Malware Epidemics Effects in a Lanchester Conflict Model

Joachim Draeger, Stephanie Öttl
IABG mbH, Ottobrunn, Germany

Abstract

For developing a better comprehension of the consequences of cyber-attacks, the paper examines the influence of system infections with self-replicating malware on the outcome of kinetic combat. The situation is represented as a system-dynamics model consisting of a SIR-like and a Lanchester component. The game-like context of kinetic combat illustrates the effects of malware in a concise way. Corresponding assessment criteria are derived and applied to scenario classes resulting from assumptions about the expected circumstances. Remaining uncertainties are taken into account by applying Monte-Carlo simulations, whereby the specific scenarios to be processed can be selected randomly by information-theoretic principles. The resulting framework allows a model-based calculation of e.g. the risk and the fraction of scenarios, in which malware attacks turn around the outcome of the kinetic combat. Some of our basic findings derived from computational calculations are: (1) Malware attacks affecting availability can turn around the outcome of kinetic combat in a significant fraction of scenarios. (2) Cyber capabilities tend to soften out kinetic superiority or inferiority. (3) Using the most aggressive malware is not necessarily the best decision for an aggressor. (4) Starting countermeasures against a malware attack at the earliest possible time is not always the best decision for a defender.

1 Introduction

Among all the threats related to cyber security, self-replicating malware like viruses or worms are some of the most important ones. Due to the capability of self-reproduction, the infection of a single unimportant system component may cause catastrophic damage to the overall system — maybe even a complete state — in the final outcome. This disproportionality between the low effort and the potentially significant damage qualifies the usage of malware for large scale attacks and cyber warfare\cite{10,22}. Indeed, the Cyber Conflict Studies Association CCSA\cite{1} lists numerous incidents at nation level. We give some examples: In 1998, the NATO attacked infrastructure and command & control structures in Serbia during the Kosovo war with self-replicating malware\cite{9}, enabling an especially successful air campaign. In April 2007, Estonia was attacked at cyber level, presumably by Russia\cite{3}. The attack has targeted ministries, banks, and media and caused injuries due to riots resulting from the effectiveness of the attack. Trojans have enforced a temporary shutdown of the computer network of the German Bundestag in 2015\cite{17,25}. More examples can be found in\cite{4,8,14,23}.

Despite of all these incidents, the knowledge about mechanisms and consequences of such large scale attacks still seem to be insufficient. One reason may be that malware infections are typically discussed from the IT security perspective alone. Such considerations neglect the effects of a malware infection, however. In an embedded system containing several computers as subsystems, each computer may provide specific functionalities of the overall system. A malware infection of a specific computer may also affect specific functionalities. Only if the (non-)availability of functionalities are taken into account, the effects of malware infections can be assessed adequately. Accordingly, we have analyzed the effects of a malware infection based on a model not only representing the cyber part, but the availability as well. The reduction of the availability caused by the malware infection provides a natural loss function and allows an objective and quantitative assessment of the malware effects. This paper carries out a corresponding analysis

\footnote{1http://www.cyberconflict.org}
for a Lanchester model of kinetic combat as exemplary system affected by malware, whereby the propagation of malware across the system is represented by a SIR-like model. The Lanchester model was chosen mainly due to its simplicity, which may enable a more direct insight into the interactions between availability and malware. Additionally, the game character of the Lanchester model immediately provides an evaluation measure of the outcome of a specific situation.

Several papers are considering co-occurring kinetic combat and cyber warfare with malware. Mishra and Prajapati discuss in their paper [21] cyber warfare based on a differential equation system as well, but they do not take availability aspects into account; instead, they focus on a stability analysis. McMorrow [18] defines the transfer of findings provided by biological epidemics to the cyber domain as one of the objectives for the development of a deeper understanding of large scale cyber attacks. Schramm [24] has developed a corresponding model combining a kinetic battle situation with a one-sided malware attack based on the SIR model [12]. Its symmetrization by Yildiz [31] assures that both forces have the same capabilities and vulnerabilities. Both [30] and [31] examine and expand the models of Schramm.

Our paper contributes to the existing literature by analyzing various scenario classes characterized by corresponding assumptions and uncertainties using Monte-Carlo simulations. It is structured as follows. The Lanchester/SIR model used for our discussion of malware effects is described in section 2. The settings of analysis, which includes the parameters of the model and the evaluation measures, is introduced and discussed in section 3. In section 4, the evaluation measures are applied to the Lanchester/SIR-model of section 2. A discussion of the results is included. The paper closes with an outlook in section 5, which summarizes the results, points to some advanced aspects, and which presents open questions.

2 Model Description

2.1 Model Structure

Kinetic Combat Component As already stated in the introduction, the kinetic combat is modeled using Lanchester equations [13], which consider two opposing homogeneous forces Blue and Red [16]. This situation is described by two coupled deterministic, time-continuous ordinary differential equations.

\[
\begin{align*}
\frac{dB}{dt} &= -\delta_r R(t) B(t) \\
\frac{dR}{dt} &= -\delta_b B(t) R(t)
\end{align*}
\] (1)

wherein \(B(t)\) and \(R(t)\) represent the sizes of the blue and red force at time \(t\) fulfilling the initial conditions \(B(0), R(0) \geq 0\). Both forces simultaneously begin fighting at time \(t = 0\) with effectiveness \(\delta_b\) and \(\delta_r\), respectively. In the following, parameters associated with the blue resp. red force are referred to by an index \(b\) resp. \(r\) in general. The parameter \(p\) describes the capabilities of the forces as an attacker, whereas \(q\) does so for the role of a defender. The exponents \(p,q\) have been introduced for a better fit of historic battles [15]. As a consequence, equation system (1) is only well-defined unless one of \(R\) or \(B\) becomes zero during the evolution. This problem is discussed in more detail in section 2.2. Despite of their simplicity, Lanchester equations are capable to describe large battles at least in some situations [7].

Malware Component The malware component represents the malware propagation across a force. It is described by a variant of an SIR-model, which was developed by Kermack & McKendrick [12]. Though originally developed for the description of biological epidemics, it was successfully applied to the propagation of malware (e.g. [20,26,27]). The naming reflects the three different compartments \(S,I,R\) of the model representing susceptible (here called vulnerable), infected, and recovered (here called patched) force elements. The replacement of the term ‘recovery’ by the term ‘patching’ takes also account of the mere cursory correspondence between biological pathogens and malware concerning the ending of an infection. In the biological domain, organism can typically self-recover, whereas force elements with a malware infection can not patch themselves. Vulnerable elements in contact with another infected individual may become infected themselves with a rate \(\beta\). Infected elements may recover with a rate \(\gamma\) and
may become patched in this way. We assume that the malware propagation within a force is homogeneous and that patching of infected systems can only happen within a force. Accordingly, the equations of the basic SIR-model are defined as follows:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta S(t)I(t) \\
\frac{dI}{dt} &= \beta S(t)I(t) - \gamma I(t) \\
\frac{dR}{dt} &= \gamma I(t)
\end{align*}
\]

(2)

Concerning initial conditions, it holds \( S(0), I(0), R(0) \geq 0 \).

**Component Integration** Lanchester and SIR components are integrated based on the interactions between them. The initial malware infection triggering a malware epidemics is caused by a malware attack of the vulnerable and patched systems of the adversarial force. The effect of a malware attack is a flow of rate \( \alpha \) from vulnerable force elements to infected force elements. Though there exist a large spectrum of infection mechanism, the considerations in this paper are restricted to a single generic mechanism. The kinetic effectiveness \( \delta_U \) of infected force elements is reduced by a factor \( \delta_I \in [0, 1] \). It is restored to its original value after patching. The patching action can be applied to infected resp. vulnerable systems with rate \( \gamma' \) resp. \( \gamma \). Once patched, a new infection (with this specific malware) is excluded. Patching of infected systems requires an interaction with vulnerable or patched systems. Infected systems can not patch other systems or themselves. The effects of kinetic combat on force elements is independent from the malware state of these elements, i.e. vulnerable, infected, and patched systems suffer losses according to the same attrition rate; the malware state influences the capabilities of force elements as attackers, not as defenders.

The assumptions for the kinetic and cyber component and their interactions lead to the structure of the overall model as shown in figure. The compartments \( S, I, R \) already known from the SIR model were supplemented by the compartment \( D \) of destroyed force elements for bookkeeping purposes. We will now quantify the flows for the blue force; the flows for Red correspond to the flows given for the blue force due to the symmetry of the model.

- \( \beta_b S_b I_b / N_b \) is the flow from \( S_b \) to \( I_b \) due to malware infections.
- \( \gamma_b S_b \) is the flow from \( S_b \) to \( R_b \) representing a patching of the vulnerability before an infection occurs.
- \( \gamma'_b I_b (S_b + R_b) / N_b \) is the flow from \( I_b \) to \( R_b \) representing the removal of the malware infection together with a patching of the vulnerability.

Some remarks concerning the normalization have to be added. The simplicity of equation results from a constant 'population' size. If concurrently to the epidemics a kinetic combat occurs inflicting losses among the force elements, a normalization of the epidemics-related interaction terms becomes necessary. This does not hold for the interaction terms related to kinetic combat and the malware attack, since here the absolute numbers are of interest.

Now, the flows related to kinetic combat are discussed. Following the structure of the equation system, the attrition rate of Red on Blue is \( \delta_{U,R}(S_r + R_r + \delta_I I_r)^p \). The factor \( \delta_I \) in this term describes the reduced effectiveness of infected force elements. The affected elements of Blue are \( S^q, I^q, R^q \), or \( D^q \).

- \( \delta_{U,R}(S_b^q + R_b^q + \delta_I I_b^q) \cdot S_b^q \) is the flow from \( S_b \) to \( D_b \) due to kinetic combat losses.
- \( \delta_{U,R}(S_b^q + R_b^q + \delta_I I_b^q) \cdot I_b^q \) is the flow from \( I_b \) to \( D_b \) due to kinetic combat losses.
- \( \delta_{U,R}(S_b^q + R_b^q + \delta_I I_b^q) \cdot R_b^q \) is the flow from \( R_b \) to \( D_b \) due to kinetic combat losses.
- \( \alpha_r(S_r + R_r) \cdot S_r \) is the flow from \( S_b \) to \( I_b \) due to a malware attack of Red.

\[\text{We are using the symbol } \bar{\gamma} \text{ instead of } \gamma \text{ for avoiding confusion with the coefficients } \gamma \text{ and } \gamma' \text{ arising in the overall system of equations.} \]

Whereas \( \bar{\gamma} \) describes self-recovery, the parameters \( \gamma, \gamma' \) represent rate coefficients of an externally triggered patching process.
In the end, we get four equations for each of the two forces. We only give the equations for Blue, since the equations for Red have symmetric form.

$$\frac{dS_b}{dt} = -\beta_b S_b I_b/N_b - \gamma_b S_b - \delta_{Ur} (S_p^e + R_p^e + \delta_{Ir} I_p^e) \cdot S_b^q - \alpha_r (S_r + R_r) \cdot S_b$$

$$\frac{dI_b}{dt} = \beta_b S_b I_b/N_b - \gamma_b' I_b (S_b + R_b)/N_b - \delta_{Ur} (S_p^e + R_p^e + \delta_{Ir} I_p^e) \cdot I_b^q + \alpha_r (S_r + R_r) \cdot S_b$$

$$\frac{dR_b}{dt} = \gamma_b S_b + \gamma_b' I_b (S_b + R_b)/N_b - \delta_{Ur} (S_p^e + R_p^e + \delta_{Ir} I_p^e) \cdot R_b^q$$

$$\frac{dD_b}{dt} = \delta_{Ur} (S_p^e + R_p^e + \delta_{Ir} I_p^e) \cdot (S_b^q + I_b^q + R_b^q)$$

A tabular overview of the parameters contained in the equation system is given in table 1. As initial conditions, the non-negativity $S(0), I(0), R(0), D(0) \geq 0$ of all compartments is required. In the future, we will also use the designation $N := S + I + R$ for the still existing force elements.

