermore, the set of malicious users is assumed to be exogenous to the model. Grossklags et al. introduce an interdependence model, called weakest target, in which an attacker targets and always compromises the user with lowest security effort [8].

In another related paper, Acemoglu et al. focus on security investments of interconnected agents, and study contagion due to the possibility of cascading failures [1]. They analyze how individual and social optima behave in the presence of endogenous attacks. The authors formulate the sufficient conditions for underinvestment in security, and demonstrate that overinvestment occurs in some cases. Interestingly, in contrast to our results, overinvestment in security may intensify when attacks are endogenous in [1]. In our paper, the imposition of fast growing security costs guarantees that underinvestment occurs.

3 Model

Here, we introduce our model of non-malicious and malicious users, their incentives, and the security interdependence between them. A list of symbols used in this paper can be found in Table 1.

We assume that the number of users is fixed and denoted by N. Each user chooses his type, malicious or honest (i.e., attacker or defender). We will denote the number of malicious users and honest users by M and $N - M$, respectively. Each user's objective is to maximize his expected payoff (i.e., utility) $\mathfrak{u}$

$$\mathfrak{u}_i = \mathfrak{u}_i(\mathbf{t}, \mathbf{s}) = \max_{t_i, s_i} \{u_i, v_i\},$$

where $v_i = v_i(\mathbf{t}, \mathbf{s})$ and $u_i = u_i(\mathbf{t}, \mathbf{s})$ denote respective utilities of malicious and honest users, and $\mathbf{s} = (s_1, \ldots, s_N)$ is a vector of the players' security choices, and $\mathbf{t} = (t_1, \ldots, t_N)$ is a vector of user types, with $t_i = 1/0$, for malicious/honest user respectively, which allows us to express the number of malicious users M as:

$$M := \sum_{i=1}^{N} t_i. \tag{1}$$

Each honest user i objective is to maximize his expected utility $u_i = u_i(\mathbf{t}, \mathbf{s})$

$$u_i = [1 - B_i(\mathbf{s})]\, U(W) + B_i(\mathbf{s}) U(W - L) - h(s_i), \tag{2}$$

Table 1. List of Symbols

Symbol	Description
Constants	
N	number of users
W	initial wealth of a user
L	loss of a user in case of a security breach
μ	probability of a malicious user getting caught
q_∞	defined as $\lim_{N\to\infty} q(N)N$
Functions	
$q(N)$	strength of interdependence between N users
$h(s)$	cost of security level s
$B_i(s_1,\ldots,s_N)$	security breach probability of user i
$G_i(M,s_1,\ldots,s_N)$	financial gain of malicious user i
$U(\ldots)$	utility function of a user
Variables	
s_i	security level of user i
M	number of malicious users
$\hat{s}$	equilibrium security level of honest users

where $B_i(\mathbf{s}) = B_i(s_i, s_{-i})$ is the probability that user i suffers a security breach, $U(w)$ is the utility with wealth w, W is the initial user wealth, and L is the loss in case of a security breach. We assume that $L \in (0, W)$. The function $h(s)$ is security cost function, with $s \in [0, 1)$ denoting the security level of the user. While we view h as the "cost" of attaining a given security level, we model these costs as separable from U because security costs are often non-monetary (e.g., inconvenience and effort).

We assume $h'(s) > 0$ and $h''(s) > 0$ for $s_i \in (0, 1)$ for every $s \in [0, 1)$, $h(0) = h'(0) = 0$, and $h(1) = \infty$.[2] In addition, we will impose $h'''(s) > 0$ to simplify the exposition. Intuitively, with these assumptions, the marginal productivity of investing in security is decreasing rapidly, and the cost of attaining perfect security is prohibitively high. We assume that the users are risk-averse, that is, the function U is concave at any wealth $w \geq 0$: $U'(w) > 0$ and $U''(w) < 0$; also we let $U(0) = 0$.

Each malicious user j maximizes $v_j = v_j(\mathbf{t}, \mathbf{s})$

$$v_j = (1 - \mu)U(G_j(\mathbf{t}, \mathbf{s})) + \mu U(0) - h(s_j), \tag{3}$$

where μ is the probability of a malicious user being caught and punished (e.g., by law enforcement), and G_j is the gain of user j from engaging in cyber-crime. We assume that honest users' losses are distributed evenly between the malicious users:

$$G_j(\mathbf{t}, \mathbf{s}) = \frac{\sum_{i\in\text{honest users}} B_i(\mathbf{s})L}{M}, \tag{4}$$

and M is given by eq. (1).

[2] In other words, the Inada conditions hold.

In our model, each user has two strategic actions: (i) user decides on his type (malicious or honest), and on his security level s (and thus, cost $h(s)$). In the next section (Section 4), we will study the Nash equilibria of our model, which are defined as follows.

Definition 1 (Nash Equilibrium). *A strategy profile* $(\mathbf{t}, \mathbf{s})$ *is a Nash equilibrium if*

- *being malicious is a best response for every malicious user and*
- *being non-malicious and investing in security level* s_i *is a best response for every non-malicious user* i*.*

3.1 Interdependent Security Model

For breach probabilities B_i, we will assume interdependent security (IDS). Our model builds on well-known interdependent security model of Kunreuther and Heal [19].

