Understanding Cyber-risk By Investigating the Behaviour of Defender and Threat Agent Organisations

Why a Complex Adaptive Systems Perspective Contributes to Further Understanding Cyber-risk

Rick Slangen, Michel J.G van Eeten, Wolter Pieters, Emile J.L. Chappin

Abstract

Cyber-attacks have become inevitable in modern day society. Therefore, the occurrence of cyber-attacks is increasingly seen as a risk in an organisation. This has increased the interest in risk analysis methods since these try to better understand this so-called cyber-risk. However, these methods fall short since they do not sufficiently take into account the behaviour of defender organisations, which can be public or private organisations, and the behaviour of threat agent organisations, those who perform cyber-attacks. These are important determinants of cyber-risk. In this paper, a complex adaptive systems (CAS) perspective is used for cyber-risk analysis. Performing cyber-risk analysis through this perspective creates increased understanding in the relationship between the defender and threat agent behaviour and cyber-risk. In order to generate these insights, an agent-based model (ABM) is constructed. I will show that new insights, regarding the cyber-risk that is carried by a defender organisation, are generated by this novel combination of cyber-risk and CAS. The novelty of these insights must encourage scholars in the field of cyber-risk to embrace the CAS-perspective in cyber-risk analysis so that the understanding of cyber-risk can be further increased.

Keywords: Cyber-risk, Successful Cyber-attack Frequency (Distributions), Complex Adaptive Systems, Agent-based Modelling, Experimental Research

Delft University of Technology
Faculty of Technology, Policy & Management
Delft, the Netherlands
20 June 2016
1 Introduction

In recent years, the importance of information technology (IT) has rapidly increased both for public and private organisations. This has attracted threat agents to perform more and increasingly severe cyber-attacks on these organisations [Gandhi et al., 2011]. Despite the rapid increase in cyber-security spending, organisations are not saved from cyber-attacks [Blakley et al., 2001, Helbing, 2013]. When an organisation is struck by a cyber-attack, how often and how severe, is however uncertain. Therefore, an organisation must treat the possibility of incurring a cyber-attack, with hazardous consequences, as a cyber-risk [Longstaff et al., 2000]. This has led to an increase cyber-risk analysis methods in the recent years, see for instance Garg et al. [2003], Gordon et al. [2003] Lenstra and Voss [2004], Årnes et al. [2006], Innerhofer-Oberperfler and Breu [2006], Jones [2006], Morali et al. [2008], Kundur et al. [2011], Lagazio et al. [2014] and Libicki et al. [2015].

These methods mainly focus on analysing the vulnerabilities of an organisation and to what extent a threat agent can cause harm by exploiting these vulnerabilities through a cyber-attack. A shortcoming of such a form of cyber-risk analysis is that it neglects that the cyber-risk of a defender organisation is partly determined by the behaviour of a multitude of defenders and threat agents. Such behaviour in the area of cyber-risk often concerns that each individual defender and threat agent continuously adapt its own behaviour to that of other defenders and threat agents [Cox Jr, 2009], resulting in a so-called complex adaptive system (CAS). In order to add to the current scientific understanding in the area of cyber-risk, we will develop an agent-based model (ABM) is capable of establishing relationships between the behaviour of defender and threat agent organisations and the cyber-risk that is carried by a defender organisation.

The rest of the paper is outlined as follows. In section 2, we will further elaborate on the definition of cyber-risk, since literature does not provide a unified definition for this. Moreover, it gives a few important inputs and outputs for the ABM. In section 3, We elaborate further on CAS, argue why this is a suitable perspective for analysing cyber-risk and show that ABM is a modelling paradigm often used to investigate a CAS. This will also show why ABM is used in this research for unravelling the relationships between defender and threat agent organisation behaviour and the cyber-risk carried by a defender organisation. The assumptions, on the behaviour of defenders and threat agents, and a few vital notes on the exact mechanics behind the ABM will be discussed in section 4. Since it is unknown for some of these assumptions about the defender and threat agent behaviour whether they hold in practice, a set of assumptions will be subject to experimentation. This experimentation will prove vital for generating understanding on how defender and threat agent organisation behaviour relate to the cyber-risk of a defender. The experimental design is discussed in section 5, after which the results of the experiments are discussed in section 6. As with any model, these results must be validated, which will be done in section 7. This paper closes in section 8 with discussing the main conclusions, limitations, contributions and suggestions for further research.
2 On the Definition of Cyber-risk

Cyber-risk, and risk in general, is ambiguously defined in literature. If one looks at the risk analysis methods to which has been referred in section 1, they often define cyber-risk in a slightly different manner. We will not discuss all these different definitions of cyber-risk, as this is not of primary interest. Instead, a cyber-risk definition is used that will fit the purpose of this research. The definition stems from the Factor Analysis Information Risk (FAIR-)framework, described in Jones [2006] and in the Risk Taxonomy defined by The Open Group [Cebula and Young, 2010]. This definition will be useful for constructing the ABM in a further stage of this research.

The attractiveness of the FAIR-framework is that it decomposes cyber-risk into more ill-defined concepts. In the first decomposition, cyber-risk is defined as the resultant of two concepts: the successful cyber-attack probability/frequency and the potential loss magnitude that a defender can experience from a successful cyber-attack. The former concept must be sharpened. Only considering the successful cyber-attack probability raises the question to which probability it refers. It is not clear whether this probability refers to the probability that a defender incurs 1, 10, 100, or in general, \( N_s \) successful cyber-attacks. The successful cyber-attack frequency is neither concrete enough. It is not clear whether it refers to, for example, the expected, median or maximum expected successful cyber-attack frequency.

The successful cyber-attack probability and frequency should be combined in one measure in order to make the cyber-risk definition more exact. This is done by a probability distribution that describes the probability that a defender incurs a certain successful cyber-attack frequency. This is referred to as the successful cyber-attack frequency distribution. To be completely exact, this distribution concerns a certain time interval. After all, the expected successful cyber-attack frequency incurred by a defender in a 10 year time interval, is likely to be higher than for a 1 year time interval. The foregoing results in the decomposition of cyber-risk as is shown in the second layer of the risk decomposition tree, exhibited in Figure 1.