### 2.2 Model Consistency

The kinetic interaction terms like $\delta_{Ur} (S_p^e + R_p^e + \delta_{Ir} I_p^e) \cdot S_b^q$ require further discussion. For $q \to 0$, one gets $S_b^q \to 1$ independently of the value of $S$. This means, the losses inflicted on the blue force by Red becomes independent of the number of blue force elements still existing. For $S_b$ close to 0, the level of $S_b$ will thus become negative in effect. Similarly, for $p \to 0$ the factor...
For avoiding such unphysical behavior, a barrier function

**Proposition 1** (Consistency of the Modified Equation System).

1. \( \frac{\delta_U(S^p + R^p + \delta_I, I^p)}{\delta_U(S^p + R^p + \delta_I, I^p)} \cdot \overline{S^p} \to 0 \) for \( S_b \to 0 \) or for \( S_r, I_r, R_r \to 0 \) and \( \delta_U(S^p + R^p + \delta_I, I^p) \cdot \overline{S^p} \approx \delta_U(S^p + R^p + \delta_I, I^p) \cdot \overline{S^p} \) otherwise. Corresponding statements are valid for \( S_r, I_b, I_r, R_b, R_r \).
2. \( S_b \to 0 \Rightarrow \overline{S^p} \to 0 \) and \( S_r \to 0 \Rightarrow \overline{S^p} \to 0 \).
3. \( N_r \to 0 \Rightarrow \overline{N^p} \to 0 \) and \( N_b \to 0 \Rightarrow \overline{N^p} \to 0 \).

**Sketch of Proof.**

1. According to construction, \( \overline{S^p} \to 0 \) for \( S_b \to 0 \) and \( S_b \approx \overline{S^p} \) otherwise. Corresponding statements are valid for \( S_r, I_b, I_r, R_b, R_r \). The statement is an immediate consequence.
Figure 2: A typical behavior of the equation system. Besides of the number of vulnerable, infected, and patched elements for both forces, the overall numbers of available and destroyed force elements are shown. Due to malware attacks applied by both forces, the red force is stronger at the beginning but will still lose in the end.

\[ b) \quad \text{The condition } S_b \to 0 \text{ assures that all flow terms in the expression of } S_b' \text{ in equations system (3) become 0; concerning the flow term representing kinetic combat, this results from part a). The claim follows for } S_r. \text{ The proof for } S_r \text{ proceeds in an analogous way.} \]

\[ c) \quad \text{The assertion } N_r \to 0 \text{ leads immediately to } S_r, R_r, I_r \to 0 \text{ due to the non-negativity of the compartment levels. Thus it holds } S_p + R_p + \delta I_r I_p \to 0 \text{ and moreover } \delta U_r (S_p + R_p + \delta I_r I_p) \cdot S_q \to 0. \text{ This gives } N_b' = S_b' + I_b' + R_b' \to 0, \text{ which is the claim.} \]

The preceding proposition excludes the two types of unphysical behavior mentioned at the beginning of this section after introduction of the barrier function \( f(x) \). Such negativities can also be generated at the computational level. For avoiding overshooting effects leading to negative compartment levels, the size of the time steps has to be chosen small enough. A less extreme barrier function \( f(x) \) — i.e. a barrier function with a smaller exponent — may avoid negativities more reliably, but its influence on the dynamics of the system will be stronger.

### 2.3 Model Extensions

Since the start of cyber and kinetic warfare may not necessarily coincide, we extend the model by allowing an onset of kinetic combat, malware attack and patching process independently from each other. In this way, situations like a preparation of a kinetic battle by a supporting malware
attack or a late start of countermeasures due to a delayed provision of appropriate patches can be modeled. Additionally, the duration of the malware attack can be restricted by \( \Delta t_m \). An early stop of the malware attack can sometimes be useful for covering up the source of the malware attack. Before the start and after the end of an action like a malware attack, the action is defined as being inactive by appropriate settings of the action parameters. Inbetween, the action parameters are set to their effective values. Details are given in table 2. If we talk about the equation system (3), we mean always its extension by the events of table 2.

| Events | Associated Parameter Changes |
|--------|-----------------------------|
| Initial settings | \( \alpha, \delta_U, \gamma, \gamma' = 0 \) |
| Start of kinetic combat at time \( t_{\text{kin}} \) | \( \delta_U \) set to (effective) parameter value |
| Start of malware attack at time \( t_{\text{mal}} = t_{\text{kin}} + \Delta t \) | \( \alpha \) set to (effective) parameter value |
| Stop of malware attack at time \( t_{\text{mal}} + \Delta t_m \) | \( \alpha = 0 \) |
| Start of patching process at time \( t_{\text{patch}} = t_{\text{kin}} + \Delta t_p \) | \( \gamma, \gamma' \) set to (effective) parameter values |

Table 2: Translation of the events resulting from the timing parameters given in table 1 to corresponding changes of the parameter settings. The term 'effective parameter value' means here the original parameter value, which is restored after switching off the corresponding part of the model momentarily by setting the parameter equal to zero in the start phase of the simulation.

**Proposition 2 (Properties of the Equation System).**

a) The equation system (3) is symmetric w.r.t. Blue and Red, i.e. an interchange of the initial conditions and parameters for Blue and Red corresponds to an interchange of the dynamics of the compartment levels \( S_b(t), I_b(t), R_b(t), D_b(t) \) and \( S_r(t), I_r(t), R_r(t), D_r(t) \).

b) The quantity \( N(t) + D(t) \) is constant over time. For an initial condition \( D(0) = 0 \), one gets \( N(0) = N(t) + D(t) \) for all times \( t \).

**Sketch of Proof.**

a) According to the structure of (3)

b) Summing up \( N'(t) + D'(t) = S'(t) + I'(t) + R'(t) + D'(t) \) the changes for all compartments gives 0, because all terms will cancel out. Thus, \( N(t) + D(t) \) is constant over time.

\[ \square \]

### 2.4 Model Validation

Our strategy of model validation is oriented towards internal consistency. This takes into account that our abstract model of a kinetic combat co-occurring with malware propagation does not aim primarily at a detailed and precise representation of a real world situation, but at enabling a discussion of the fundamental phenomena of the interactions between availability of system capabilities and malware effects. Furthermore, it has to be noted that real word comparison data are not yet accessible.

The two key components of the model — the kinetic combat and the malware propagation component — are validated by comparing their behavior with very basic models of the pure Lanchester and SIR equations. In this way, the correct formulation and implementation of equation system (3) has been checked. Unused parts of (3) were switched off for the validation by appropriate parameter settings. For comparing the Lanchester part of (3) with the pure Lanchester model (1), all model parameters are set to zero resp. neutral values with exception of \( \delta_{Ub}, \delta_{Ur}, p, q \). For the effectivity reduction of force elements due to malware infections, we have chosen \( \delta_{Ib}, \delta_{Ir} = 1 \).

For executing a cross-validation of the cyber warfare component, the model parameters are set to neutral values with exception of \( \beta, \gamma, \gamma' \). Especially, it holds \( \delta_{Ub}, \delta_{Ur}, \alpha_b, \alpha_r = 0 \). Furthermore,
we will limit our considerations to Blue due to the symmetry of (3) according to proposition 2.
This leads to the following comparison model.

\[
\begin{align*}
\frac{dS_B}{dt} &= -\beta_B S_B I_B / N_B - \gamma_B S_B \\
\frac{dI_B}{dt} &= \beta_B S_B I_B / N_B - \gamma_B I_B (S_B + R_B) / N_B \\
\frac{dR_B}{dt} &= \gamma_B S_B + \gamma_B I_B (S_B + R_B) / N_B
\end{align*}
\] (5)

This equation system differs from common SIR-models with biological origin by an unusual 'recovery' term \(\gamma_B I_B (S_B + R_B) / N_B\). For the cross-validation, we will use the initial conditions \(S_B(0) \in [0,1,1,0]\) and \(I_B(0) := 0.1 \cdot S_B\). Using \(I_B(0) > 0\) is a consequence of the missing option of a malware attack; thus, we have to start with a non-zero fraction of infections. Applying a pre-implemented ODE solver for the comparison models validates also the Euler method used as solution algorithm for (3). The existence of events changing parameter values discontinuously makes it advantageous to use a simple explicit solution method.

Additionally, the overall model and thus the interactions between the two main components was examined by face-validation. Besides of the plausibility of the effects of parameter changes, checks of the reproducibility of constraints like the conservation of the overall number \(N_B(t) + D_B(t)\) resp. \(N_r(t) + D_r(t)\) of force elements or the monotonic decrease of existing force elements \(N_B(t)\) resp. \(N_r(t)\) over time were executed.

3 Simulation Designs and Observables

3.1 Design and Outcome Space

In order to analyze the behavior of the system (3), simulation experiments are executed for specific scenarios \(x \in X\). The space \(X = \times_i X_i\) of scenarios is composed of the admissible domains \(X_i\) of the parameters and of the initial conditions of the model. In the following, the component \(X_i\) associated with, say, the malware attack rate \(\alpha_B\) of Blue is designated as \(X_{\alpha_B}\). The set \(X\) is also called design space.

A specific scenario \(x \in X\) provides the input for the simulation. Executing the simulation \(\text{sim}: X \to Y\) establishes an input/outcome relation by assigning an outcome \(y \in Y\) to the input \(x\). The space \(Y = (\mathbb{R}_+^8 \to \mathbb{R}_+^8)\) of simulation outcomes records the dynamics of the model (3) as the time-dependent variations of the levels of all eight compartments. Thus, an outcome \(y \in Y\) has the form

\[
\left\{(S_B(t))_{t \in T}, (I_B(t))_{t \in T}, (R_B(t))_{t \in T}, (S_r(t))_{t \in T}, (I_r(t))_{t \in T}, (R_r(t))_{t \in T}, (D_r(t))_{t \in T}\right\}
\]

with \(T = [0, \infty]\) as the simulation time.

3.2 From Trajectories to Scalar Observables

The components of the outcome space \(Y\) consist of time-dependent trajectories of infinite length. For such function spaces usually no canonical ordering ‘<’ exist, which is a serious obstacle for comparing scenario outcomes. Without a canonical ordering relation, it is hard to justify why an outcome \(y\) is considered as better than an outcome \(y'\). An option of reducing the time-dependent trajectories to single scalar values would be helpful in this respect. The following proposition improves the situation.