In this model, a user can be compromised (i.e., breached) in two ways: (i) directly and (ii) indirectly. The probability of a *direct breach* reflects the probability that an honest user is breached directly by an adversary. For each user i, the probability of being compromised directly is modeled as Bernoulli random process, with the failure probability equal to $(1 - s_i)$ when security investment is $h(s_i)$. This means that the probability of user i being safe from direct attacks is equal to that user's security level s_i, and does not depend on other users' security choices. We assume that for any two users, the probabilities of direct compromise are independent Bernoulli random processes.

Indirect breach probability reflects the presence of IDS – the users are interdependent. More specifically, we assume that in addition to direct compromise, the user can be breached indirectly – i.e., via a connection to another user, who was compromised directly. The assumption of indirect compromise reflects the connectivity and trust between the users. Let $q_{ij}(N)$ denote the conditional probability that user i is compromised indirectly by user j in the network with N users, given that user j is directly compromised. To simplify, for now we will assume that $q_{ij}(N)$ is a constant (independent of i and j): $q_{ij}(N) = q(N)$. Then, the probability of user i to be breached indirectly can be expressed as

$$
\begin{aligned}
&\Pr[\text{compromised indirectly}] \\
=&1 - \Pr[\text{not compromised indirectly}] && (5)\\
=&1 - \prod_{j \neq i} \Pr[\text{no indirect compromise from user } j] && (6)\\
=&1 - \prod_{j \neq i} (1 - \Pr[\text{user } j \text{ is directly compromised}] \Pr[\text{successful propagation}]) && (7)\\
=&1 - \prod_{j \neq i} (1 - (1 - s_j) q(N)). && (8)
\end{aligned}
$$

Next, let $B_i = B_i(\mathbf{s})$ denote the probability that user i is compromised (i.e., breached) either directly or indirectly:

$$B_i = 1 - \Pr[\text{not compromised}] \tag{9}$$
$$= 1 - \Pr[\text{not compromised directly}] \Pr[\text{not compromised indirectly}] \tag{10}$$
$$= 1 - s_i \prod_{j \neq i} (1 - (1 - s_j) q(N)). \tag{11}$$

In practical scenarios, $q(N)$ must decrease with N (the number of network users). As it is standard in aggregative games, we let the limit of $q(N)$ equal to zero as N approaches infinity.

4 Analysis

Next, we present theoretical results on our model of interdependent security and incentives for malicious behavior. First, in Section 4.1, we consider breach probabilities in large-scale networks. We show that the IDS model allows approximating a user's breach probability using the user's own security level and the average security level of the network. Second, in Section 4.2, we study equilibrium security choices for a game with a fixed number of malicious users. Finally, in Section 4.3, we study the equilibrium of the game where the number of malicious users is endogenous: it is determined by user choices.

4.1 Large-Scale Networks

We begin our analysis by studying the honest users' breach probabilities in large-scale networks (i.e., when the number of users N is high). Our goal here is to express the breach probabilities in a simpler form, which will facilitate the subsequent analysis of the users' equilibrium choices.

First, recall that in practical scenarios, $q(N)$ approaches zero as N grows (i.e., $\lim_{N \to \infty} q(N) = 0$). Hence, we can discard the terms with $q(N)^2, q(N)^3, \ldots$, and obtain the following approximation for large-scale networks:

$$B_i(\mathbf{s}) = 1 - s_i \prod_{j \neq i} (1 - (1 - s_j) q(N)) \tag{12}$$
$$\approx 1 - s_i \left(1 - \sum_{j \neq i} (1 - s_j) q(N) \right) \tag{13}$$
$$\approx 1 - s_i \left[1 - q(N) N \left(1 - \frac{\sum_{j \neq i} s_j}{N} \right) \right]. \tag{14}$$

Let $\bar{s}$ denote the average of the security levels taken over all users; formally, let $\bar{s} = \frac{\sum_j s_j}{N}$. Next, we use that the fraction $\frac{\sum_{j \neq i} s_j}{N}$ approaches the average security level $\bar{s}$ as N grows, and obtain:

$$1 - s_i \left[1 - q(N) N \left(1 - \frac{\sum_{j \neq i} s_j}{N} \right) \right] \approx 1 - s_i \left(1 - q(N) N (1 - \bar{s}) \right). \tag{15}$$

Finally, we assume that $q(N)N$ has a limit as N approaches infinity, and this limit is less than 1. Then, we let $q_\infty = \lim_{N\to\infty} q(N)N$, which gives us:

$$1 - s_i\,(1 - q(N)N(1-\bar{s})) \approx 1 - s_i(1 - q_\infty(1-\bar{s})) \tag{16}$$

$$= 1 - s_i(1-q_\infty) - s_i q_\infty \bar{s}. \tag{17}$$

Thus, for large-scale networks, breach probability B_i is a function of user security s_i and the average security $\bar{s}$:

$$B_i(s_i, s_{-i}) = 1 - s_i(1-q_\infty) - s_i q_\infty \bar{s}. \tag{18}$$

In the remainder of the paper, we use (18) for breach probability B_i of user i.