The successful cyber-attack distribution will be further decomposed into more granular concepts. As can be seen from Figure 1, the successful cyber-attack distribution is decomposed into the cyber-attack frequency distribution and the vulnerability. The cyber-attack frequency distribution is the probability distribution of the cyber-attack frequency which concerns both successful and unsuccessful attacks. If a cyber-attack is successful depends on whether a vulnerability within the defender organisation is exploited by a threat. If this is the case, a cyber-attack becomes a successful cyber-attack [Haimes, 2006, Jerman-Blazić et al., 2008, Aven, 2011]. When a threat agent performs a successful cyber-attack, it is able to gain from the cyber-attack which also leads to losses for the defender organisation that is successfully attacked.

Whether a vulnerability is exploited is the resultant of how well a defender is able to resist cyber-attacks and how capable a threat agent is in performing these attacks. These are respectively referred to as the control strength of a defender organisation and the threat capability of a threat agent organisation. Both are multi-dimensional concepts that depend on various phenomena, such as how much resources defenders and threat agents spend on respectively cybersecurity and attacking, and the efficiency of how they use these resources. We
will not further dive into the exact definition of both concepts. Neither will be
determined, for now, how the control strength and threat capability relate to
the defender’s vulnerability. We rather discuss the intuition of this decompo-
sition. Suppose that a defender is poorly defended. When the threat agents
are not capable, it is unlikely that a cyber-attack becomes a successful cyber-
attack. Despite the weakness of the defender, the threat agent does not have the
capability to exploit the defender’s vulnerability. When the threat capability
increases, the likelihood that a cyber-attack becomes successful increases, unless
the defender also builds up more strength to prevent this from happening.

Figure 1. Definition of cyber-risk according to the Factor Analysis Information
Risk (FAIR)-framework.

3 Cyber-risk, Complex Adaptive Systems and
Agent-based Modelling

In section 1, it has been emphasised that the focus of this research concerns
the relationship between defender and threat and behaviour and the cyber-risk
that is carried by a defender organisation. It has also been mentioned that cur-
rent risk analysis methods hardly treat defender and threat agent behaviour.
Recently, a few risk analysis methods incorporate some kind of defender and
threat agent behaviour in the form of game theory [Cox Jr, 2009, Fielder et al.,
2014]. Yet, game theory is a very simplified way of formalising defender and
threat agent behaviour for only a few defenders and threat agents. This model
simplification does not correspond to the real-world practice in which multiple
threat agents can choose to attack a defender organisation from a multitude of
defender organisations. Moreover, the stylised character of game theory only
allows for analysing the cyber-risk of a defender organisation in the near future.
This does however not allow to investigate how the cyber-risk of a defender
organisation develops on the longer term. This is a pitfall, since cyber-risk not
only concerns the short term but also the long term.

Understanding Cyber-risk by Investigating the Behaviour of Defender and
Threat Agent Organisations
The model therefore asks for a ‘systems perspective’, in which a relatively large number of defender organisations and threat agent organisations are considered. Which defenders and threat agents must be incorporated is a subjective process and is determined which part of reality one wants to investigate [Foster-Fishman et al., 2007]. Modelling this part of reality requires simplification but not as rigidly like is done in the area of game theory. This leads to a model that is a more feasible representation of reality. This part of reality is often ‘enduring’ in a systems perspective [Ryan, 2008], meaning that the investigated part of reality will likely exist a considerable amount of time. Translating this to the area of cyber-risk, a reality must be modelled in which the same set of defender organisations and threat agent organisations interact in the course of the whole study period.

In order to make the model better correspond to reality, it must take into account the adaptive nature of defender and threat agent organisations. That is, the behaviour of each defender and threat agent is influenced, and thus influences, the behaviour of other defenders and threat agents. This corresponds to the main thought of the earlier mentioned game theory. The notion of adaptive behaviour must thus be combined with the systems perspective, in which many defenders and threat agents interact for a considerable amount of time. The adaptive behaviour of many agents results, through a complex sequence of action and reaction, in unpredictable system outcomes. In the light of this research, this means that it is hard to see the relationship between the behaviour of defender and threat organisations and the cyber-risk carried by a defender. Systems in which many agents show adaptive behaviour are therefore often called complex adaptive systems (CAS) [Perrow, 1999, Cilliers and Spurrett, 1999, Foster-Fishman et al., 2007].

A model paradigm that is able to investigate a CAS is the agent-based modelling (ABM) paradigm [van Dam et al., 2012]. ABM is a quantitative simulation method that simulates the consequences of adaptive behaviour of multiple agents on the overall system output, also for situations in which the adaptive behaviour has long term effects. In other disciplines, such as macro-economics and energy policy, the CAS-perspective has already been acknowledged, see respectively Standish and Keen [2004] and Chappin [2011]. They also used ABM for generating understanding about the CAS that they investigated. Therefore, this research will also construct an ABM in order to generate understanding about the relationship between defender and threat agent behaviour and the cyber-risk that a defender organisation carries.

### 4 The Implemented Agent-based Model

This section discusses the implementation of the ABM. In subsection 4.1, a high level model narrative is presented that yields a set of assumptions. These assumptions concern the behaviour of defender and threat agent organisation and must be seen as a description of how a system with defender organisations and threat organisations may look like. Some of these high-level assumptions are further specified in an unambiguous manner in subsection 4.2. This is needed in order to make simulation through ABM possible. The latter subsection will also address how some parts of the ABM are initialised, i.e. the initial values of the ABM input variables. This is also a requirement for making simulation
possible. The purpose of this section is to help the reader to become familiar with how the implemented ABM works.

## 4.1 Conceptualisation of the Agent-based Model

As has been indicated in section 3 an ABM is based on assumptions, mainly concerning the behaviour of the incorporated agents in the model. The assumptions concerning the behaviour of threat agent organisations and defenders are shown in Figure 2. The rest of this section gives a brief model narrative, a common way to conceptualise an ABM [van Dam et al., 2012], on which these assumptions are based.