Proposition 3 (Dynamics at Infinity). For \(t \to \infty\), one gets \(S(t), I'(t), R'(t), D'(t) \to 0\)

Sketch of Proof. In the following, we assume w.l.o.g. that all events have already been processed, i.e. that no model parameters will change anymore in the simulation run. Since the compartment \(S\) has no inflow, the level of \(S\) is monotonically decreasing. According to \(S'' < 0\) — derivable directly from (3) — the decrease of \(S(t)\) is monotonic as well; thus, an already small flow rate can not increase again. Due to the monotonic decrease of \(S(t)\) and \(S'(t)\) on the one hand and
the limitation given by \( S(t) \geq 0 \) on the other, the decrease must be fading out. We can state \( \forall \varepsilon > 0 \exists t' \forall t > t': |S'(t)| < \varepsilon \). This proves the claim \( S' \to 0 \). Concerning the claim \( D' \to 0 \), an analogous reasoning can be made. Here, the compartment \( D \) has no outflow leading to a monotonic decrease of \( D(t) \) and \( D'(t) \). The claim holds, because \( D(t) \) is limited from above according to \( D(t) \leq S(0) = N(0) \) because of proposition 2.\( [b] \)

The statement \( S' \to 0 \) means according to the flows shown in figure 1 that for \( t > t' \), there is no significant inflow to the compartment \( I \) anymore. From this time on, the compartment level of \( I \) will change significantly only due to an eventual outflow. We can argue again analogously to \( S' \) and \( D' \) and state that \( I(t) \) and \( I'(t) \) is monotonically decreasing. Consequently, \( \forall \varepsilon > 0 \exists t'' > t \forall t > t'': |I'(t)| < \varepsilon \). This proves \( I' \to 0 \) as well. Finally, we make use of the preservation of \( N(t) + D(t) = S(t) + I(t) + R(t) + D(t) \) over time according to proposition 2.\( [b] \). Since we have already shown \( S', I', D' \to 0 \), we get \( R' \to 0 \) as well.

Proposition 3 means that the dynamics of \( C \) is fading for \( t \to \infty \). This justifies in effect to interpret the values \( C := \lim_{t \to \infty} C(t) \), \( C \in \{S_b, I_b, R_b, D_b, R_s, I_r, R_r, D_r\} \) of the compartment levels at infinity as ‘result’ of the simulation. Due to \( C \in \mathbb{R} \), a canonical total ordering ‘\(<\)’ is available for assessment purposes then. Additionally, a fading dynamics is established as a plausible stop criterion, because afterwards no significant changes of the compartment levels will occur anymore and the state of the system at this time is approximately equal to its state at infinity. Accordingly, the stop is triggered if all compartments \( C \in \{S_b, I_b, R_b, D_b, R_s, I_r, R_r, D_r\} \) fulfill the criterion \( |C(t) - C(t + \Delta t_D)| < \varepsilon \) for a ‘long’ period \( \Delta t_D \). The end time of the simulation given by the stopping criterion is designated as \( t_{\text{end}} \). For assuring that all temporal events are already processed — they may trigger a fundamental change of the situation — we start to check this criterion after processing all events, i.e. only for \( t > t_{\text{kin}}, t_{\text{mal}} + \Delta t_m, t_{\text{patch}} \). This approach will work of course only as intended, if \( \Delta t_D \) is chosen sufficiently large and \( \varepsilon \) sufficiently small. Unfortunately, for each choice of \( \Delta t_D \) and of \( \varepsilon \) there exist scenarios with an arbitrary slow dynamics leading to large approximation errors, because in such cases an early stop of the simulation provides intermediate instead of ‘final’ results. These exceptions are considered as tolerable here, since our intention is a statistics-based analysis of the model behavior as explained later in section 3.4.

A weaker analogon to proposition 3 can be used for defining the end time \( t_{\text{kin-end}} \) of kinetic combat. We can state that an almost vanished force will not change its own size significantly anymore and will also be unable to change the size of the opposing force significantly because of its almost vanished fighting power.

**Proposition 4 (Effects of a Destroyed Force).** If \( N_r \to 0 \) or \( N_b \to 0 \), then \( N'_b, N'_r, D'_b, D'_r \to 0 \).

**Proof.** W.l.o.g. one can assume \( N_b \to 0 \); otherwise change blue and red side. Since \( N_b + D_b \) is preserved over time according to proposition 2,\( [b] \) and since \( N_b \) will not significantly change anymore, \( D_b \) will not change significantly either. We can thus state \( N'_b, D'_b \to 0 \). The claim \( N_b \to 0 \Rightarrow N'_b \to 0 \) holds according to proposition 1.\( [b] \). Proposition 2,\( [b] \) states that \( N_r(t) + D_r(t) \) is constant over time; thus, \( N'_r \to 0 \) gives \( D'_r \to 0 \) as well.

In accordance with proposition 3 we define the end time \( t_{\text{kin-end}} \) of kinetic combat based on the criterion \( N_r(t) < \varepsilon \lor N_b(t) < \varepsilon \). Of course, \( t_{\text{kin-end}} \) and \( t_{\text{end}} \) will not necessarily coincide, because even after annihilation of one force a malware epidemics may still be underway in the other. The application of the two criteria for triggering the stop of the simulation and for detecting the end of kinetic combat leads to the simulation algorithm 1.

### 3.3 Space of Observables

In the following, the assessment measures — called observables here — are defined. Since we aim at measuring the effects of a malware infection, the numbers of, say, infected or patched force elements are of minor interest only. Instead we are focusing on the eventually reduced availability of infected force elements. Accordingly, the remaining survivors \( N_b, N_r \) and cumulated losses \( D_b, D_r \) are counted at the end \( t = t_{\text{end}} \) of the simulation. They are of interest, because force elements infected with malware may alter the course of kinetic combat due to their reduced effectiveness. Since \( N_b(t), N_r(t) \) are nonnegative, the relative number \( \Delta N := N_b(t_{\text{end}}) - N_b(t_{\text{end}}) \)
of surviving force elements seems to be a suitable assessment criterion. Correspondingly, the relative number $\Delta D := D_b(t_{\text{end}}) - D_r(t_{\text{end}})$ of destroyed elements at time $t_{\text{end}}$ can be applied. The interpretation of these relative assessment criteria is straightforward. The case $\Delta N > 0$ indicates a win of Blue, whereas the case $\Delta N < 0$ indicates a win of Red. A situation with $\Delta N = 0$ could be judged as Remis. Analogously, $\Delta D > 0$ indicates an advantage for Red, whereas $\Delta D < 0$ indicates an advantage for Blue. Again, $\Delta D = 0$ could be judged as Remis because the losses of both sides have the same amount. The inclusion of both $\Delta N$ and $\Delta D$ is justified, because results with e.g. $\Delta N > 0$ and $\Delta D > 0$ are possible due to different force sizes and force effectivenesses.

The set of observables is completed with the duration $\Delta T := t_{\text{kin-end}} - t_{\text{kin}}$ of kinetic combat and with the absolute number $L_b := D_b(t_{\text{end}})$ of losses for the blue force. The observables used in this paper are listed in Table 3. In the following, the set of values of an observable, say, $\Delta N$, for a set $X \subseteq X$ of scenarios is designated as $\Delta N(X)$.

### Observables

| Observables | Description | Codomain | Range |
|-------------|-------------|----------|-------|
| $\Delta N := N_b(t_{\text{end}}) - N_r(t_{\text{end}})$ | Relative number of existing force elements at $t_{\text{end}}$ | $\Delta N \in \mathbb{R}$ | $\Delta N \in [-1,1]$ |
| $\Delta D := D_b(t_{\text{end}}) - D_r(t_{\text{end}})$ | Relative number of destroyed elements at $t_{\text{end}}$ | $\Delta D \in \mathbb{R}$ | $\Delta D \in [-1,1]$ |
| $L_b := D_b(t_{\text{end}})$ | Destroyed elements of the blue force at $t_{\text{end}}$ | $L_b \in \mathbb{R}_0^+$ | $L_b \in [0,1]$ |
| $\Delta T := t_{\text{kin-end}} - t_{\text{kin}}$ | Time span of kinetic combat | $\Delta T \in \mathbb{R}_0^+$ | $\Delta T \in \mathbb{R}_0^+$ |

Table 3: List of the observables used for assessment purposes. In the column ‘Range’ the set of possible outcomes for the initial values and parameter values taken into account in this paper is given.

Important properties of the observables are given in the following proposition.

**Proposition 5** (Extrema of Observables).

a) Let the values of $S_b(0), S_r(0)$ be given and may hold $I_b(0), R_b(0), D_b(0), I_r(0), R_r(0), D_r(0) = 0$. Then $\max(\Delta N) = \max(\Delta D) = N_b(0)$ and $\min(\Delta N) = \min(\Delta D) = -N_r(0)$.

b) Let the values of $S_b(0), S_r(0)$ be given and may hold $I_b(0), R_b(0), D_b(0), I_r(0), R_r(0), D_r(0) = 0$. Then $\max(L_b) = N_b(0)$ and $\min(L_b) = 0$.

**Sketch of Proof.**

a) Due to the definition of $\Delta N$ and the monotonic decrease of $N_b$, the observable $\Delta N$ can not have a value larger than $N_b(0)$. It reaches this value at the end of the simulation, if all force elements of Blue survive e.g. due to $\delta_{b,t} = 0$ and no elements of Red survive due to $\delta_{r,t} > 0$ and e.g. $\delta_{rb} = 1$. Proposition 2 leads to $\min(\Delta N) = -N_r(0)$. Then, the corresponding statements for $\Delta D$ are a consequence of the preservation of both $N_b(t) + D_b(t)$ and $N_r(t) + D_r(t)$ over time according to proposition 2.

b) Proof analogous to a)
Quantitative assessments enable comparisons of scenario outcomes, but will not allow judging an outcome as especially ‘good’ or ‘bad’. Such an absolute assessment becomes possible, however, as soon as the range of possible values of the assessment measure is known. Proposition 5 gives the ranges of $\Delta N$, $\Delta D$, and $L_b$. One has to keep in mind, however, that constraints defined on the design space restrict these ranges of possible values as well.

### 3.4 Information-theoretic Designs

Since the details of a future malware attack are unknown, it is advisable to consider the whole spectrum $X$ of possible scenarios instead of concentrating on a few manually selected scenarios of limited representability. In this way, a selection bias is avoided. In order to indicate the frequency of occurrences of scenarios $x \in X$, the set $X$ is now enriched by a notion of probability $p$. This gives the so-called Monte-Carlo design space $(X, p)$. The probability distribution $p$ represents the available knowledge (and assumptions) about the actual situation — or, seen from a different point of view, the incompleteness and the imperfections of this knowledge. We have to avoid a $p(x)$, which contains more information about the situation as actually given; thus, we choose the probability distribution $p(x)$ with the highest entropy among all distributions fulfilling the constraints for the given situation. According to [11], the entropy $H(p)$ of a continuous probability distribution $p$ is given by $H(p) = -\int p(x) \log p(x) dx$. Thus, we have to maximize the entropy $H(p)$ of $p(x)$ under the constraint that $p(x)$ is compatible with the existing knowledge. In this paper, we limit ourselves to range restrictions of the parameters contained in $X$ as knowledge for reasons of simplicity. It results a uniform probability distribution $p(x)$ [2]. Renouncing any knowledge would be a problem, because in this case the finiteness of $H(p)$ can not be assured anymore.