4.2 Game with Exogenous Number of Malicious Users

Next, let us consider a game with a fixed number M of malicious users, that is, a game in which the strategic choice of every user i is limited to selecting security s_i. From Equation (3), malicious users incur no losses, thus, they will not invest in network security (see Section 3.1). Hence, in any equilibrium, $s_j = 0$ for every malicious user j.

Let $\bar{s}_H$ denote the average security level of honest users:

$$\bar{s}_H = \frac{\sum_{j\in\text{honest users}} s_j}{N-M}. \tag{19}$$

Recall that malicious users contribute zero towards the security of the network, that is, $s_j = 0$ for every malicious user j. Hence, the breach probability of an honest user i can be expressed as

$$B_i(s_i, \bar{s}_H) = 1 - s_i(1-q_\infty) - s_i q_\infty \bar{s} \tag{20}$$

$$= 1 - s_i(1-q_\infty) - s_i q_\infty \frac{N-M}{N}\bar{s}_H. \tag{21}$$

Using $B_i(s_i, \bar{s}_H)$, the expected utility of user i can be expressed as

$$u = [1 - B_i(s_i, \bar{s}_H)]\,U(W) + B_i(s_i, \bar{s}_H)U(W-L) - h(s_i) \tag{22}$$

$$= U(W-L) + [1 - B_i(s_i, \bar{s}_H)]\,\Delta_0 - h(s_i), \tag{23}$$

where

$$\Delta_0 = U(W) - U(W-L). \tag{24}$$

Our goal is to characterize the equilibrium security levels when user types are given. Thus, in the game $\Gamma(M)$ we assume that the users' types are fixed and their strategic choices are restricted to selecting security levels, and we study the Nash equilibrium of this game.

Definition 2 (Nash Equilibrium with Fixed M). *Consider the game $\Gamma(M)$ in which the number of malicious users M is given. A strategy profile $(s_1, \ldots, s_N)$ is a Nash equilibrium if security level s_i is a best response for every user.*

Lemma 1. *In any equilibrium of the game $\Gamma(M)$, for each user type, security choices are identical.*

Proof. First, we notice that for any M, malicious users do not invest in security. From the definition of malicious user utilities (3), they have no losses, and thus have no incentive to invest in security: thus, for any M, it is optimal to choose $s_j^*(M) = 0$ for every malicious user j.

Second, we show that every honest user has a unique best response, and this best response is independent of user identity, which means that any equilibrium is symmetric. Consider some $\mathbf{s} = (\cdot, s_{-i})$. To find user i's optimal security (i.e., the utility maximizing security s_i), we take the first derivative of (2) with respect to s_i (user i FOC):

$$\frac{d}{ds_i} u_i = -\frac{d}{ds_i} B_i(s_i, s_{-i}) \Delta_0 - h'(s_i) = 0, \tag{25}$$

where we use B_i given by (14)

$$\frac{d}{ds_i} B_i(s_i, s_{-i}) = \frac{d}{ds_i} \left(1 - s_i \left[1 - q(N) N \left(1 - \frac{\sum_{j \neq i} s_j}{N} \right) \right] \right) \tag{26}$$

$$= - \left[1 - q(N) N \left(1 - \frac{\sum_{j \neq i} s_j}{N} \right) \right]. \tag{27}$$

Since the second order condition (SOC) is negative:

$$\frac{d^2}{ds_i^2} u_i = -h''(s_i) < 0,$$

there exists a unique optimal response s_i^* to any $s_i^* = s_i^*(M, s_{-i})$, and it is given by the solution of FOC (25).

For large N, we have:

$$\frac{d}{ds_i} u_i = -\frac{d}{ds_i} B_i(s_i, s_{-i}) \Delta_0 - h'(s_i) \tag{28}$$

$$= \underbrace{\left[1 - q_\infty \underbrace{\left(1 - \frac{N-M}{N} \bar{s}_H \right)}_{<1} \right]}_{>0} \Delta_0 - h'(s_i). \tag{29}$$

Since $h'(s_i)$ is increasing in s_i, the derivative u' is a decreasing function of s_i. Furthermore, since the first term is positive and $h'(0) = 0$, the derivative u' is positive at $s_i = 0$. Consequently, user i best response s_i^* is interior (because $s_i = 1$ cannot be optimal as it is unaffordable), and it is given by:

$$u' = 0 \tag{30}$$

$$\left[1 - q_\infty \left(1 - \frac{N-M}{N}\bar{s}_H\right)\right] \Delta_0 - h'(s_i) = 0 \tag{31}$$

$$\Delta_0 = \frac{h'(s_i)}{1 - q_\infty \left(1 - \frac{N-M}{N}\bar{s}_H\right)}. \tag{32}$$

Finally, since the solution of (32) is independent of user identity, we infer that best responses are identical for all honest users. □

From Lemma 1, we infer that the honest users' security levels are identical in an equilibrium. The following theorem shows that the equilibrium security level always exists, and is unique. This implies that there is a unique Nash equilibrium of the game $\Gamma(M)$.