Consider a homogeneous group of defender organisations with respect to the asset value that may be at risk curing a cyber-attack. In other words, the potential loss magnitude of the incorporated defender organisations is similar. We furthermore that, when a threat agent organisations performs a successful cyber-attack, the potential gain for the threat agent equals the potential loss for the defender organisation. This assumption is commonly used in the area of cyber-security [Zhu and Başar, 2011, Esmalifalak et al., 2013]. The potential gain of a cyber-attack is thus not a decision variable for the threat agents considering when, whether and which defender agent it shall attack. After all, the potential gain for the threat agent is equal, regardless of the defender agent it decides to attack.

The decision regarding when, whether and whom to attack is then only based on how well a defender is defended. In other words, this decision is based on the control strength of the defender organisations under investigation. This is similar to the ‘weakest link’ principle, in which is assumed that a threat agent attacks the weakest (part of) a defender [Arce, 2003, Böhme and Moore, 2010, Kundur et al., 2010, Pieters, 2013]. It is assumed that a threat agent always attacks the defender organisation with the lowest control strength (Assumption 1-2). However, a threat agent is expected that it will only attack a defender organisation when it can lift the vulnerability of a defender. Or, as is sketched in Figure 1, that its threat capability is high enough to overcome the control strength of the defender organisation (Assumption 3).

It may however be that some defenders have an equal control strength. In the ABM it is assumed that a threat agent has the means to attack only one defender organisation at the same time. If multiple defender organisations have the same control strength and when the threat agent has a threat capability that is high enough to break through this control strength, the threat agent is indifferent in whom to attack (Assumption 4). After all, each defender organisation has a similar potential gain for threat agent organisations. The mechanism as sketched here applies to fully rational threat agents (Assumption 5) who are aware of their own threat capability and the control strength of each defender organisation. Rationality is for a large part determined by the availability of information [Sen, 1990, Arrow, 1991, Grün-Yanoff, 2012].

The previous implies that a threat agent, once reached a sufficiently high threat capability, can keep on performing successful cyber-attacks. This seems not realistic. Threat agents build up their threat capability in a certain environment where defender organisation have implemented vulnerabilities. After a defender is struck by successful cyber-attack, it will soon try to fix this vulnerability. In this adapted realm, a threat agent organisation has to adapt itself
1. Threat agent organisations perform a cyber-attack on the defender organisation with the lowest control strength.

2. The potential gain of a cyber-attack does not influence the threat agents in their choice regarding which defender to attack at what moment.

3. Threat agent organisations only perform cyber-attacks on a defender organisation if their own threat capability exceeds the control strength of this defender organisation.

4. A threat-agent can only attack one defender organisation at the same time. If multiple defender organisations have the same control strength, the threat agent organisation attacks only one of these defender organisations.

5. Only a fully rational threat agent organisation always attacks a defender organisation with the lowest control strength of all defender organisations which is also smaller than the threat agent’s threat capability.

6. The threat capability of a threat agent is reset to its lowest possible level after it performs a successful cyber-attack.

7. The intrinsic skill and resource level determine the pace at which a threat agent organisation expects to increase its threat capability. The intrinsic skill and resource level is not equal for all threat agent organisations.

8. For a certain period after the most recent cyber-attack, defender organisations use a reactive defence strategy instead of a default defence strategy. The latter is followed if no successful cyber-attack has recently been incurred.

9. The investment level of a defender determines the pace at which a defender organisation expects to increase its control strength. The investment level is not equal for all defender organisations.

10. Each defender organisations invests the same, high amount of resources in their reactive defence strategy.

Figure 2. Overview of assumptions concerning agent behaviour in the ABM.

too. It thus needs to get familiar in this changed environment. Therefore, after performing a successful cyber-attack, the threat capability of a threat agent is reset to its lowest level (Assumption 6). This is a similar mechanism as is applied in Pieters et al. [2014] and Pieters and Davarynejad [2015].

The pace at which threat agents become more capable different amongst threat agents [McQueen et al., 2006]. This pace is determined by, the what we
4.2 Initialising the Agent-based Model

Although the model narrative in subsection 4.1 and the corresponding model assumptions in Figure 2 sketch the general working of the ABM, it is at some point not specific enough to perform the model simulation. The model is specified in an unambiguous way by describing the most important elements of the ABM in detail. This entails how the model is initialised in the first place, i.e. the starting values of the model input variables, see subsubsection 4.2.1. Furthermore, the details of how the default and reactive defence strategies and the threat capability learning strategy are implemented are given in subsubsection 4.2.2.

4.2.1 Initialising the Agent-based Model

A first important subject is the number of defender organisations and threat agent organisations that are incorporated in the ABM. We assume that a threat agent a priori selects a certain type of defender organisations to attack, such as big financial service providers. These kinds of organisations contain a lot of potential gain for threat agent organisations. In fact, investigating for example a population of big European banks, is likely to result in a set of defenders in which each of the defender contains a similar gain for the threat agent organisations.

Since there are not that many of these big organisations, A relatively small number of defender organisations are considered. This number may however not be too small since a CAS requires that a multitude of agents are incorporated in the ABM. Therefore, 30 defender organisations are incorporated in the model. How many threat agent organisations are interested, and able, to attack these kinds of big organisations is difficult to say. There are no empirical data about this. In this research, 90 threat agent organisations are incorporated in the model.

A second important consideration before starting any simulation is the length
of the study period. This study period will be quite long. As has been argued in section 3, the study period must take a long term into account since this allows to investigate possible long term consequences of agent behaviour or whether certain trends can be observed with respect to the cyber-risk of a defender organisation. Therefore a study period of 3 years is considered. For convenience, a month consists of 30 days, so that the study period amounts to 1080 days.