A complete overview of the system behavior would be provided by applying the simulation to all scenarios $x \in X$ belonging to the design space $X$. Due to the typically infinite size of $X$, we are restricting ourselves to a finite subset $\tilde{X} \subset \text{fin} X$ of $X$. The set $\tilde{X}$ is called a simulation design.

The subset $\tilde{X}$ is selected according to the probability distribution $p(x)$ of the Monte-Carlo design space $(M, p)$ by executing corresponding random experiments. The restriction of $X$ to a finite subset $\tilde{X}$ is a necessary step for computational tractability; in this respect, it is a counterpart to the restriction of the simulation runs to finite runtimes. Both measures provide computational approximations of the noncomputable exact values. The outcomes of the simulation of scenarios $x \in \tilde{X}$ are designated as $\tilde{Y} \subseteq Y$.

For monitoring the quality of the approximation, we compare the properties of the set $\tilde{X} = X_{\tilde{X}}, \tilde{X}$, which is generated by computational means, with the corresponding exact properties of the full design $(X, p)$. The exact values can be derived analytically. The outcomes $\tilde{Y}$ can be used for monitoring purposes as well. Concerning the inputs $x \in \tilde{X}$ one may check for example, how far the actual statistics of $\tilde{X}$ reflects the properties of the probability distribution $p$. In the case of uniform distributions, the measured values $\text{mean}(\tilde{X})$ and $\sigma(\tilde{X})$ of the components $\tilde{X}_i$ have to be compared with the theoretically expected values $\text{mean}(X) = (\min(X) + \max(X))/2$ and $\sigma(X) = (\max(X) - \min(X))/\sqrt{12}$. Concerning the outcomes, the observed maximum and minimum of the observables $\Delta N$ and $\Delta D$ over the set $\tilde{X}$ of scenarios can be compared with the theoretical range of these observables predicted in proposition [5](a). This helps to supervise the realized coverage of $X$ by $\tilde{X}$. Another monitoring option provides proposition [2](a), which makes predictions for a design space $X$, which is symmetric w.r.t. Blue and Red. For an uniform probability distribution $p$ it must hold $\text{mean}(\Delta N) \approx 0$ and $\text{mean}(\Delta D) \approx 0$ according to the law of large numbers. A numerical example for both inputs and outcomes is shown in figure [3](a).

### 3.5 Risk of Designs

The statistical mean of an observable is intimately related to the von Neumann-Morgenstern theory of expected utility. Restricting the considerations to disadvantageous aspects leads to the notion of risk $\mathcal{R}$ instead of the expected utility. Formally, $\mathcal{R}$ is defined as the expectation value of a loss function $L([1])$. In our case, we naturally consider the observable $L = D(t_{\text{end}})$ of destroyed
force elements as loss value assigned to a single simulation run. The probability distribution \( p \) of the underlying Monte Carlo design space \( (X, p) \) introduces the frequency with which such loss values occur. Accordingly, the risk \( \mathcal{R} \) can be measured as the average of \( L(X) \).

**Proposition 6 (Properties of Risk).**

a) For the simulation design \( \tilde{X} \) it holds \( \text{mean}(N(0)) = \text{mean}(N(t_{\text{end}})) + \text{mean}(D(t_{\text{end}})) = \text{mean}(N(t_{\text{end}})) + \mathcal{R} \).

b) \( \mathcal{R} \leq (\max(\tilde{X}_{N(0)}) + \min(\tilde{X}_{N(0)}))/2 \) for a uniform probability distribution of \( \tilde{X}_{N(0)} \) in the simulation design \( \tilde{X} \).

c) \( \mathcal{R} \leq \max(\tilde{X}_{N(0)}) \).

Proof.

a) According to proposition 2, one gets \( N(0) = N(t_{\text{end}}) + D(t_{\text{end}}) \). Applying the operator \( \text{mean} \) to both sides of the equation and taking the linearity of \( \text{mean} \) into account, the definition of \( \mathcal{R} \) gives the claimed statement.

b) The risk is maximal, if the losses \( L \) are maximal, i.e. if no survivors occur. Thus, it holds \( \text{mean}(N(t_{\text{end}})) = 0 \) in this case. Furthermore, for a uniform probability distribution with upper and lower bounds \( \max(\tilde{X}_{N(0)}), \min(\tilde{X}_{N(0)}) \) it holds \( \text{mean}(N(0)) = (\max(\tilde{X}_{N(0)}) + \min(\tilde{X}_{N(0)}))/2 \). The assertion is an immediate consequence.

c) In the statement \( \text{mean}(N(0)) = \text{mean}(N(t_{\text{end}})) + \mathcal{R} \) of part a), the risk \( \mathcal{R} \) is maximal, if \( N(t_{\text{end}}) \) is minimal and \( N(0) \) maximal. For an arbitrary simulation design \( \tilde{X} \), there may never be a survivor at the end, and the initial number \( N(0) \) of force elements may always be maximal indeed. Formally, this leads to \( N(t_{\text{end}}) = 0 \) and \( N(0) = \max(\tilde{X}_{N(0)}) \). This gives the claim.

Of course, it is possible to define a chance \( \mathcal{C} = \text{mean}(N(t_{\text{end}})) \) analogously to the risk \( \mathcal{R} = \)
mean(D(t_{end})). Due to proposition 6, C can then be calculated by $C = \text{mean}(N(0)) - R$. Since this gives no new essential information, we will discuss only the risk in the following.

4 Analysis of Model Behavior

4.1 Analysis of Scenario Classes

We will now analyze the statistics of outcomes for the scenario classes given in table 4. Concerning the initial conditions, we assume $I(0) = 0, R(0) = 0, D(0) = 0$. For the ranges of model parameters and the initial number of vulnerable elements it may hold in general:

\[
\begin{align*}
\alpha & \in [0, 1] & \beta & \in [0, 5] \\
\gamma & \in [0, 1] & \gamma' & \in [0, 1] \\
\delta_I & \in [0, 5] & \delta_I' & \in [0, 1] \\
p & \in [0, 3] & q & \in [0, 3] \\
\Delta_t & \in [-2, 4] & \Delta t_m & \in [0, 1] \\
\Delta t_p & \in [-2, 4] & S(0) & \in [0, 1, 1]
\end{align*}
\]

The ranges may be subject to additional constraints in specific scenario classes; for details, see table 4. Though asymmetric cyber capabilities are more interesting for assessing the potential influence of these capabilities on the outcome, the symmetric cases 'kin' and 'pat' defined in table 4 provide reference points for comparisons. For 'pat', the characteristics introduced by setting both $\gamma, \gamma'$ to zero are more subtle. As stated before, force elements infected with malware typically have a reduced kinetic effectiveness. The setting $\gamma' = 0$ represents the inability to patch an infected element for reestablishing the original fighting strength, i.e. these elements can not recover effectively. This means that the outflow of the compartment $I$ is blocked. In phases without kinetic combat, the level of the compartment $I$ will thus increase monotonically. As a supplement, the condition $\gamma = 0$ blocks the bypass of $I$ through a direct flow from $S$ to $R$. This increases the inflow to $I$ indirectly, i.e. it increases the number of infected force elements and thus decreases the fighting capability further. It will thus be advantageous for the opposite force in this case to start the malware attack at the earliest possible time and in the strongest way possible. The earlier and the more intense the malware attack, the higher the level of infections and the higher the chances of a successful kinetic combat for the attacker.

For allowing a concise assessment of the consequences of malware attacks, we supplement now kinetic equality by the notions of kinetic inferiority and kinetic superiority. Together, these notions partition the design space $X$ in three disjoint subsets. In the following, we will discuss the properties of these subsets.

**Definition** (Kinetic Superiority and Kinetic Inferiority). Let $g_{\text{kin}}: X \to X$ designate the mapping, which transforms a scenario $x \in X$ to a corresponding scenario $x' \in X$ with $x'_{I_{fs}} = x_{I_{fs}} = 1$ and $x_i = x'_i$ for all other components. In effect, the mapping $g_{\text{kin}}$ provides a pure kinetic scenario $x'$ resulting from $x$ by hiding all malware effects. Then, Blue is designated as kinetic superior resp. kinetic inferior for a scenario $\tilde{x} \in \tilde{X}$, if $\Delta N(g_{\text{kin}}(\tilde{x})) > 0$ resp. $< 0$.

Kinetic superiority and inferiority make an individual handling advisable, because malware is used with fundamentally different intentions. In the case of superiority, malware serves purposes of risk reduction. In the case of inferiority, malware intends to change the winning side by compensating inferiority. This means formally, that Blue aims at $\Delta N(\tilde{x}) > 0$ despite of $\Delta N(g_{\text{kin}}(\tilde{x})) < 0$ for a given scenario $\tilde{x} \in \tilde{X}$. Later in section 4.2 we will take a closer look at such changes due to modifications of the given scenario. Altogether, 7150 Monte-Carlo simulation runs were executed for each scenario class defined in table 4. Using a fixed step size of $\delta t = 0.05$, a simulation run was stopped as soon as the change of the value was smaller than $3.0 \cdot 10^{-4}$ for each compartment for at least $\lfloor 1/\delta t \rfloor$ simulation steps.
### Table 4: List of scenario classes specifically discussed in the analysis. For a better overview, they are grouped in symmetric cases (both sides have the same capabilities) and asymmetric cases (some capabilities belong to one side only). As a special kind of symmetry, kinetic equality is considered. Asymmetric cases are mainly used for discussing the advantages resulting from malware attack and defense capabilities.

| Id | Parameter Settings | Designation | Description |
|----|-------------------|-------------|-------------|
|    |                   |             | Symmetric Cases |
| gen | -                 | General case | No additional constraints |
| kin | $\delta_{I_b}, \delta_{I_r} = 1$ | Pure Lanchester case | Pure kinetic combat without cyber component at all |
| pat | $\gamma_b, \gamma_r, \gamma'_b, \gamma'_r = 0$ | No-defense case | Neither side is capable of patching |
|    |                   |             | Asymmetric Cases |
| b-a | $\delta_{I_b} = 1$ | One-sided attack case | The blue side is not affected by malware, i.e. Red is fighting only at the kinetic level |
| b-p | $\gamma_r, \gamma'_r = 0$ | One-sided defense case | The red side can not patch contrary to Blue |
| equ | $N_b(0) = N_r(0), \delta_{U_b} = \delta_{U_r}, p = q$ | Equality case | Both sides are kinetically equal due to equality in force sizes, kinetic effectiveness, and Lanchester coefficients $p, q$ |

The numerical results can be found in the appendix in the tables 6 and 7 for the general case and the case of kinetic equality and in tables 8 and 9 for kinetical inferiority/superiority. Figure 4 provides a graphical representation of the mean values of observables in the scenario classes defined in table 4. For kinetic superiority resp. inferiority, the mean $\Delta N(\tilde{X})$ deviates significantly from classes without such an imbalance. The influence of kinetic superiority resp. inferiority on the mean $\Delta D(\tilde{X})$ is slightly smaller. The risk $R(\tilde{X})$ representing the mean absolute number of losses is typically less influenced by superiority or inferiority than the mean relative number $\text{mean}(\Delta D(\tilde{X}))$ of losses. Kinetical equality increases the risk $R(\tilde{X})$ both for malware attack and defense situations to a level comparable to situations with kinetic inferiority. Contrary to kinetic inferiority, the higher risk for situations with kinetic equality is accompanied by a prolongation of the phases of kinetic combat as indicated by the mean $\text{mean}(\Delta T(\tilde{X}))$. Value distributions of $\Delta N$ are shown in figure 9 in the appendix. Complementary information about $\Delta N$ for kinetically superior and inferior forces can be found in figure 10 and about one-sided attack and defense in figure 11. Value distributions of the losses $L$ are included in the figures 10 and 11 as well.