Theorem 1. *For a given M, the honest users' equilibrium security $s^*(M)$ is unique.*

Proof. By definition, identical security level s is an equilibrium if and only if security level s is a best response for every honest user. Consequently, it follows from the proof of Lemma 1 that an identical security level s is an equilibrium if and only if

$$\Delta_0 = R(s, M), \tag{33}$$

where

$$R(s, M) = \frac{h'(s)}{1 - q_\infty + q_\infty \frac{N-M}{N} s}. \tag{34}$$

In order to prove the claim of the theorem, we have to show that Equation (33) has a unique solution.

First, notice that

$$R(0, M) = 0 \tag{35}$$

since $h'(0) = 0$, and

$$R(1, M) = \infty \tag{36}$$

since $h(s)$ grows without bound as s approaches 1. Therefore, there must exist a value s^* between 0 and 1 for which $R(s^*, M) = \Delta_0$ as $R(s, M)$ is a continuous function on $[0, 1)$.

To prove that this s^* exists uniquely, it suffices to show that $\frac{d}{ds}R(s, M) > 0$ on $(0, 1)$. The first derivative of $R(s, M)$ with respect to s is

$$\frac{d}{ds}R(s, M) = \frac{h''(s)\left[1 - q_\infty + q_\infty \frac{N-M}{N} s\right] - h'(s) q_\infty \frac{N-M}{N}}{\left[1 - q_\infty + q_\infty \frac{N-M}{N} s\right]^2}. \tag{37}$$

Since the denominator is always positive, we only have to show that the numerator is positive on $(0, 1)$. First, observe that the numerator is non-negative at $s = 0$, since

$$\underbrace{h''(0)}_{\geq 0} \underbrace{\left[1 - q_\infty + q_\infty \frac{N-M}{N} s\right]}_{>0} - \underbrace{h'(0)}_{=0} q_\infty \frac{N-M}{N} \geq 0. \tag{38}$$

Finally, we prove that the numerator is strictly increasing on $[0,1)$ by showing that its first derivative with respect to s is positive:

$$\begin{aligned}
&\frac{d}{ds}\left(h''(s)\left[1-q_\infty+q_\infty\frac{N-M}{N}s\right]-h'(s)q_\infty\frac{N-M}{N}\right)\\
=\;& h'''(s)\left[1-q_\infty+q_\infty\frac{N-M}{N}s\right]+h''(s)q_\infty\frac{N-M}{N}\\
&-h''(s)q_\infty\frac{N-M}{N} &(39)\\
=\;&\underbrace{h'''(s)}_{>0}\underbrace{\left[1-q_\infty+q_\infty\frac{N-M}{N}s\right]}_{>0} &(40)\\
>\;&0. &(41)
\end{aligned}$$

Since the numerator is non-negative at $s=0$ and it is strictly increasing in s on $[0,1)$, it must be positive for any $s\in(0,1)$. Therefore, the first derivative of $R(s,M)$ is also positive, which proves that the solution s^* exists uniquely for a given number of malicious users M. □

Equilibrium in the game $\Gamma(M)$ exists and is unique. This allows us to define the equilibrium security level as a function $s^*(M)$ of M.

Theorem 2. *As the number of malicious users M increases, the honest users' equilibrium security $s^*(M)$ decreases.*

Proof. Since $\Delta_0 = R(s^*(M),M)$ must hold for every pair $(s^*(M),M)$ (see Equation (33)), we have

$$\begin{aligned}
0=&\frac{d}{dM}R(s^*(M),M) &(42)\\
0=&\;\frac{h''(s^*(M))s^{*\prime}(M)\left(1-q_\infty+q_\infty\frac{N-M}{N}s^*(M)\right)}{\left(1-q_\infty+q_\infty\frac{N-M}{N}s^*(M)\right)^2}\\
&-\frac{h'(s^*(M))q_\infty\left(\frac{-1}{N}s^*(M)+\frac{N-M}{N}s^{*\prime}(M)\right)}{\left(1-q_\infty+q_\infty\frac{N-M}{N}s^*(M)\right)^2} &(43)\\
&-h'(s^*(M))q_\infty\left(\frac{-1}{N}s^*(M)+\frac{N-M}{N}s^{*\prime}(M)\right) &(44)\\
0=&\;s^{*\prime}(M)\left[h''(\hat{s}(M))\left(1-q_\infty+q_\infty\frac{N-M}{N}s^*(M)\right)-h'(s^*(M))q_\infty\frac{N-M}{N}\right]\\
&-h'(s^*(M))q_\infty\frac{-1}{N}s^*(M) &(45)\\
s^{*\prime}(M)=&\frac{h'(s^*(M))q_\infty\frac{1}{N}s^*(M)}{h'(s^*(M))q_\infty\frac{N-M}{N}-h''(s^*(M))\left(1-q_\infty+q_\infty\frac{N-M}{N}s^*(M)\right)}. &(46)
\end{aligned}$$

Notice that the denominator of the above fraction is the inverse of the numerator of the right-hand side of Equation (37). Since we have shown in the proof of

Theorem 1 that the numerator of the right-hand side of Equation (37) is positive, we have that the denominator of the above fraction is negative. Further, the numerator of the above fraction is obviously positive since it consists of only positive factors. Hence, $s^{*\prime}(M)$ is negative, which proves that the honest users' equilibrium security decreases as the number of malicious users increases. □