Another element of the ABM that must be specified is the time step used within the simulation. The variables in the model, such as the control strength of a defender, are periodically updated. Taking a too short period into account will make the simulation too time consuming from a computational point of view. A too great time step makes the agent not very responsive. For instance, if the time step would equal 1 month, this would mean that an agent starts adapting a month after the decision made by other agents. This is unrealistic. A time step of 1 day will be considered so that the variables in the model are updated on a daily basis.

So far, so-called global variables have been initialised. In Table 1, a detailed overview is given about the possible values the variables can take which are carried by the agents and how these variables are initialised. The table shows that both the control strength and the threat capability are defined as discrete scales with levels 1, 2, ..., 10. Since there are no data available about the defenders’ control strength, this kind of abstraction must be used. subsection 4.2.2 will show that this abstraction is very convenient for defining the defence strategies and the threat capability learning strategies. The investment level of defenders and the intrinsic skill and resource level of the threat agents will be distinguished in three levels: a low, medium and high level. How many of the defender organisations will carry which investment level is further discussed when designing the experiment, see section 5. The same holds for how the intrinsic skill and resource levels are distributed over the threat agent organisations. The period that a reactive defence strategy takes is fixed and equal for all defenders. With the exact period will however be experimented, see section 5. The same holds for the degree of rationality of threat agent organisations.

<table>
<thead>
<tr>
<th>Control strength</th>
<th>Default defence strategy</th>
<th>Days left reactive strategy</th>
<th>Threat capability</th>
<th>Threat capability learning strategy</th>
<th>Degree of rationality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible values</td>
<td>Low investment</td>
<td>Fixed period</td>
<td>Low intrinsic skill</td>
<td>Fixed %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium investment</td>
<td>equal for all</td>
<td>Medium intrinsic skill</td>
<td>equal for all</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High investment</td>
<td>defenders</td>
<td>High intrinsic skill</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial values</th>
<th>Assign initial control strength</th>
<th>Assign threat capability of 1 to all threat agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender organisations</td>
<td>Threat agent organisations</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Tabular overview of input variables carried by the agents and its possible values.
4.2 Initialising the Agent-based Model

4.2.2 Detailed Mechanics of Agents’ Behaviour

The remaining elements of the ABM that are still ambiguously specified are the default and reactive defence strategies of the defender organisations and the threat capability learning strategy of the threat agents. This subsection will explain how these strategies are implemented in the ABM.

The mechanism that is used to steer the movement of the control strength over time is a Markov chain. Detailed background about Markov chains can be found in Ross [2014]. First, consider the default and reactive defence strategies. In essence, the Markov chain in this research contains the probability that the control strength either decreases with one unit, stays the same or increases each time step, so each day. These are the so-called transition probabilities. In order to make the control strength not too volatile, the control strength can experience a maximum change of one unit each day. When the investment level of a defender organisation increases, the probability that the control strength increases with a unit increases too. Automatically, the probability that the control strength stays the same or decreases with one unit diminishes then.

Specifying the defence strategies by means of a Markov implicitly implements three important phenomena. First of all, although one expects that a defender with a higher investment has a higher probability of being at a higher control strength, this is not necessarily the case. This builds in some realistic insecurity about the effectiveness of investing more in cyber-security [Rue et al., 2007]. Secondly, a Markov chain also implements the realistic situation in which a lower investment level increases the likelihood of a deteriorating control strength [Zhang-Kennedy et al., 2014]. Lastly, a Markov chain builds in some volatility in the control strength, resembling that the exact control strength is a simplified metric of which the value is not exactly known. After all, whether the control strength of a defender equals for example 1, 2 or 3 is uncertain. That the control strength of this defender lies somewhere around these values is however quite certain, since this organisation can be seen as a weak defender.

Based on the foregoing, the Markov chains as shown in Table 2, Table 3 and Table 4 are assigned to defender organisations with respectively a low, medium and high investment default defence strategy. The Markov chains show the transition probabilities from a certain control strength at time $t$ to a different control strength at time $t + 1$. The Markov chain corresponding to the reactive defence strategy is shown in Table 5. One can see that the transition probabilities in this table are specified in such a way that the likelihood of reaching and staying at a high control strength is fairly high. This is the consequence of heavy investments made during the reactive strategy, see Assumption 8.

The threat capability learning strategy is defined along the same lines as the default defence strategies, thus also through Markov chains. In fact, the Markov chains that apply to threat agent organisations with a low, medium and high intrinsic skill and resource level equal those of the defender organisations with a low, medium and high investment level in the default defence strategy. Thus, these Markov chains correspond to those shown in Table 2, Table 3 and Table 4.
### 4.2 Initialising the Agent-based Model

<table>
<thead>
<tr>
<th>Control strength at time $t+1$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.6</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
<td>0.2</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Table 2. Markov chain representing the default defence strategy of defenders with investment level 1 and threat agents with intrinsic skill and resource level 1.

<table>
<thead>
<tr>
<th>Control strength at time $t+1$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.5</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Table 3. Markov chain representing the default defence strategy of defenders with investment level 2 and threat agents with intrinsic skill and resource level 2.

<table>
<thead>
<tr>
<th>Control strength at time $t+1$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.4</td>
<td>0.6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.3</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0.3</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.4</td>
<td>0.3</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Table 4. Markov chain representing the default defence strategy of defenders with investment level 3 and threat agents with intrinsic skill and resource level 3.

Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations
Experimental Design

Some assumptions concerning the behavioural rules of the threat agents are not yet exactly defined. As can be derived from Table 1 these concern:

1. how investment levels are distributed over the defender organisations, i.e. which defender organisations follow which default defence strategy;
2. how intrinsic skill and resource levels are distributed over the threat agent organisations, i.e. which threat agent organisations follow which threat capability learning strategy;
3. the period length of the reactive strategy;
4. the rationality of the threat agents.

The input values that describe these phenomena, such as rationality, are unknown. This is often the case with agent based models in which phenomena are incorporated that do not follow fixed regularities such as physical laws [Louie and Carley, 2008]. We will therefore experiment with the input values describing these phenomena.

How the experiment looks like is shown in subsection 5.2. But before that, some important notes about the output variables of the experiment in subsection 5.1 will be given.