As a final remark, we want to add that attack and (no-)defense situations are commonly similar. One reason for this similarity may be that without malware attacks, there are also no defense actions (If there is no action, counteractions do not make sense).
Figure 4: The bar charts give the mean values of the observables $\Delta N$, $\Delta D$, $\Delta T$, and the risk $R = \text{mean}(D_b(t_{\text{end}}))$ for various scenario classes. The classes are organized in eight groups. The first four groups display the results for situations with and without kinetic equality constraint for both cyber attack and cyber defense situations. The last four groups repeat these considerations for the cases of kinetic superiority and inferiority. Each group consists of the case without further constraints, the one-sided cyber capability case and the case without corresponding cyber capabilities.

In all symmetric cases, $\text{mean}(\Delta N) \approx 0$ and $\text{mean}(\Delta D) \approx 0$ due to the symmetry of (3). Accordingly, fighting out a combat for both sides not only at the kinetic but on the cyber level as well does not influence the chances of survival in the mean. If only the blue side supports its kinetic combat with a malware attack, $\text{mean}(\Delta N)$ is increased and $\text{mean}(\Delta D)$ decreased. If only patching capabilities are limited to Blue (defense case), $\text{mean}(\Delta N)$ is only slightly increased. The value of $\text{mean}(\Delta D)$ is decreased accordingly. The expected number of surviving force elements is considerably smaller than the expected number of killed force elements; this holds due to the fact, that the loosing side of a kinetic combat has no surviving force elements, whereas even the force of the winning side is reduced by a certain amount of elements destroyed in combat. The risk is reduced in the case of one-sided malware attacks or defenses.
4.2 Analysis of Scenario Class Changes

In the previous section, the statistics of the observables defined in table 3 is given for various scenario classes. The scenario classes are characterized by constraints on the parameter ranges, which are considered as being a part of the knowledge about the situation. Now we extend our considerations to changes of the actual situation. More precisely, we will look at improvements of the state of knowledge defining the scenario class and the effects of these improvements on the statistics of the observables. As already mentioned, we restrict ourselves here to such modifications of the state of knowledge, which leads to modified ranges of parameter domains. Aim is the assessment of the influence of scenario class modifications and thus modifications of the design space \( X \) on the outcomes.

For realizing this approach, we have to compare a general scenario \( x \in X \) with a corresponding reference scenario \( x' \in X' \subseteq X \). The corresponding modification of the input \( x \) is realized by applying a transformation mapping \( g : X \to X' \subseteq X \). The resulting change of the outcome of the simulation is determined by calculating the difference of the value of an observable \( o \) like \( \Delta N \).

Thus, we are executing a comparison of two scenarios \( x, x' \) related to each other by \( x' = g(x) \) via a relative assessment measure \( d_o(x, g(x)) := o(x) - o(g(x)) \). This can be diagramed as follows.

\[
\begin{align*}
\text{general case} & \quad x & \xrightarrow{\text{sim}} & o(x) & \xrightarrow{\Delta} & d_o(x, g(x)) := o(x) - o(g(x)) & \text{comparison} \\
\text{reference case} & \quad g(x) & \xrightarrow{\text{sim}} & o(g(x))
\end{align*}
\]

The measure \( d_o \) isolates the effects resulting from the application of the transformation \( g \) between general scenario \( x \) and reference scenario \( x' = g(x) \), while it abstracts from other properties common to \( x, x' \). The comparisons utilized in our analysis are listed in table 5.

For the analysis of the influence of knowledge modifications, we have used the same simulation runs as described in section 4.1. The numerical results of the analysis are represented in the tables 10 - 13 in the appendix.

We begin the analysis with a discussion of the influence of kinetic superiority or inferiority on the changes of the outcomes. Corresponding histograms of the behavior of \( \text{mean}(d_{\Delta N}) \) and \( \text{mean}(d_{L_b}) \) are given in figure 6. For the transformation classes A2 and A3, adding cyber capabilities will increase the number of survivors especially for situations with kinetic inferiority. The effect for situations with kinetic superiority is significantly smaller. For the general case and kinetically equal forces, no significant effect can be observed for the cases A1 and D1 concerning \( \text{mean}(d_{\Delta N}) \) or \( \text{mean}(d_{\Delta D}) \).

From the viewpoint of the absolut number \( L_b \) of losses, the situation is different. The value of \( |L_b| \) is significantly larger for kinetically equal forces than for the general case. Figure 10 considers the value distributions of \( \Delta N \) and of \( L_b \) for kinetic superiority or inferiority without distinguishing different levels.

Concerning the behavior in the case of kinetic superiority resp. inferiority, figure 5 provides some supplementary information. An additional cyber capability for Blue (case A3) increases the losses especially for kinetically equal forces. For kinetic superiority resp. inferiority, the increase is larger resp. smaller than in the general case. Equalizing the red capabilities by adding a cyber capability to the red force as well (case A2) leads to a different behavior. Here, the number of losses will increase for Blue especially in the case of kinetic superiority.

Of special interest are situations, in which the winning side changes due to the usage of malware. Such situations are considered in more detail in the figures 5, 7, 12. Whereas figure 5 gives mean values of the changes of the relative number \( \Delta N \) of survivors and of the absolute number \( L_b \) of losses for transitions between scenario classes, figure 12 in the appendix focuses more detailed on the influence of malware attacks on the value distributions of surviving and killed force elements.

Accordingly, histograms of \( d_{\Delta N} \) and \( d_{L_b} \) are given for the transformation classes A1, A2, and A3 (see table 5). The data are presented with and without restriction to situations with a change of the winning side due to cyber combat support. All data indicate, as expected, that malware can turn around a situation in a significant number of situations. An especially large number of
Figure 5: Mean changes of observables for various types of scenario class changes. The first two bar charts document the mean values of the changes of the relative number $\Delta N$ of survivors and of the absolute number $L_b = D_b(t_{\text{end}})$ of losses for the transitions between scenario classes defined in table 5. Below, the corresponding values for situations with a change of the winning side due to the transitions are given. The results are grouped according to the transformation classes A1, A2, A3, D1, D2, D3; each group covers the case without other constraints, the case of kinetically equal forces, and the cases of kinetic superiority resp. inferiority.

Let us at first consider the general cases shown in the upper two charts. For A1 and D1, mean($d_{\Delta N}$) and mean($d_{L_b}$) is close to zero, whereas for A2/A3 resp. D2/D3 significant deviations can be observed. The different behavior is caused by the fact that both A1 and D1 describe transformations between symmetric cases, whereas A2, A3, D2, and D3 transforms symmetric to asymmetric cases and vice versa.

The mean values of the measures $d_{\Delta N}$, $d_{L_b}$ restricted to situations with a change of the winning side are usually much more pronounced. For kinetically equal forces, this scale up of the values is smaller than in the other cases, however. No data are given for kinetically equal forces for the classes A1 and A3, since the original situation has an even outcome per definition. For kinetically superior (blue) forces in the case A3, which describes the addition of cyber capabilities to Blue, naturally no change of the winning side can be expected.
| Id | General Case | Reference Case | Description |
|----|--------------|----------------|-------------|
|    | 'gen'        | 'kin'          | General case vs. pure kinetic combat |
| A1 | 'gen'        | 'b-a'          | General case vs. one-sided malware attack (Red equalizes the cyber capability of Blue; equivalently, Blue loses perfect immunity against cyber attacks) |
| A2 | 'b-a'        | 'kin'          | One-sided malware attack vs. pure kinetic combat (Additional one-sided cyber capability for Blue; equivalently, Red loses perfect immunity against cyber attacks contrary to Blue) |
|    | 'gen'        | 'pat'          | General case vs. combined kinetic/cyber combat without countermeasures |
| D1 | 'gen'        | 'b-p'          | General case vs. one-sided malware defense (Red makes countermeasures available equalizing corresponding capabilities of Blue) |
| D2 | 'b-p'        | 'pat'          | One-sided malware defense vs. combined kinetic/cyber combat without countermeasures (Blue gains one-sided capability of applying countermeasures) |

Table 5: List of generic comparisons between two situations (designated as the general and the reference case), whereby general and reference case belong to the scenario classes presented in table 4. We distinguish comparisons related to malware attack capabilities and to malware defense capabilities related to the patching process.

Winning changes are observed for one-sided capabilities (see figures 5 and 7). One effect of the changes of the winning side is the absolutely large value of the minimum and maximum of \( d_\Delta N \) and \( d_\Delta D \) (see tables 10 - 13). This indicates the possibility of a large decrease or increase of the corresponding observables.

### 4.3 Influence of Dynamic Phenomena

In this paper, the model is analyzed based on input-outcome relationships. This essentially abstracts from the dynamics of the model. For enabling a better understanding of the model behavior, at least an rudimentary look at the phenomena of the dynamical evolution of a situation seems to be helpful, however.

Since infected force elements may be subject to a reduction of kinetic effectiveness, a temporal coincidence of the peak of infection in a force and the phase of kinetic combat is advantageous for the opposing force. Timing of the cyber attack and parametrization of the malware have to be set accordingly. Choosing an attack time too early gives the enemy the option of patching and thus restoring the kinetic effectiveness of many force elements until kinetic combat starts, whereas a late start time of the malware attack does not yet have a significant influence on the kinetic combat due to the small number of infections taking place until \( t_{kin} \) is reached. Let us consider some specific examples.

An alignment of the malware infection peak with the phase of kinetic combat can be reached
Figure 6: The charts show the dependence of the behavior of the system on the level of kinetic superiority or inferiority. For this purpose, the set of scenarios was partitioned in 10 classes depending on the value of $\Delta N$ for the associated pure Lanchester scenario. Scenarios with the strongest inferiority $\Delta N < -0.8$ are shown at the outermost left in the histograms, the scenarios with the strongest superiority $\Delta N > 0.8$ at the outermost right. In the first row, we show the mean values of $\Delta N$, $\Delta T$, and $L_b$ for general scenarios assuming symmetric cyber capabilities (i.e. scenario class 'gen'). Beyond that, the mean changes $\text{mean}(d\Delta N)$, $\text{mean}(d\Delta T)$, and $\text{mean}(dL_b)$ for the transition classes A1, A2, A3 are given. The variation of $\Delta N$ across the inferiority and superiority classes corresponds to the definition of these classes; the antisymmetry w.r.t. $\Delta N = 0$ is preserved. The additional usage of malware dampening the existing kinetic differences slightly, however, as is indicated by the behavior of $\text{mean}(d\Delta N)$ for the class A1.