Unfortunately, $s^*(M)$ cannot be expressed in closed form. Nonetheless, we can easily find $s^*(M)$ numerically for any M. On the other hand, we can express the number of malicious users as a function $M(s^*)$ of the equilibrium security level s^* in closed form:

$$\Delta_0 = \frac{h'(s^*)}{1 - q_\infty + q_\infty \frac{N-M}{N} s^*} \tag{47}$$

$$q_\infty \frac{N-M}{N} s^* = \frac{h'(s^*)}{\Delta_0} + q_\infty - 1 \tag{48}$$

$$M(s^*) = N \left[1 - \frac{\frac{h'(s^*)}{\Delta_0} + q_\infty - 1}{q_\infty s^*} \right]. \tag{49}$$

The value of $M(s^*)$ can be interpreted as the number of malicious users which induces the honest users to choose security $s^*(M)$. Note that from Theorem 2, we readily have that $M(s^*)$ is a decreasing function of s^*.

4.3 Incentives for Becoming Malicious

In the previous subsection, we studied a restricted version of our game $\Gamma(M)$, in which the number of malicious users was exogenously given. We found the equilibrium of the game $\Gamma(M)$ as the solution of (34), from which the honest users' equilibrium security levels can be found.

Next, we will study the game Γ, in which users choose their types (honest or malicious). We will solve the game Γ by building on the results of the previous subsection.

First, Theorem 1 provides the honest users' equilibrium security level $s^*(M)$. Thus, we can express a malicious user's gain as a function $G_i(M)$ of the number of malicious users M:

$$G_i(M) = \frac{\sum_{j \in \text{honest users}} B_j(s_j, \bar{s}_H) L}{M} \tag{50}$$

$$= \frac{(N-M)\left(1 - s^*(1-q_\infty) - s^{*2} \frac{N-M}{N} q_\infty\right) L}{M}. \tag{51}$$

From Theorem 1, honest users choose $s^*(M)$ in an equilibrium. Next, we will find an equilibrium number of malicious users of M. For this purpose, we have to determine the combinations of M and $s^*(M)$ that form a strategy profile such that being malicious is a best response for malicious users and being honest is a best response for honest users.

Finally, now we are ready to prove that there always exists an equilibrium of the game in which users self-select their types (honest or malicious). Effectively, for each equilibrium number of malicious users M, the equilibrium security choices will be identical to equilibrium security $s^*(M)$ in the game $\Gamma(M)$ with that same fixed number of malicious users M.

Theorem 3. *There exists at least one Nash equilibrium.*

Proof. Assume the reverse. Then, at any $M \in [0, N-1]$ there exists (i) malicious or (ii) honest user, for whom a deviation to the opposite user type is profitable:

$$v(M, s^*(M)) < u|_{M-1, s_{-i}=s^*(M)} := \max_{s_i} u_i(M-1, s_i, s_{-i}), \quad \text{(i)} \tag{52}$$

or

$$u(M, s^*(M)) < v(M+1, s^*(M)), \quad \text{(ii)} \tag{53}$$

where $v(M, s^*(M))$ and $u(M, s^*(M))$ denote, respectively, the malicious and honest users' utility with M malicious users and all honest users choosing security $s^*(M)$, and $u_i(M, s_i, s_{-i})$ denotes honest user i's utility given that he chooses security s_i and all other honest users choose s_{-i}. From Lemma 1, the honest users' best response to M and $s_{-i} = s^*(M)$ is $s^*(M)$, which gives:

$$u|_{M, s^*(M)} \leq u(M, s^*(M)). \tag{54}$$

From Theorem 2, $s^*(M)$ decreases in M, which gives:

$$v(M+1, s^*(M)) < v(M+1, s^*(M+1)), \tag{55}$$

because ceteris paribus, lower security benefits malicious users. Similarly, we have from Theorem 2 and (54) that:

$$u|_{\tilde{M}, s^*(\tilde{M}+1)} < u|_{\tilde{M}, s^*(\tilde{M})} \leq u(M, s^*(M)) \tag{56}$$

because ceteris paribus, higher security benefits honest users.

Let (52) hold[3] for any $M > \tilde{M}$, but not for $\tilde{M}$. Hence, at $\tilde{M}+1$ we have:

$$v(\tilde{M}+1, s^*(\tilde{M}+1)) < u|_{\tilde{M}, s^*(\tilde{M}+1)}. \tag{57}$$

Then, if $\tilde{M}$ is not an equilibrium, (53) must hold:

$$u(\tilde{M}, s^*(\tilde{M})) < v(\tilde{M}+1, s^*(\tilde{M})). \tag{58}$$

Combining (58) and (57) with (55) and (56) provides:

$$u(\tilde{M}, s^*(\tilde{M})) < v(\tilde{M}+1, s^*(\tilde{M})) < v(\tilde{M}+1, s^*(\tilde{M}+1)) \tag{59}$$

$$v(\tilde{M}+1, s^*(\tilde{M}+1)) < u|_{\tilde{M}, s^*(\tilde{M}+1)} \leq u(\tilde{M}, s^*(\tilde{M})), \tag{60}$$

which contradict each other. Thus, Theorem 3 is proven. □

[3] If (52) holds for all $M \in [1, N-1]$, we let $\tilde{M} = 0$.