5.1 Experimentation and Output Variables

In the course of this paper, it has been made clear that the successful cyber-attack frequency distribution is the main variable of interest when investigating cyber-risk in this research. After all, the other cyber-risk pillar, the potential loss magnitude of defenders, is held similar amongst defenders throughout the simulation. This results in a situation where threat agent organisations do not take the potential gain of a cyber-attack into account in their attack strategy.

In section 2, the successful cyber-attack frequency distribution concerned an individual defender. However, studying the successful cyber-attack frequency distribution of each single defender does not make sense. One must study under

<table>
<thead>
<tr>
<th>Control strength at time $t + 1$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control strength at time $t$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0.2</td>
<td>0.8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.1</td>
<td>0.2</td>
<td>0.7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0.2</td>
<td>0.2</td>
<td>0.6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.2</td>
<td>0.6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.3</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.4</td>
<td>0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.5</td>
<td>0.3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.5</td>
<td>0.3</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.6</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

Table 5. Markov chain representing the reactive defence strategy
which kinds of situations or which kinds of defenders have a certain successful cyber-attack frequency distributions. Doing this would allow to make generalised statements about the successful cyber-attack frequency distribution, and thus the cyber-risk of a certain type of defender organisation or under certain circumstances. The successful cyber-attack frequency distribution of a defender is therefore studied conditional on the characteristics of the defender and threat agents that respectively incurs and perform the successful cyber-attack. These specifically concern:

1. the control strength of the successfully attacked defender;

2. the threat capability of the threat agents that perform the successful cyber-attack incurred by the defender;

3. whether a defender is successfully attacked while performing a default or reactive defence strategy;

4. if successfully attacked during a reactive defence strategy, in which phase does this happen.

It must be emphasised that this distribution is an empirical distribution, generated by the collection of simulations that are performed by the experiment. Each single experiment records the successful cyber-attack frequency of defenders, with for example a certain control strength, after a certain time period after the start of the simulation. Multiple simulation runs generate multiple successful cyber-attack frequencies for this group of defenders, together forming an empirical successful cyber-attack frequency distribution that applies for this type of defenders. These successful cyber-attack frequencies are not only constructed at the end of each simulation run, so not only after 3 years. Since for each simulation run the successful cyber-attack frequencies are counted at 3 months, 6 months and 1 year after the start of the simulation, similar distributions can be made that hold for 3 months, 6 months and 1 year after the start of the simulation. As mentioned in section 2, the successful cyber-attack frequency distribution is likely to differ when a different time interval is concerned. Constructing these successful cyber-attack frequency distributions at different points in time allows to inspect these differences and whether certain trends can be observed in these distributions in the course of the simulation runs.

5.2 Experimental Setup

In the introduction of this section, four variables are mentioned that will be subject of experimentation. These variables touch upon the behaviour of defender and threat agent organisations. The empirical successful cyber-attack frequency distributions that have been discussed in subsection 5.1 will be generated under various values of those experimental variables. Hence, successful cyber-attack frequencies are generated under various combinations of defender and threat agent organisations. This generated different successful cyber-attack frequency distributions under different forms of defender and threat agent organisation behaviour. This allows to establish the relationship between these behaviours and the successful cyber-attack frequency distributions. And thus, this makes
<table>
<thead>
<tr>
<th>Level</th>
<th>Share of population with certain default defence strategy</th>
<th>Level</th>
<th>Share of population with certain intrinsic skill and resource level</th>
<th>Level</th>
<th>Period length reactive defence strategy</th>
<th>Level</th>
<th>Degree of rationality</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Number of days</td>
</tr>
<tr>
<td>1</td>
<td>1/3</td>
<td>1/3</td>
<td>1/3</td>
<td>1/3</td>
<td>1/3</td>
<td>1/3</td>
<td>10 days</td>
</tr>
<tr>
<td>2</td>
<td>2/3</td>
<td>1/6</td>
<td>1/6</td>
<td>2/3</td>
<td>1/6</td>
<td>1/6</td>
<td>30 days</td>
</tr>
<tr>
<td>3</td>
<td>1/6</td>
<td>2/3</td>
<td>1/6</td>
<td>1/6</td>
<td>2/3</td>
<td>1/6</td>
<td>90 days</td>
</tr>
<tr>
<td>4</td>
<td>1/6</td>
<td>1/6</td>
<td>2/3</td>
<td>1/6</td>
<td>1/6</td>
<td>2/3</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0%</td>
</tr>
</tbody>
</table>

Table 6. Experimental setup.
it possible to unravel the relationship between defender and threat agent behaviour and the cyber-risk carried by a defender organisation in a system where defender organisations have similar potential loss magnitude and potential gain for the threat agents. The question now is however under which forms of defender and threat agent behaviour, i.e. input values of the experimental variables, the distributions are generated.

Since the defence strategies and the threat capability learning strategies follow stochastic processes, each run may yield different outcomes, even when all inputs in the ABM are equal. This means that, in order to generate more reliable experimental results, multiple simulations must be conducted under the same combination of input values [Bluman, 2012, van Dam et al., 2012]. A certain combination of input variables is often referred to as a configuration. The number of simulation under one configuration must thus be quite large in order to make the results sufficiently reliable. However, a too large number of simulations per configuration will increase the time that it takes to complete the experiment, due to an increased number of computations this requires. This cannibalises on the number of configurations that can be used for experimentation. Therefore, in this research, each configuration will be simulated 50 times.

There is not a single right answer on which configurations of input variables must be used in the experiment. Insights are more easily generated when there is experiments are performed in which the input variables greatly differ. This increases the likelihood that different successful cyber-attack frequency distributions are generated, increasing the chance that clear relationships between defender and threat agent behaviour and successful cyber-attack frequency distributions are unveiled. Especially, picking configurations with quite extreme values, such as full rationality or full irrationality, is then attractive as these configurations differ greatly.