The losses are substantially smaller for superior forces than for inferior forces. One has to note, that the highest losses do not occur for extreme inferiority, but for significant inferiority. This is caused by the fact that typically the initial number of force elements in the class of strongest inferiority is quite small, thus not leading to high losses. The additional usage of malware decreases the losses in the case of strong superiority, but will increase it in the case inferiority or weak superiority. The increase is caused by the overall reduction of kinetic effectiveness of force elements due to malware infections, which will level out inferiority and superiority to some degree. As a result, the losses on both sides will increase in many situations.
Figure 7: The bar chart at the top shows the fractions of scenarios \( x \), in which the usage of malware changes the winning side. The chart at the bottom gives the corresponding values for the subset of all scenarios \( x \in X \) with a corresponding pure Lanchester scenario \( g_{kin}(x) \) fulfilling \( \Delta T \geq 50 \), i.e. with a long phase of kinetic combat (see section 4.4). The results are grouped according to the transformation classes \( A1, A2, A3, D1, D2, D3 \); each group covers the case without other constraints, the case of kinetically equal forces, and the cases of kinetic superiority resp. inferiority. No data are given for kinetically equal forces for the classes \( A1 \) and \( A3 \), since the considered transition starts with a scenario with an even outcome per definition. Thus, it does not make sense to talk about a change of the winning side here.

In many cases indeed a turn around of the situation by changing the winning side occurs after additional usage of malware. Furthermore, in the case of long lasting kinetic battles usually a slightly higher fraction of turn-arounds can be observed. This means, malware is more effective in situations, in which it has more time to influence the outcome. For transition classes \( D1, D2, D3 \), which are related to defense capabilities against malware, the fraction of situations with a change of the winning side is typically smaller than for the classes \( A1, A2, A3 \) related to the overall malware usage capability. This is caused by the more radical changes described by the transition classes \( A1, A2, A3 \).

by setting the value of the infection rate \( \beta \) appropriately. High infection rates are not always recommendable due to a maybe untimely peak of infections. Similarly, a prolongation of the duration \( \Delta t_m \) of a malware attack may sometimes have negative consequences as well. For the defending side, analogous paradoxes exist. Early countermeasures set into effect by choosing an appropriate \( \Delta t_p \) may sometimes be disadvantageous. The malware epidemics may be weakened, thus shifting the epidemics peak to later times. As a consequence, the peak of infections may now be located in the phase of kinetic combat causing a larger number of losses than before.

At the cyber level, the co-occurring reduction of malware attack capabilities of the defender — only vulnerable and patched force elements can execute a malware attack, but not infected force elements — is a back-effect on the attacker.

The influence of the variation of some input parameters on the relative number \( \Delta N \) of survivors is shown exemplary in figure 8. The figure also shows the sometimes minor importance of the duration \( \Delta t_m \) of a malware attack. This supports the conjecture that an effective malware attack does not necessarily need to last long.
Figure 8: Relationship between variations of the input and the outcome of the simulation. We have calculated the dependence of the relative number $\Delta N$ (black line) of survivors on the variations of several input parameters for an example defined by the parameter values given in the table. The input parameters taken into consideration are (from left to right, from top to bottom) $\Delta t_b$, $\Delta t_{mb}$, $\Delta t_{pb}$, $\alpha_b$, $\beta_r$, and $\gamma_r'$. The plots indicate the influence of the position $t_{\text{max}}(I_r)$ of the malware infection peak and the phase of kinetic combat relative to each other. This is done by showing the position of the time $t_{\text{max}}(I_r)$ (red line) at which the maximum number of infected force elements is reached, with start and end time $t_{\text{kin}}^{\text{start}}$, $t_{\text{kin}}^{\text{end}}$ of kinetic combat (grey region). As can be seen, the change of input parameters may lead to shifts of the time $t_{\text{max}}(I_r)$. The relationship is quite often nontrivial. Note that timing of countermeasures of Red has an influence as well.
4.4 Duration of Kinetic Combat

Numerical data about the duration $\Delta T$ of kinetic combat for different scenario classes are given in the tables 6–9. For all scenario classes, the mean duration $\text{mean}(\Delta T)$ of kinetic combat is much smaller than the observed maximum duration $\text{max}(\Delta T)$. The minimum duration $\text{min}(\Delta T)$, on the other hand, is consistently close to zero. The comparatively large maxima result from situations with very slow dynamics caused by small kinetic effectiveness of both sides. In such a case it will take a long time until one force is annihilated ending the combat. In situations with a still slower dynamics, the simulation misinterprets the absence of significant changes of the force sizes as end of kinetic combat (or triggers even a stop of the whole simulation run). Since this may be done immediately after the start of kinetic combat, one gets $\text{min}(\Delta T) \approx 0$. Another reason for short-duration combats is a strong superiority or inferiority of one force leading to a victory or defeat within short time. Such situations indeed exist, as is indicated by the higher risk for kinetic combat with short duration.

A short duration of the kinetic combat limits the influence of an eventual malware infection. Due to the short duration, the malware has typically not much time for being effective in combat (see figure 13 in the appendix). Furthermore, the probability that the malware infection reaches its peak (and thus its highest effectivity) in the phase of kinetic combat is smaller (look at the wandering of the peak of infection due to input parameter variation in figure 8).

The tables 10–13 supplement the considerations about $\Delta T$ with information about the behavior of $\Delta^2 T$. Figure 6 indicates in the case of kinetic equality that the usage of malware leads typically to a slightly prolonged kinetic combat, often due to reduced kinetic effectiveness of both sides as demonstrated in figure 6. The equalization of the kinetic effectiveness of the two forces is another possible cause. In fact, the duration $\Delta T$ of kinetic combat is the longest for kinetically equal forces. With increasing degree of inferiority or superiority, the duration of kinetic combat decreases, whereby the duration decreases stronger in the case of superiority than in the case of inferiority. In figure 13 in the appendix, the tendency of an equalization of effectiveness by malware usage can be observed as a shift of the peak in the distribution of losses to higher values especially for short-duration kinetic combats.

In some situations, however, the additional usage of malware reduces the duration significantly. In such cases, presumably the malware turns out to be effective for just one side. This will simultaneously shorten and intensify kinetic combat. Obviously, the effects enabling a faster decision of combat are stronger than than the prolongation of kinetic combat due to reduced kinetic effectiveness.

5 Outlook

5.1 Our Main Contributions

- Enabling comparisons between scenarios by simulation-based calculation of the scenario outcomes and their quantitative assessment.
- Enabling absolute assessments of scenario outcomes by referring to their possible range.
- Analysis of various scenario classes under inclusion of uncertainties using Monte-Carlo simulations.
- Inclusion of knowledge and assumptions about the situation by information-theoretic principles.
- Automated model-based calculation of statistical scenario class properties like the risk.
- Determination of the changes of the outcomes after an update of the available knowledge.
- Demonstration of synergies resulting from a combined handling of availability and malware infections.
5.2 Analysis vs. Computation

The paper discusses the interactions between security and availability based on a model representing the effects of self-replicating malware propagating across force elements engaged in kinetic combat. The behavior of the model — especially the influence of malware on kinetic combat — was analyzed both analytically and computationally. In this way, synergies between analytical and computational methods could be exploited. The analytical part makes essential contributions for enabling a computational analysis under well-defined conditions and plays a decisive role in the interpretation of the results. The computational part, on the other hand, provides the calculation of the statistics of outcomes, which is done quantitatively based on Monte-Carlo simulations and can hardly be realized at the analytical level.

5.3 Abstraction Level of Model

Despite of the simplicity of the model, we have been able to gain new insight into the properties and behavior of a combined kinetic and cyber warfare model. This may be astonishing in view of the many missing details. Due to the many unknowns, the usability of a much more detailed model seems to be indeed questionable. Substantial details characterize a very specific situation. The probability for a future situation to coincide with these details becomes infinitesimally small. On the other hand, even highly detailed models may not reproduce all effects occurring in reality. A highly abstract model has decisive advantages. Besides of allowing an analytical handling, a simple model of small computational complexity assures a practical tractability of the large number of simulation runs, which are required for reaching a sufficiently dense coverage of the design space $X$. We have made use of two paradigms for gaining the necessary simplicity. First, we have chosen a system dynamics model (though with some extensions like an event-like structure). Second, we have permitted descriptive modeling aspects like the inclusion of exponents $p, q$ instead of insisting on purely explanatory models.

5.4 Synergies between Dependability Aspects

We have discussed the interplay between the availability of capabilities of force elements and a propagating malware infection. Whereas the malware reduces the kinetic effectiveness of a force impeding its capability to carry out kinetic combat, kinetic capabilities will restrict in turn both malware attack and patching capabilities of the enemy. Effects of the malware on the availability can be determined directly by quantifying the outcome of the kinetic combat with and without usage of malware. The availability perspective, on the other hand, can be used to give the malware infection a ‘meaning’ beyond the rudimentary observation whether an infection exists or not. In this way our considerations show the strengths of the domain of dependability, which discusses various secondary system properties (availability, reliability, safety, security, maintainability, ...) in a combined way. The advantage consists of taking interactions and trade-offs between the secondary properties into account.

Accordingly, the approach presented in this paper is also related to the unified simulation-based risk assessment concept for safety and security suggested in [5],[6]. Whereas malware aspects belong to the domain of security, the notion of availability is related to both safety and security. Though appealing from the theoretical point of view, a practical realization of an ‘exact’ simulation-based risk assessment is impeded often by the very high computational complexity of such an algorithm. This complexity results from the simulation of the various options of system evolutions for determining the contributions of these branches to the overall risk in a brute-force way. Maybe the principle of a knowledge-based selection of representative scenarios provides a viable option for the approximation of the precise value of the risk in this more complex context as well. The idea is to restrict the simulation runs to a limited number of appropriate evolution branches, whereby the representativeness of the contributions of these branches to the risk has to be assured by corresponding system properties. Monte-Carlo simulation based risk assessments are already successfully applied to e.g. the assessment of project risks [19].

---

3The primary system properties are the system functionalities.
5.5 Future Research

The semi-automatization achieved by the implementation of a model-based computational analysis process can be used to analyze the differences between various attack methods, infection mechanisms, propagation pathways, and countermeasures. Furthermore, it enables the experimentation with the consequences of different knowledge (or assumptions) about the situation. In our paper the considerations are limited to the most simple constraints leading to uniform probability distributions for the design space. The full vision would be to run a maximum-entropy algorithm for defining probabilities of scenario selection for much more general constraints and knowledge fragments. Another opportunity for future research is a closer look at the underlying dynamics. Our experiments have shown that the timing of actions and countermeasures may influence the outcome significantly.

For optimizing the utilization of malware, the peak of the malware infection presumably has to be aligned with the phase of kinetic combat. Furthermore, the characteristics of malware propagation and of the force elements have to be adapted to each other. It would be interesting to discuss the improvements possible by such an optimization of the malware utilization.