5 Numerical Illustrations

Here, we present present numerical results showcasing our model and illustrating our theoretical findings. First, we instantiate our model using the following parameter values:

- number of users $N = 500$,
- initial wealth $W = 100$,
- potential loss $L = 30$,
- security interdependence $q_\infty = 0.5$,
- probability of a malicious user getting caught $\mu = 0.2$,

and we use the following security-cost function (see Figure 1):

$$h(s) = 10\frac{s^2}{\sqrt{1-s}} \tag{61}$$

and the following utility function:

$$U(x) = x^{0.9}. \tag{62}$$

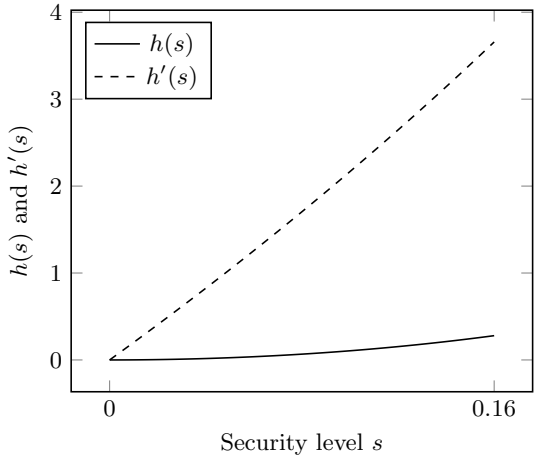

Fig. 1. The security-cost function $h(s)$ and its first derivative $h'(s)$ used in the numerical illustrations.

Figure 2 shows the honest users' equilibrium security level $s^*(M)$ as a function of M. Furthermore, it also shows the honest and malicious users' utilities u and v for these equilibrium security levels (i.e., utilities given that there are M malicious users and the honest users choose $s^*(M)$). We see that – as established by Theorem 2 – the equilibrium security level is a strictly decreasing function of the number of malicious users. Moreover, we see that the utilities are also strictly decreasing. For the honest users, this is easily explained by the

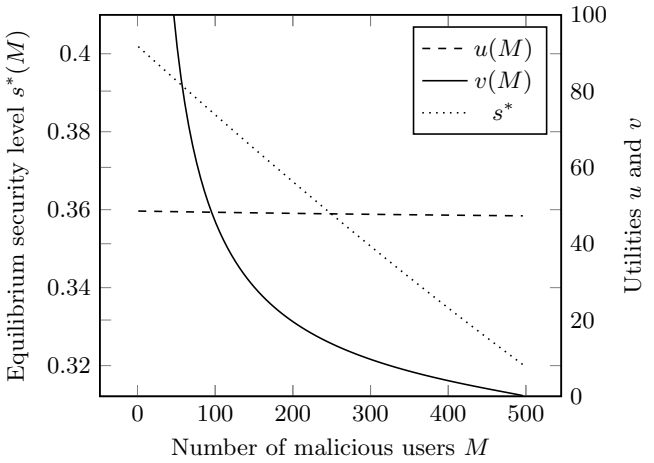

Fig. 2. The equilibrium security level s^* and the resulting utilities u and v for honest and malicious users as functions of the number of malicious users M. Please note the different scalings of the vertical axes.

decrease in both the individual security level and the number of honest users who contribute. For the malicious users, the utility decreases because the gain from decreasing security levels is outweighed by the increasing competition between more and more malicious users. Finally, we can see that the equilibrium number of malicious users is at $M = 96$ since the users have incentive to become malicious for lower values of M (i.e., utility for being malicious is much higher) and they have incentive to become honest for higher values of M.

Figures 3 and 4 show respectively the security level s^* and the number of malicious users $\hat{M}$ in Nash equilibrium as functions of the potential loss L and interdependence q_∞. Note that the values s^* and $\hat{M}$ are well defined because the equilibrium exists uniquely for each parameter combination (q_∞, L) in this example. As expected, we see that higher potential losses lead to higher security levels since honest users have more incentive to invest in security, and they lead to higher numbers of malicious users since committing cybercrime becomes more profitable. On the other hand, stronger interdependence leads to lower security levels since the honest users' breach probabilities becomes less dependent on their own security levels, which disincentivizes investing or making an effort. Conversely, stronger interdependence leads to higher numbers of malicious users since propagating security breaches becomes easier, which makes cybercrime more profitable.

Figure 5 shows the security level s^* and the number of malicious users $\hat{M}$ in Nash equilibrium as functions of the probability μ of a malicious user getting caught. Note that the values s^* and $\hat{M}$ are again well defined because the equilibrium exists uniquely for each parameter value μ in this example. As expected, we see that a higher probability of getting caught disincentivizes users

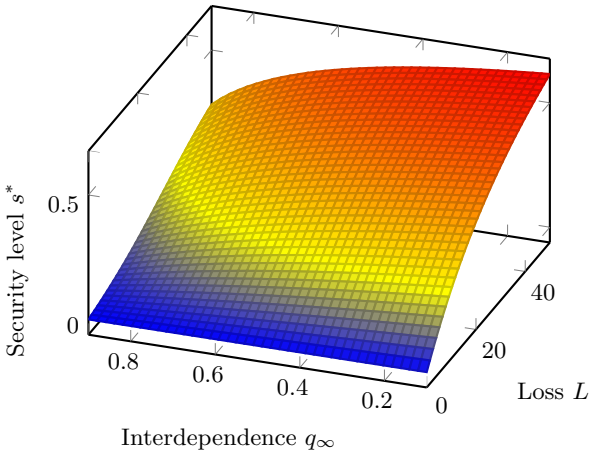

Fig. 3. Security level s^* in Nash equilibrium as a function of potential loss L and interdependence q_∞.