With the previous in mind, the experimental setup is defined according to Table 6. From this setup, one can see that the default defence strategies are distributed in 4 ways over the defender organisations. The same holds for the number of ways in which the threat capability learning strategy is distributed over the threat agent organisations. 3 different time periods of the reactive strategy are taken into account and 6 different degrees of rationality. The total number of configurations with which can be experimented is then $4 \times 4 \times 3 \times 6 = 288$. Since an experiment is performed under each possible configuration, and the number of simulation runs per configuration amounts to 50, the total number of simulations equals 14400.

6 Results of the Experiment

During the experiment an enormous amount of data is collected. In order to keep this paper relatively short, only the relationship between the degree of rationality and the successful cyber-attack frequency (distribution) conditional on the control strength of defender organisation, is discussed, see subsection 6.1. This will yield an interesting first key insight. Other key insights from the experiment that relate to other experimental variables are briefly discussed in subsection 6.2.
6.1 Showcase of Results: Rationality and the Successful Cyber-attack Distribution

In Figure 3, the successful cyber-attack frequency is shown on the y-axis. The control strength of the defenders is shown on the x-axis. Of all the 14400 simulations, this figure shows the successful cyber-attack frequency after 90 days of the simulation. The collection of these successful cyber-attack frequencies are shown in the form of so-called notched box plots, initially constructed by McGill et al. [1978]. How such a notched box-plot must be read is shown in Figure 4. In essence, the notched box plots shown in this paper are rough depictions of empirical successful cyber-attack frequency distributions, conditional on the control strength of the defender organisations. The notched box plots show the median successful cyber-attack frequency incurred by defenders with a particular control strength, to what extent these frequencies are spread and skewed and whether outliers are present in the distribution.

The notched box plots also provide a visual way to statistically test whether the median successful cyber-attack frequency of two distributions differ. As shown in Figure 4, the ‘hourglass shaped’ notches resemble a 95% confidence interval. Comparing these confidence intervals can be done in Figure 3. When the notches of two notched box plots do not overlap, one concludes that, based in a 95% confidence interval, the medians of the distributions, captured by these box plots, significantly differ from each other. This makes it possible to test in Figure 3 whether two median successful cyber-attack frequencies have a significantly different magnitude.

Furthermore, each control strength contains multiple coloured notched box plots, each corresponding to a certain degree of rationality. The legend of Figure 3 shows to which colour which degree of rationality belongs. The figure thus contains the information to compare successful cyber-attack frequencies incurred by defenders with a different control strength under different degrees of rationality.

In Figure 3a it is shown that under a higher degree of rationality, the successful cyber-attack frequency incurred by defender organisations, when having a low control strength, is likely to increase. Compare for example the yellow coloured notched box plots, resembling the successful cyber-attack frequency distributions generated under complete rationality (100% rationality), with their black counterparts, indicating the successful cyber-attack frequency distributions generated under complete irrationality (0% rationality).

This can be explained. Under full rationality, threat agent organisations attack the weakest defender organisation if its threat capability is large enough, see Assumption 1 and 3 in Figure 2. When threat agents become less rational, they are less informed about the control strength of the defenders and their own threat capability, as has been mentioned subsection 4.1. Threat agent organisation then become less able to determine which defender agents are weak enough to successfully attack and which of those are the weakest defenders. This leads to a situation in which threat agents behave less according to model Assumption 1 and 3 so that not always the weakest defender organisation is attacked. In fact, as can be seen from the black notched box plots for the lower control strengths in Figure 3a, the successful cyber-attack frequency incurred by weak defenders is very low under complete irrationality.

The notches in the notched box plots allow for testing whether the me-
6.1 Showcase of Results: Rationality and the Successful Cyber-attack
Distribution

Figure 3. Incurred successful cyber-attacks versus control strengths after 90 days (3 months) under various degrees of rationality of threat agent organisations.

Understand Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations
6.1 Showcase of Results: Rationality and the Successful Cyber-attack

Distribution

Figure 4. Basic visualisation of a notched box plot.

dian successful cyber-attack frequency, incurred by defenders with a low control strength, diminishes significantly when the degree of rationality decreases. The width of the notches are very small, and even hardly visible for the notched box plots shown in Figure 3a. This implies small 95% confidence intervals. It can be seen from Figure 3a that the confidence intervals of the notched box plots at the lower control strengths do not overlap. This gives statistical evidence that the median successful cyber-attack frequency, incurred by defenders with a low control strength, decreases (increases) when the degree of rationality decreases (increases).

In order to investigate the relationship between the degree of rationality and the successful cyber-attack frequency incurred by a defender organisation with a high control strength, Figure 3 zooms in on these higher control strengths. One can see that under high levels of rationality, defender organisations with a high control strength are hardly attacked successfully. In fact, under full rationality, defenders are never successfully attacked when having control strength 8 or higher. This changes when the degree of rationality increases. These defender organisations are more often successfully attacked when threat agent organisations behave less rational. This can be seen by the fact that at the higher control strengths, almost only black notched box plots appear.

The previous can be explained by the fact that, under low levels of rationality, threat agents will tend to attack defenders on a more random basis due to the limited information they have. Hence, defender organisations with a high control strength are more often attacked, thus also successfully, than in a situation with highly rational threat agents since in the latter situation, the weakest defender organisations are attacked. The former is confirmed by the fact that notches of the box plots do not overlap each other at a high control strength level. There is thus statistical evidence that, for defenders with a high control strength, the successful cyber-attack frequency is likely to increase when the degree of rationality decreases. Defenders with a control strength of 10 form an exception since, in the model specification, these cannot be successfully attacked at all.

Until now, this section only discusses the relationship between the degree of rationality and the successful cyber-attack frequency (distribution) incurred by a defender. However, the objective of this research is to generate insights concerning the cyber-risk that a defender carries. A translation thus has to be made from the successful cyber-attack frequency (distribution) towards cyber-risk of

Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations
a defender organisation. For that, recall from subsection 4.1 that for each defender, the potential loss magnitude and the potential gain for the threat agent are similar throughout the study period. This excludes the potential gain as a criterion on which threat agent organisations base their attack strategy, see Assumption 2 in Figure 2. A change in the successful cyber-attack frequency thus occurs while the potential loss magnitude is kept fixed. One of the two pillars that determines the cyber-risk of a defender organisation is thus held constant. Thus, when the probability of incurring a high successful cyber-attack frequency - the other pillar of cyber-risk - increases (decreases), the cyber-risk of a defender organisation automatically increases (decreases) too.