6 Acknowledgements

The authors are grateful for many helpful remarks provided by Filipa Campos-Viola, Stefan Hahndel, Thomas Rieth, Harald Schaub, and Christine Schwarz-Hemmert. Additionally, we want to thank Simon Hurst for his support for validating the implementation of the computational model.

References

[1] James O Berger. *Statistical decision theory and Bayesian analysis*. Springer Science & Business Media, 2013.

[2] Keith Conrad. Probability distributions and maximum entropy. *Entropy*, 6(452):10, 2004.

[3] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1(1):24–34, 2011.

[4] Dancho Danchev. Coordinated russia vs georgia cyberattack in progress. *ZDNet*, 2008.

[5] Joachim Draeger. Roadmap to a unified treatment of safety and security. In *Proceedings of the 10th IET System Safety and Cyber-Security Conference*. IET, 2015.

[6] Joachim Draeger. Formalized risk assessment for safety and security. *arXiv preprint 1709.00567*, 2017.

[7] Joseph H Engel. A verification of lanchester’s law. *Journal of the Operations Research Society of America*, 2(2):163–171, 1954.

[8] Kenneth Geers. *Cyber war in perspective: Russian aggression against Ukraine*. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, 2015.

[9] Rebecca Grant. Airpower made it work. *Air Force Magazine*, 82(11):30–37, 1999.

[10] Edward F Halpin, Philippa Trevorrow, David Webb, and Steve Wright. *Cyberwar, netwar and the revolution in military affairs*. Springer, 2006.

[11] Edwin T Jaynes. Information theory and statistical mechanics. *Physical review*, 106(4):620, 1957.

[12] William O Kermack and Anderson G McKendrick. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 115(772):700–721, 1927.
[13] Frederick William Lanchester. Mathematics in warfare. *The world of mathematics, 4:2138–2157*, 1956.

[14] Robert Lee, Michael Assante, and Tim Conway. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[15] Thomas W Lucas and Turker Turkes. Fitting lanchester equations to the battles of kusk and ardennes. *Naval Research Logistics (NRL)*, 51(1):95–116, 2004.

[16] Niall J MacKay. Lanchester combat models. *arXiv preprint math/0606300*, 2006.

[17] Helmut Martin-Jung. Cyberangriff auf den bundestag - für lücken büszen. *Süddeutsche Zeitung*, 2015.

[18] D McMorrow. Science of cyber-security. Technical report, Mitre corporation, 2010.

[19] Mira Mileusnić Škrtić and Karolina Horvatinčić. Project risk management: comparative analysis of methods for project risks assessment. *Collegium antropologicum*, 38(1):125–134, 2014.

[20] Bimal Kumar Mishra and Gholam Mursalin Ansari. Differential epidemic model of virus and worms in computer network. *IJ Network security*, 14(3):149–155, 2012.

[21] Bimal Kumar Mishra and Apeksha Prajapati. Modelling and simulation: Cyber war. *Procedia Technology*, 10:987–997, 2013.

[22] Scott Musman, Aaron Temin, Mike Tanner, Dick Fox, and Brian Pridemore. Evaluating the impact of cyber attacks on missions. In *International Conference on Cyber Warfare and Security*, page 446. Academic Conferences International Limited, 2010.

[23] Jose Pagliery. Scary questions in ukraine energy grid hack, 2016.

[24] Harrison C Schramm and Donald P Gaver. Lanchester for cyber: The mixed epidemic-combat model. *Naval Research Logistics (NRL)*, 60(7):599–605, 2013.

[25] Thorsten Severin, Michael Nienaber, and Andrew Heavens. Cyber attack on german parliament still active, could cost millions. 2015.

[26] Sekaran Sneha, Lakshmanan Malathi, and R Saranya. A survey on malware propagation analysis and prevention model. *Int J Adv Technol*, 6(148):2, 2015.

[27] Pei-Chen Sung and Chien-Yuan Su. Using system dynamics to investigate the effect of the information medium contact policy on the information security management. *International Journal of Business and Management*, 8(12):83, 2013.

[28] James G Taylor. Lanchester-type models of warfare and optimal control. *Naval Research Logistics (NRL)*, 21(1):79–106, 1974.

[29] James G Taylor. *Lanchester-Type Models of Warfare. Volume I & II*. 1983.

[30] Fatih Yildiz. Modeling the continuous effects of cyber operations on kinetic battles. *Turkish Army War College*.

[31] Fatih Yildiz. Modeling the effects of cyber operations on kinetic battles. Technical report, Naval Postgraduate School Monterey CA Dept of Operations Research, 2014.
A Appendix: Results
Figure 9: Behavior of the relative number $\Delta N$ of survivors for different scenario classes. The figure shows on the left side the value distributions of $\Delta N$ in general case, the case with one-sided usage of malware and the case with one-sided defense, i.e. with one-sided patching and malware removal capabilities. The right column gives histograms for the situations with kinetic equality as additional constraint. For the symmetric case, the histogram has a flat peak symmetric w.r.t. zero according to $\text{mean}(\Delta N(\tilde{X})) \approx 0$. The whole possible range of values $\Delta N(\tilde{X}) \subseteq [-1,1]$ is covered. For the cases with one-sided additional capabilities for Blue, the peak of the distribution of $\Delta N$ is shifted toward positive values, i.e. one may expect more survivors for Blue than for Red.

For scenario classes assuming kinetically equal forces, the variations of the outcomes are much smaller. For asymmetric capabilities, the peak of the values of $\Delta N$ for kinetically equal forces is closer to the center than for situations without equality constraint. For one-sided cyber attacks with kinetic equality it holds $\Delta N \geq 0$.

The behavior of one-sided defense is halfway between the symmetric general case and the situation of a one-sided malware attack.

### Table 9.1: Behavior of $\Delta N$ for different scenario classes

| Scenario Class         | All Kinetic Situations | Kinetically Equal Situations |
|------------------------|------------------------|-----------------------------|
| General Situations     | ![Histogram](image1)    | ![Histogram](image2)        |
| One-Sided Attack       | ![Histogram](image3)    | ![Histogram](image4)        |
| One-Sided Defense      | ![Histogram](image5)    | ![Histogram](image6)        |
Figure 10: The histograms show the value distributions of $\Delta N$ (left column) and $L_b = D_b(t_{\text{end}})$ (right column) for the general case (top row) and for the subclasses of kinetic superiority (middle row) and of kinetic inferiority (bottom row). Concerning the case of kinetic superiority, the value distribution of $\Delta N$ for $\Delta N \geq 0$ close to zero is approximately flat with a strong decline towards large positive values of $\Delta N$. This means, that even in the case of superiority, almost all force elements will survive only in a few cases. The tail of the distribution for $\Delta N < 0$ indicates, that the usage of malware by both sides may change the winner in a significant number of cases. For kinetic inferiority, the situation is similar; situations with a number of blue survivors close to zero are less frequent however. This difference can be detected in the distribution of losses $L_b$ as well. On the whole, for kinetic superiority a low number of losses is much more frequent than a high number with a monotonic decline. In the case of kinetic inferiority, the peak of the frequency is shifted to slightly higher values as one may have expected.
In the case of kinetic inferiority, a one-sided cyber attack can very well turn around the situation as indicated by non-vanishing frequencies for $\Delta N \geq 0$. The situation of a one-sided defense essentially resembles the one of one-sided attacks, but is less pronounced. Whereas for kinetic superiority with or without one-sided cyber attacks a win is assured (i.e. $\Delta N \geq 0$), one-sided capabilities of cyber defense will not exclude outcomes with $\Delta N < 0$. This means, the opponent may be able to turn around the situation.

The relative number $\Delta D$ of losses behaves analogously to $\Delta N$, though of course $\Delta N > 0$ is related to $\Delta D < 0$ and vice versa. Since even a convincing win is usually associated with some losses, the value distribution of $\Delta D$ is typically less pronounced than $\Delta N$. In the case of kinetic superiority, the opposing force suffers still the majority of losses. For kinetic inferiority, however, the value distribution of $\Delta D$ already becomes roughly symmetric, though a significant shift towards $\Delta D > 0$ prevails.

The correspondence between $\Delta N$ and $\Delta D$ can be extended to the distribution of absolute losses $L_b$. As already indicated in the text, a small value of $L_b$ is much more frequent than a high value in general. The observed decline is typically monotonic. In the case of kinetic inferiority, however, the peak of the frequency is shifted to slightly higher values.
Figure 12: Value distributions of the relative number $\Delta N$ of survivors and of the absolute number $L_b$ of losses for the transition classes A1, A2 and A3. Again, we consider both the whole set of situations belonging to the scenario class change and the subset, in which the winning side changes in the course of transition. As usual, the transition class A1 leads to approximately symmetric distributions for $d_{\Delta N}$ and $d_{L_b}$. For A2 and A3, in the contrary, the one-sided addition of a malware usage capability can also only lead to improvements for one side. Accordingly, $d_{\Delta N}$ and $d_{L_b}$ are restricted for A2 to negative resp. positive values — the number of survivors can only increase, and the number of losses can only decrease. For A3, the distributions change their sign. The distributions of $d_{\Delta N}$, $d_{L_b}$ for the transitions A1, A2, A3 restricted to situations with a malware-induced change of the winning side (right part of the figure) exhibit a much larger variance.
Figure 13: Dependence of survivors and losses on the duration of kinetic combat. Since the effectiveness of malware presumably influences the duration of kinetic combat, we take a look at the value distributions of the relative number of survivors $\Delta N$ (left column) and the absolute number of losses $L_b$ (right column). This is done for short ($\Delta T < 50$) and long ($\Delta T \geq 50$) kinetic combats, whereby the distinction between a short and a long duration is done for both the corresponding pure Lanchester situation and the combined kinetic/cyber case.