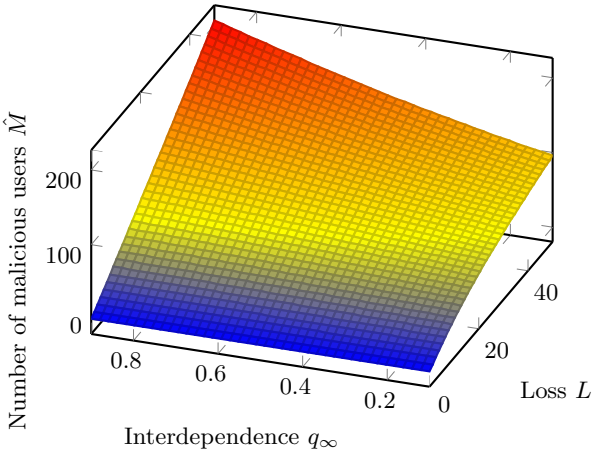

Fig. 4. Number of malicious users $\hat{M}$ in Nash equilibrium as a function of potential loss L and interdependence q_∞.

from engaging in cybercrime and reduces the number of malicious users. On the other hand, the probability of getting caught has an almost negligible effect on the honest users security level.

6 Conclusion

We studied users' incentives to become cybercriminals in networks where the users' security is interdependent. Based on a well-known model of interdependent security, we introduced a game-theoretic model, in which each user can

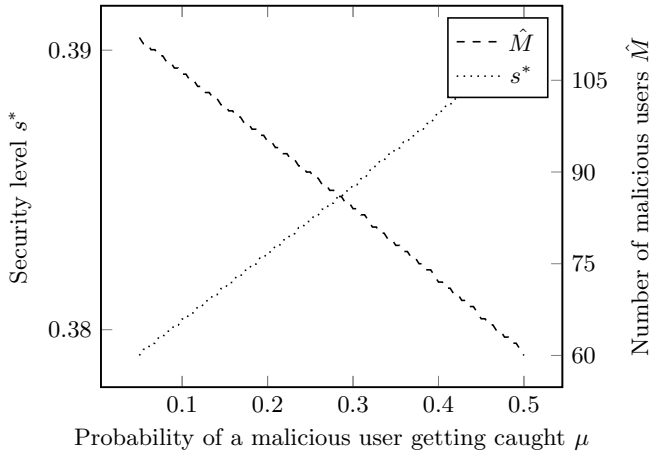

Fig. 5. Security level s^* and number of malicious users $\hat{M}$ in Nash equilibrium as functions of the probability μ of a malicious user getting caught.

choose to be either honest or malicious (i.e., cybercriminal). First, we showed how to compute security-breach probabilities in this model for large-scale networks. Then, we showed that if users are homogeneous, all honest users select the same security level in an equilibrium, and this level exists uniquely for a fixed number of malicious users. Furthermore, we found that this security level is a strictly decreasing function of the number of malicious users, which means that the overall security of a network drops rapidly as more and more users choose to be malicious. Equivalently, the number of malicious users is a strictly decreasing function of the honest users' security levels, which is not surprising: as users become less secure and easier to exploit, choosing to be malicious and taking advantage of them becomes more profitable. Finally, we found that the game always has a Nash equilibrium.

There are multiple directions for extending our current work. Firstly, we plan to study heterogeneous users, who may have different initial wealth, probability of getting caught, etc. While our current model, which assumes homogeneous users, is very useful for studying how the users' choices are affected by changing various parameters, a heterogeneous-user model will enable us to study the differences between individual users' choices. We conjecture that even though users may choose different security levels, their equilibrium security levels will decrease as the number of malicious users increases. Secondly, we plan to extend our current model by considering cyber-insurance, that is, by allowing users to purchase cyber-insurance policies in addition to investing in security. In practice, the adoption of cyber-insurance is growing rapidly as the market size is estimated to increase from $2.5 billion in 2015 to $7.5 billion in 2020 [28]. Consequently, users' security choices are increasingly affected by the availability of cyber-insurance. We conjecture that increasing the number of malicious users will

have an opposite effect on cyber-insurance as compared to security investments: decreasing security levels will result in increasing adoption of cyber-insurance.

Acknowledgment This work was supported in part by FORCES (Foundations Of Resilient CybEr-Physical Systems), which receives support from the National Science Foundation (NSF award numbers CNS-1238959, CNS-1238962, CNS-1239054, CNS-1239166).