This leads to the first key insight, which establishes how the degree of rationality of threat agent organisations relates to the successful cyber-risk of a defender organisation. This key insight is only applicable in situations where defender organisations have a similar potential loss magnitude and potential gain for threat agent organisations.

**Key insight 1**: When threat agents become less rational, the cyber-risk carried by a weakly protected defender decreases whereas the cyber-risk carried by a well protected defender increases.

This insight is based on the data that are gathered 3 months after the start of the simulation. In Slangen [2016], the data are also collected and visualised in a similar fashion as Figure 3 further on in the study period. To be exact, this is done after 6 months, 1 year and 3 years in the study period. These data show that the patterns, exhibited in Figure 3, persist in the course of time, confirming Key Insight 1 also for the longer term.

## 6.2 Key Insights of the Experiment

As indicated in the introduction of this section, similar analyses as those performed in subsection 6.1 but on the three other experimental variables than the degree of rationality. four more key insights have been generated by these analyses, concerning these three other experimental variables. These insights are deduced on similar figures as shown in Figure 3. The only difference in the figures concerns the values of the experimental variables to which the coloured notched box plots refer. In order to keep this paper concise, the exact outcomes of these analyses are shown in [Slangen, 2016]. These outcomes are not only generated at 3 months after the start of the simulation but also after 6 months, 1 year and 3 years, so that it is checked whether certain outcomes persist over time. This paper limits itself the key insights that are generated during these analyses which are, next to Key Insight 1, summarised in Figure 5. Again, these key insights only hold for the situation in which defender organisations have a similar potential loss magnitude and potential gain for the threat agent organisations.

Key Insight 2, concerning the default defence strategy distribution amongst defender organisations, needs some further attention since this insight does not reflect upon the cyber-risk of an individual defender organisation but rather on the group of defender organisations with a certain control strength. The reason is that it has been impossible to specify these generic results to an individual defender. After all, the groups of defender organisations with a certain
Validation of the Model and Results

1. When threat agents become less rational, the cyber-risk carried by a weakly protected defender decreases whereas the cyber-risk carried by a well protected defender increases.

2. When less defenders decide to heavily invest in cyber-security, the group of defenders with a low control strength carry a higher cyber-risk. When more defenders decide to heavily invest in cyber-security, the number of successful cyber-risk of defenders with a high control strength more or less stays the same.

3. When more threat agents become more skillful and resourceful, this will increase the cyber-risk carried by a defender organisation with a relatively high control strength, not the cyber-risk carried by a defender organisation with a low control strength.

4. When defender organisations follow a reactive strategy with very high investment for a longer period, a defender organisation, that invests quite a lot in cyber-security by default, is likely to see its cyber-risk increase.

5. Longer spells of a reactive strategy are more effective than short spells of a reactive strategy with respect to lowering the cyber-risk that is carried by a defender.

Figure 5. Summary of key insights concerning cyber-risk with respect to a situation where defenders have a similar potential loss magnitude.

control strength themselves depend on how the default defence strategies are distributed over the defender organisations. If for example many defender organisations have a high investment default defence strategy, the group of defender organisations having a higher (lower) control strength will increase (decrease). After all, a lower (higher) investment level likely leads to a (lower) higher control strength, see subsubsection 4.2.2. Yet, how this group size changes is unknown since this is very volatile in the course of the simulation. For instance, when this group of defender organisations has a higher cyber-risk due to an increased number of defenders that invest heavily in cyber-security, this makes it impossible to say anything about the cyber-risk of an individual defender organisation that belongs to this group. During the validation of the model and the results in the next chapter, we try to unravel the implications of a changing distribution of the three default defence strategies on the cyber-risk of an individual defender organisation.

7 Validation of the Model and Results

Validation is the process of checking whether the model that is built is a feasible description of reality [van Dam et al., 2012]. As is the case with any model, validation of the model and the results generated by the model are important.
Validating quantitative models is often done by checking whether the model output corresponds with the real world data [Cameron and Trivedi, 2005]. In this research, this would mean that the successful cyber-attack frequency (distributions), generated by the ABM, would be compared with the real-world data about this successful cyber-attack frequency (distributions). Yet, the ABM models a fictitious system of defenders and threat agent organisation, used as an experimentation tool for generating insights about the cyber-risk of a defender. It is thus not a model that describes an existing system of which empirical data about the successful cyber-attack frequency (distribution) are available.

Other methods than empirical comparison must thus be used for validation. In ABM, expert validation is commonly used [Balci, 1994, Louie and Carley, 2008]. Often this validation concerns two steps.

1. Validation of model assumptions that shape the mechanics of the ABM, in this research the assumptions shown in Figure 2.
2. Validation of model results by assessing their feasibility.

Both the validation steps will be discussed in the remainder of this section.

First of all, the model assumptions have been validated in the course of the model conceptualisation. During this conceptualisation phase, the feasibility of the model assumptions have been assessed in bi-weekly meetings with experts from an internationally operating consulting firm, active in the field of cyber-security for mainly financial service providers. For the sake of confidentiality, their anonymity is preserved. This type of validation is referred to as the ‘companion modelling approach’ [Barreteau et al., 2003]. The assumptions that follow from the model conceptualisation are thus seen as valid by those experts who partook in the companion modelling approach.

In order to further increase the validity of the model assumptions, the model assumptions are discussed with an expert panel, consisting of seven experts of which one has been part of the companion modelling approach. This validation session has had the form of a workshop in which the validity of the model assumptions, shown in Figure 2, were discussed. The first main mechanics that have been discussed is the exclusion of the potential loss magnitude and thus the potential gain for threat agent organisation. The experts deemed this simplification credible for a limited type of real world settings, most prominently those containing a relatively small number of large defender organisations. The financial service sector is a good example of such a system. The experts emphasised that this must be kept in mind when establishing the key insights.