In general, a long duration of kinetic combat leads to a higher frequency of values of $\Delta N$ close to zero, i.e. of situations with an even outcome. For short durations, in the contrary, values of $\Delta N$ far away from zero are more prominent. Since for long lasting kinetic combats a low number of losses is more frequent than a high number, the prevalence of even outcomes must not be compulsory interpreted as mutual annihilation of both forces. Ineffectiveness of the forces leading to a stop of simulation due to a faded dynamics is considered as preferable explanation. For short durations, in the contrary, the peak of losses is shifted towards higher values interpretable as higher intensity of the kinetic combats than usual.
Table 6: The table summarizes the behavior of the observables $\Delta N$, $\Delta D$, $\Delta T$ as well as the risk $\mathcal{R}$ for the three basic cases of model behavior concerning malware attacks. The three basic cases are the general system, situations with one-sided malware attacks, and the pure Lanchester case without any cyber component at all. The summary includes minimum, maximum, statistical mean, and statistical variance. Additionally, corresponding data for the special case of two forces of equal size and kinetic effectiveness are given. A short discussion of these data can be found in section 4.1.
Table 7: The table summarizes the behavior of the observables $\Delta N$, $\Delta D$, $\Delta T$ as well as the risk $\mathcal{R}$ for the three basic cases of model behavior concerning malware defense. The three basic cases are the general system, situations with one-sided malware recovery, and situations without recovery for both sides. A short discussion of these data can be found in section 4.1.
### Malware Attack

| Parameter | Blue as Kinetically Superior Force | Blue as Kinetically Inferior Force |
|-----------|-----------------------------------|-----------------------------------|
|           | General | One-Sided | Pure Kinetic | General | One-Sided | Pure Kinetic |
| $\min \Delta N$ | -0.967 | 0.001 | 0 | -0.993 | -0.993 | -0.993 |
| $\max \Delta N$ | 0.993 | 0.993 | 0.982 | 0.893 | 0.893 | 0 |
| $\text{mean} \Delta N$ | 0.335 | 0.429 | 0.374 | -0.348 | -0.277 | -0.381 |
| $\text{var} \Delta N$ | 0.103 | 0.061 | 0.059 | 0.097 | 0.099 | 0.059 |
| $\min \Delta D$ | -0.981 | -0.981 | -0.981 | -0.913 | -0.95 | -0.69 |
| $\max \Delta D$ | 0.957 | 0.786 | 0.807 | 0.967 | 0.952 | 0.962 |
| $\text{mean} \Delta D$ | -0.146 | -0.24 | -0.185 | 0.149 | 0.079 | 0.183 |
| $\text{var} \Delta D$ | 0.113 | 0.077 | 0.075 | 0.112 | 0.115 | 0.074 |
| $\min \Delta T$ | 0 | 0 | 0 | 0 | 0 | 0 |
| $\max \Delta T$ | 491.155 | 519.655 | 461.574 | 993.339 | 993.339 | 577.697 |
| $\text{mean} \Delta T$ | 61.983 | 49.946 | 53.92 | 61.836 | 65.241 | 52.555 |
| $\text{var} \Delta T$ | 6394.049 | 4657.775 | 4906.755 | 6772.351 | 6684.845 | 4672.606 |
| $\mathcal{R}$ | 0.261 | 0.198 | 0.251 | 0.403 | 0.391 | 0.428 |

Table 8: The table summarizes the behavior of the observables $\Delta N$, $\Delta D$, $\Delta T$ as well as the risk $\mathcal{R}$ for the three basic cases of model behavior concerning malware attacks. The three basic cases are the general system, situations with one-sided malware attacks, and the pure Lanchester case without any cyber component at all. The summary includes minimum, maximum, statistical mean, and statistical variance. We give corresponding values for Blue as kinetic superior as well as inferior force. A short discussion of these data can be found in section 4.1.
### Malware Defense

| Parameter | Blue as Kinetically Superior Force | Blue as Kinetically Inferior Force |
|-----------|------------------------------------|------------------------------------|
|           | General | One-Sided | No Defense | General | One-Sided | No Defense |
| min $\Delta N$ | $-0.967$ | $-0.967$ | $-0.967$ | $-0.993$ | $-0.99$ | $-0.99$ |
| max $\Delta N$ | $0.993$ | $0.993$ | $0.972$ | $0.893$ | $0.893$ | $0.867$ |
| mean $\Delta N$ | $0.335$ | $0.375$ | $0.328$ | $-0.348$ | $-0.296$ | $-0.343$ |
| var $\Delta N$ | $0.103$ | $0.096$ | $0.113$ | $0.097$ | $0.114$ | $0.106$ |
| min $\Delta D$ | $-0.981$ | $-0.981$ | $-0.981$ | $-0.913$ | $-0.962$ | $-0.962$ |
| max $\Delta D$ | $0.957$ | $0.957$ | $0.958$ | $0.967$ | $0.955$ | $0.973$ |
| mean $\Delta D$ | $-0.146$ | $-0.187$ | $-0.139$ | $0.149$ | $0.097$ | $0.144$ |
| var $\Delta D$ | $0.113$ | $0.105$ | $0.12$ | $0.112$ | $0.125$ | $0.116$ |
| min $\Delta T$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| max $\Delta T$ | $491.155$ | $510.155$ | $731.777$ | $993.339$ | $653.398$ | $603.747$ |
| mean $\Delta T$ | $61.983$ | $58.622$ | $66.579$ | $61.836$ | $71.832$ | $65.827$ |
| var $\Delta T$ | $6394.049$ | $5872.975$ | $6992.89$ | $6772.351$ | $8588.886$ | $6867.066$ |
| $\mathcal{R}$ | $0.261$ | $0.229$ | $0.257$ | $0.403$ | $0.383$ | $0.391$ |

Table 9: The table summarizes the behavior of the observables $\Delta N$, $\Delta D$, $\Delta T$ as well as the risk $\mathcal{R}$ for the three basic cases of model behavior concerning malware defense. The three basic cases are the general system, situations with one-sided malware recovery, and situations without recovery for both sides. We give corresponding values for Blue as kinetic superior as well as inferior force. A short discussion of these data can be found in section 4.1.
Table 10: Some statistical properties of the comparison measure $d$ applied to the various general/reference case comparisons indicated in table 5. We give corresponding values for both unconstrained forces and equal-sized forces. A short discussion of these data can be found in section 4.2.

| Parameter          | Unconstrained Forces | Kinetically Equal Forces |
|--------------------|----------------------|--------------------------|
|                    | $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ | $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ |
| Case A1: Malware attack for both sides omitted |
| min                | $-1.27$     | $-1.519$    | $-560.165$ | $-0.921$    | $-0.96$     | $-0.987$     | $-503.17$    | $-0.93$    |
| max                | $1.519$     | $1.27$      | $905.4$    | $0.861$     | $0.987$     | $0.96$       | $399.95$     | $0.187$    |
| mean               | $-0.003$    | $0.003$     | $8.664$    | $-0.007$    | $-0.004$    | $0.004$      | $-8.112$     | $-0.057$   |
| var                | $0.048$     | $0.048$     | $2496.265$ | $0.018$     | $0.067$     | $0.067$      | $1797.813$   | $0.024$    |

| Case A2: Malware attack for one side omitted, present for the other |
| min                | $-1.408$    | $-0.051$    | $-300.178$ | $-0.102$    | $-1.38$     | $-0.014$     | $-503.17$    | $-0.014$   |
| max                | $0.051$     | $1.408$     | $449.3$    | $0.864$     | $0.014$     | $1.38$       | $344.8$      | $0.921$    |
| mean               | $-0.082$    | $0.082$     | $4.42$     | $0.038$     | $-0.113$    | $0.113$      | $0.506$      | $0.036$    |
| var                | $0.029$     | $0.029$     | $1611.839$ | $0.01$      | $0.039$     | $0.039$      | $1174.36$    | $0.006$    |

| Case A3: Malware attack for one side omitted, not present for the other |
| min                | $-0.001$    | $-1.519$    | $-560.165$ | $-0.932$    | $-0.001$    | $-0.987$     | $-301.55$    | $-0.942$   |
| max                | $1.519$     | $0.001$     | $905.4$    | $0.017$     | $0.987$     | $0.001$      | $180.8$      | $0.005$    |
| mean               | $0.079$     | $-0.079$    | $4.244$    | $-0.045$    | $0.109$     | $-0.109$     | $-8.618$     | $-0.093$   |
| var                | $0.026$     | $0.026$     | $1619.68$  | $0.011$     | $0.032$     | $0.032$      | $1052.682$   | $0.027$    |
| Parameter | Blue as Kinetically Superior Force | Blue as Kinetically Inferior Force |
|-----------|-----------------------------------|-----------------------------------|
| $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ | $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ |
| **Case A1: Malware attack for both sides omitted** | | | | | | | |
| min | $-1.27$ | $-0.813$ | $-243.1$ | $-0.813$ | $-0.758$ | $-1.519$ | $-560.165$ | $-0.921$ |
| max | 0.813 | 1.27 | 368.153 | 0.861 | 1.519 | 0.758 | 905.4 | 0.077 |
| mean | $-0.039$ | 0.039 | 8.063 | 0.01 | 0.034 | $-0.034$ | 9.28 | $-0.025$ |
| var | 0.05 | 0.05 | 2018.973 | 0.026 | 0.044 | 0.044 | 2986.509 | 0.009 |
| **Case A2: Malware attack for one side omitted, present for the other** | | | | | | | |
| min | $-1.408$ | $-0.024$ | $-243.6$ | $-0.008$ | $-1.325$ | $-0.051$ | $-300.178$ | $-0.102$ |
| max | 0.024 | 1.408 | 415.655 | 0.864 | 0.051 | 1.325 | 449.3 | 0.733 |
| mean | $-0.094$ | 0.094 | 12.037 | 0.063 | $-0.07$ | 0.07 | $-3.405$ | 0.012 |
| var | 0.038 | 0.038 | 1867.009 | 0.016 | 0.019 | 0.019 | 1229.309 | 0.002 |
| **Case A3: Malware attack for one side omitted, not present for the other** | | | | | | | |
| min | $-0.001$ | $-0.82$ | $-248.31$ | $-0.82$ | 0.0 | $-1.519$ | $-560.165$ | $-0.32$ |
| max | 0.82 | 0.001 | 172.05 | 0.0 | 1.519 | 0.0 | 905.4 | 0.017 |
| mean | 0.055 | $-0.055$ | $-3.974$ | $-0.052$ | 0.104 | $-0.104$ | 12.686 | $-0.037$ |
| var | 0.012 | 0.012 | 442.53 | 0.011 | 0.039 | 0.039 | 2688.66 | 0.012 |

Table 11: Some statistical properties of the comparison measure $d$ applied to the various general/reference case comparisons indicated in Table 5. We give corresponding values for Blue as kinetic superior and for Blue as inferior force. A short discussion of these data can be found in section 4.2.
### Table 12: Some statistical properties of the comparison measure $d$ applied to the various general/reference case comparisons indicated in table 5. We give corresponding values for both unconstrained forces and equal-sized forces. A short discussion of these data can be found in section 4.2.

| Parameter | Unconstrained Forces | Kinetically Equal Forces |
|-----------|-----------------------|--------------------------|
|           | $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ | $d_{\Delta N}$ | $d_{\Delta D}$ | $d_{\Delta T}$ | $d_{L_b}$ |
| min       | $-1.36$ | $-1.593$ | $-634.473$ | $-0.813$ | $-1.568$ | $-1.472$ | $-596.66$ | $-0.904$ |
| max       | 1.593 | 1.36 | 893.6 | 0.845 | 1.472 | 1.568 | 324.35 | 0.93 |
| mean      | 0.001 | $-0.001$ | $-4.297$ | 0.008 | $-0.003$ | 0.003 | 0.479 | 0.019 |
| var       | 0.031 | 0.031 | 2551.207 | 0.011 | 0.05 | 0.05 | 1518.741 | 0.016 |

Case D1: Malware defense for both sides omitted

Case D2: Malware defense for one side omitted, present for the other

Case D3: Malware defense for one side omitted, not present for the other

Table 12: Some statistical properties of the comparison measure $d$ applied to the various general/reference case comparisons indicated in table 5. We give corresponding values for both unconstrained forces and equal-sized forces. A short discussion of these data can be found in section 4.2.
Table 13: Some statistical properties of the comparison measure $d$ applied to the various general/reference case comparisons indicated in table 5. We give corresponding values for Blue as kinetic superior and for Blue as inferior force. A short discussion of these data can be found in section 4.2.