References

1. Acemoglu, D., Malekian, A., Ozdaglar, A.: Network security and contagion. Working Paper 19174, National Bureau of Economic Research (June 2013), `http://www.nber.org/papers/w19174`
2. Anderson, R., Moore, T.: The economics of information security. Science 314(5799), 610–613 (October 2006)
3. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J., Levi, M., Moore, T., Savage, S.: Measuring the cost of cybercrime. In: The economics of information security and privacy, pp. 265–300. Springer (2013)
4. Asghari, H., Van Eeten, M., Arnbak, A., Van Eijk, N.: Security economics in the HTTPS value chain. In: 12th Workshop on the Economics of Information Security (WEIS) (2013)
5. Aspnes, J., Chang, K., Yampolskiy, A.: Inoculation strategies for victims of viruses and the sum-of-squares partition problem. In: Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA). pp. 43–52. SIAM (2005)
6. Aspnes, J., Chang, K., Yampolskiy, A.: Inoculation strategies for victims of viruses and the sum-of-squares partition problem. Journal of Computer and System Sciences 72(6), 1077–1093 (2006)
7. Fultz, N., Grossklags, J.: Blue versus red: Towards a model of distributed security attacks. In: Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC), pp. 167–183. Springer (2009)
8. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: A game-theoretic analysis of information security games. In: Proceedings of the 17th International Conference on World Wide Web (WWW). pp. 209–218. ACM (2008)
9. Hausken, K.: Income, interdependence, and substitution effects affecting incentives for security investment. Journal of Accounting and Public Policy 25(6), 629–665 (2006)
10. Heal, G., Kunreuther, H.: Interdependent security: A general model. Tech. Rep. Working Paper 10706, National Bureau of Economic Research (2004)
11. Heal, G., Kunreuther, H.: Modeling interdependent risks. Risk Analysis 27(3), 621–634 (2007)
12. Honeyman, P., Schwartz, G., Assche, A.V.: Interdependence of reliability and security. In: 6th Workshop on the Economics of Information Security (WEIS) (2007)
13. Johnson, B., Grossklags, J., Christin, N., Chuang, J.: Uncertainty in interdependent security games. In: Proceedings of the 1st International Conference on Decision and Game Theory for Security (GameSec). pp. 234–244. Springer (2010)
14. Johnson, B., Laszka, A., Grossklags, J.: The complexity of estimating systematic risk in networks. In: Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF). pp. 325–336 (2014)

15. Khouzani, M.R., Sen, S., Shroff, N.B.: An economic analysis of regulating security investments in the internet. In: Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM). pp. 818–826. IEEE (2013)
16. Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., Jones, K.: A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection 9, 52–80 (2015)
17. Konradt, C., Schilling, A., Werners, B.: Phishing: An economic analysis of cybercrime perpetrators. Computers & Security 58, 39 – 46 (2016), http://www.sciencedirect.com/science/article/pii/S0167404815001844
18. Kraemer-Mbula, E., Tang, P., Rush, H.: The cybercrime ecosystem: Online innovation in the shadows? Technological Forecasting and Social Change 80(3), 541 – 555 (2013), http://www.sciencedirect.com/science/article/pii/S0040162512001710, future-Oriented Technology Analysis
19. Kunreuther, H., Heal, G.: Interdependent security. Journal of Risk and Uncertainty 26(2-3), 231–249 (2003)
20. Laszka, A., Felegyhazi, M., Buttyan, L.: A survey of interdependent information security games. ACM Computing Surveys 47(2), 23:1–23:38 (Aug 2014)
21. Laszka, A., Johnson, B., Grossklags, J., Felegyhazi, M.: Estimating systematic risk in real-world networks. In: Proceedings of the 18th International Conference on Financial Cryptography and Data Security (FC). pp. 417–435 (2014)
22. Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., et al.: Click trajectories: End-to-end analysis of the spam value chain. In: Proceedings of the 32nd IEEE Symposium on Security and Privacy (S&P). pp. 431–446. IEEE (2011)
23. Moscibroda, T., Schmid, S., Wattenhofer, R.: When selfish meets evil: Byzantine players in a virus inoculation game. In: Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing (PODC). pp. 35–44. ACM (2006)
24. Öğüt, H., Menon, N., Raghunathan, S.: Cyber insurance and IT security investment: Impact of interdependence risk. In: 4th Workshop on the Economics of Information Security (WEIS) (2005)
25. Öğüt, H., Raghunathan, S., Menon, N.: Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis 31(3), 497–512 (2011)
26. Olson, M.: The rise and decline of nations: Economic growth, stagflation, and social rigidities. Yale University Press (2008)
27. Olson, M.: The logic of collective action, vol. 124. Harvard University Press (2009)
28. PricewaterhouseCoopers: Insurance 2020 & beyond: Reaping the dividends of cyber resilience. http://www.pwc.com/insurance (2015), accessed: June 16th, 2016
29. Schwartz, G.A., Sastry, S.S.: Cyber-insurance framework for large scale interdependent networks. In: Proceedings of the 3rd International Conference on High Confidence Networked Systems (HiCoNS). pp. 145–154. ACM (2014)
30. Symantec: Emerging threat: Dragonfly / Energetic Bear – APT group. *Symantec Connect*, http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group (June 2014), accessed: February 16th, 2016
31. Tullock, G.: The welfare costs of tariffs, monopolies, and theft. Economic Inquiry 5(3), 224–232 (1967)
32. Varian, H.: System reliability and free riding. In: Economics of Information Security, pp. 1–15. Springer (2004)