A second point that has been made by the experts is that the distinction between a default and reactive strategy, and the fact that the latter is followed by a defender after incurring a successful cyber-attack, is feasible. However, experts criticised the fact that the ABM does not account for a possible time lag with which this reactive strategy is implemented. Defender organisations are not always capable of directly spotting a successful cyber-attack. On top of that, it may take time to unfold a reactive strategy. This turned out to be the most important mechanism that the experts missed in the model assumptions.

A last mechanism that has been discussed is the implementation of the default and reactive strategies and the threat capability learning strategies. The experts were explained that, in essence, these strategies contain a mechanism in which a higher investment level in the default defence strategy likely leads

Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations
to a higher control strength. But, this is not necessarily the case, since higher investments do not by definition lead to a higher control strength. The same mechanism is specified between the threat capability learning strategy and the threat capability of a threat agent organisation. The expert panel reckoned this as a feasible implementation of these strategies.

In the second part of this workshop, the results were validated by discussing the key insights. Key Insight 1 and 3 have been hardly discussed, as the experts quickly agreed upon the validity of these results in a setting where defender organisations have similar potential loss magnitude and potential gain for the threat agent organisations.

However, Key Insight 2 has been elaborately discussed. As has been mentioned in subsection 6.2, no insights could be given on the cyber-risk carried by an individual defender organisation if the distribution of default defence strategies over these defender agents is changed. During the workshop, the experts agreed that when many defenders follow a low investment default defence strategy, each individual defender incurs a relatively small number of successful cyber-attacks. This is because the total number of successful cyber-attacks is divided over, most likely, many defender organisations.

But, if a greater set of defenders decide to invest more in cyber-security, the remaining defenders that invest little in cyber-security will incur a lot of successful cyber-attacks whereas those that invest a lot in cyber-security are likely to be safe from successful cyber-attacks. After all, successful cyber-attacks are most likely directed to the defender organisations with a low investment default defence strategy, since these are likely to be the weakest defender organisations.

But, if the remaining defender organisations with low cyber-security investments also decide to gear up this spending, all defender organisations are again more or less equally strong, diminishing the effectiveness of the higher investments for those organisations that already had decided to highly invest in cyber-security. The previous shows that the cyber-risk of a defender organisation, that invests little in cyber-security, heavily increases when many of its peers follow a high investment default defence strategy. This gives insight in how the default defence strategies followed by defender organisations influence the cyber-risk carried by a defender organisation. The validation workshop thus extended Key Insight 2, that only concerned the cyber-risk carried by a group of defender organisations.

Key Insights 4 and 5 were also subject to discussion due to the fact that the reactive strategy is implemented without any lag, as is discussed earlier in this section. The experts generally agreed upon the validity of the key insights, provided that the reactive defence strategy is directly implemented by the defender organisations. If this is not the case, defenders that are successfully attacked are likely to remain with a low control strength for a longer period, also after this successful cyber-attack. This is because the reactive strategy, that should increase this control strength, is not directly implemented. Yet, it has been mentioned in this section that it is disputable whether defender organisations are able to directly implement a reactive strategy after incurring a successful cyber-attack. Altogether, the expert panel concluded that Key Insight 4 and 5 are likely to be true when a defender organisation is able to quickly implement a reactive strategy after incurring a successful cyber-attack.
8 Conclusion and Discussion

In this conclusion, I will firstly discuss the main contributions in subsection 8.1 followed by the limitations of this research and suggestions how to tackle these limitations in subsection 8.2.

8.1 Main Contributions

The main objective of this research was to generate insights about the cyber-risk a defender organisation in relation to the behaviour of defender and threat agent organisations. This would increase the understanding of an organisation’s cyber-risk since no research in the area of cyber-risk has been conducted yet that generates such insights. This paper has shown that these kind insights are generated by following a complex adaptive systems (CAS) perspective. The generated insights have been shown in Figure 5. The conclusion is thus that the research objective is fulfilled. Yet, this is not the main contribution of this research.

What must realised from this research is that insights, about the relationship between defender and threat agent behaviour and the cyber-risk of a defender, are not generated by conventional cyber-risk analysis methods. These methods, that predominantly focus on the vulnerabilities within a single defender organisation, do not take this behaviour into account. Rather, one must use a CAS-perspective, in which the cyber-risk of a defender is seen as the resultant of continuously adapting behaviour of defenders and threat agents. This should encourage researchers in the area of cyber-risk to apply such a CAS-perspective for conducting cyber-risk analysis.

8.2 Limitations and Further Research

In this research, three major types of limitations are encountered.

1. The key insights only hold for systems in which defender organisations have a similar potential loss magnitude and potential gain for the threat agent organisations.

2. Some assumptions of the ABM implement defender and threat agent behaviour in a way that possibly not corresponds with reality. For instance, in this research, increased irrationality is considered as a mechanism that makes threat agents more randomly attack. However, it may be that irrationality manifests itself differently, for instance by threat agents that mimic each other [Sofaer and Goodman, 2001, Kayode et al., 2014]. If under a different assumed mechanisms, results would be generated that contradict the key insights of this research, this would make the validity of these insights questionable.

3. Possibly important mechanisms, that are apparent in the real system, are not incorporated in the ABM as an assumption. For instance, collaboration between defender organisations, in order to collectively prevent successful cyber-attacks, is not taken into account whereas this is increasingly the case in the area of cyber-security [Hernandez-Ardieta et al., 2013].
The advantage however of the agent-based model (ABM), constructed in this research, can be adapted and extended in a way that implements the considerations mentioned in the three types of limitations. Tackling these limitations must thus be seen as a next step in increasing the understanding of cyber-risk in relation to defender and threat agent organisation behaviour.
References


Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations


*Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations*
REFERENCES


---

*Understanding Cyber-risk by Investigating the Behaviour of Defender and Threat Agent Organisations*

Alex J Ryan. What is a systems approach?, 2008.


